No. 10-1011

IN THE

SUPREME COURT OF THE UNITED STATES

HECTOR ESCATON,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

ON WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE FOURTEENTH CIRCUIT

BRIEF FOR RESPONDENT

Team P3

Counsel for Respondent

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

United States Supreme Court Cases

United States Circuit Court Cases

Statutes

Constitutional Provisions

Other Authority

QUESTIONS PRESENTED

I. Did the Fourteenth Circuit err is affirming the District Court's decision denying the Motion to Suppress evidence finding that Cullen did not exceed the scope of the Border Exception and did not violate Petitioner's Fourth Amendment right against unreasonable search by admitting evidence after conducting a routine search at an international border?

II. Does the request and acquisition of Petitioner's historical cell-site location information through a court order constitute a search and violate his Fourth Amendment rights when fewer than seven days' worth of information was collected?

OPINION BELOW

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 for the Fourteenth Circuit, respectfully submit this brief on the merits and ask the Court to affirm the Fourteenth Circuit's decision below.

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 violates, 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

Summary of the Argument:

Because the Fourteenth Circuit did not err in upholding the District Court's ruling denying Escaton's Motion to Suppress evidence, the Respondent respectfully requests this Court uphold the decision of the Fourteenth Circuit.

Escaton's Fourth Amendment right against unreasonable searches was not violated since the search of his electronic devices was part of a routine border search that was conducted at an international border. Searches are deemed reasonable simply by the fact that they occur at the border. A person expects less privacy upon entering and exiting the United States than in his movements and affairs within the United States. There is also a heightened national security interest at an international border with monitoring what is entering and leaving the United States. Because the Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border, border searches are generally deemed reasonable simply by virtue of the fact that they occur at the border. Officer Stubbs performed a routine border search upon Escaton's return back into the United States from Mexico. With Escaton returning back into the United States from an international location, it is not required that Stubbs have reasonable suspicion to be able to search his vehicle and belongings to be able to ensure the national safety of the United States. Therefore, the border exception applies, and this is not a violation of Escaton's Fourth Amendment right.

Nor do the government's requests for historical cell-site location information (CSLI) and for tower dumps violate Escaton's Fourth Amendment right against unreasonable searches and seizures. This is because the searches do not reveal the privacies of Escaton's life and comport with the Court's decision in *Carpenter*. Collection of three-day records does not provide law enforcement with enough information to reveal the intimate details of a person's private life.

Further, they are well within the limit established in *Carpenter.* The same applies to the collection of week day records when the information acquired is less than seven days of information. Finally, the acquisition of the tower dumps are not only not a search under *Carpenter,* but should be treated as business records under the third-party doctrine.

STATEMENT OF THE CASE

Statement of Facts

Petitioner, Mr. Hector Escaton, entered the United States from Mexico through West Texas, the state in which he maintains residency, at an official border checkpoint on September 25, 2019. R. at 2. A routine border search of Petitioner's car was conducted by Customs and Border Protection (CBP) Officer Ashley Stubbs ("Officer Stubbs"), who found three large suitcases in the back of the car. R. at 2. During the search, Officer Stubbs also found an iPhone, a laptop, three external hard drives, and four USB devices. R. at 2. After placing the iPhone on airplane mode and ensuring the laptop was not connected to a wireless service, Officer Stubbs manually searched both devices without assistive technology. R. at 2. Through his manual search he found a paper note below the keyboard of the laptop that read "Call Delores (201) 181-0981 $$$." R. at 2. Officer Stubbs returned Petitioner's iPhone to him but detained the remaining electronic devices after recording the iPhone number. R. at 2-3.

While none of the electronics were password protected, Officer Stubbs found that certain folders on the laptop were password protected, along with the contents of the USB devices. R. at 3. This led him to transfer the electronics to Immigration and Customs Enforcement (ICE) into the care of Senior Special Agent & Computer Forensic Examiner, Theresa Cullen ("Cullen"). R. at 3. Senior Special Agent Cullen used forensic software to copy and scan the electronic devices, a process that takes several hours. R. at 3. At the conclusion of the scan she examined the results and found that the laptop held documents containing several bank account numbers and pins. R.

at 3. Cullen also found traces of malware on the USB devices through her forensic scan. R. at 3. She did not find incriminating evidence on the hard drives, so she deleted those scans and reported her complete findings to Officer Stubbs. R. at 3.

Immediately upon receipt of the incriminating findings, CBP notified the Federal Bureau of Investigation (FBI). R. at 3. The FBI had an open investigation into incidents of "ATM skimming" of Mariposa Bank ATMs in Sweetwater in October 2018. R. at 3. Mariposa Bank owns several branches in Sweetwater, including the Boswell Street branch where the local branch manager discovered the ATM tampering. R. at. 3. Upon further inspection by an ATM engineer it became clear that malware had infected the Boswell Street ATMs through the USB port. R. at 3. The malware allowed the criminal to read information from customers who used the infected ATM terminal. R. at 3. An internal investigation revealed that four additional ATMs in Sweetwater had been used for skimming, along with three in neighboring town Escalante. R. at 3. Mariposa Bank was only able to determine that the skimming occurred in early October. R. at 4.

In addition to the ATMs in Sweetwater that were infected with malware, the internal investigation by Mariposa Bank revealed that two other ATMs in Sweetwater had foreign "skimmers" overlaying the debit card readers that also allowed the criminal to steal customer information. R. at 4. The final Sweetwater ATM was infected with more sophisticated malware that allowed the criminal to take out cash at the ATM. R. at 4. Mariposa Bank estimates $50,000 in losses to both the bank and its customers as a result of the October 2018 ATM skimming. R. at 4. In addition to the monetary loss, hundreds of identities of Mariposa Bank customers were stolen. R. at 4. All of Mariposa Bank's findings were reported to the FBI. R. at 4.

Special Agent Catherine Hale of the FBI began an investigation into the connections between the forensic evidence found on Petitioner's electronics and that reported by Mariposa Bank. R. at 3. She had information on the malware used and surveillance photographs of a man in a black sweatshirt from near three of the ATMs, which she used to request three tower dumps from the cell sites near three Sweetwater ATMs for 30 minutes before and 30 minutes after the man in a black sweatshirt approached the ATMs. R. at 4. Because Agent Hale had Petitioner's information, including his iPhone number, from the CBP she discovered that his was one of the numbers generated from the three tower dumps. R. at 5. She was also able to determine that the malware found on the USB devices in Petitioner's possession was similar to the malware that infected the Mariposa ATMs in Sweetwater. R. at 5.

Based on this information, Agent Hale worked with U.S. Attorney Elsie Hughes to apply for court orders to obtain Petitioner's cell phone records. R. at 5. In her affidavit, Agent Hale notes that the cell towers in Escalante are not as accurate, as it is a small town, and the information collected is often only accurate within 1,000 feet of the individual. R. at 23. Despite this lower accuracy, Agent Hale states that the information collected would be pertinent to her investigation. R. at 25. A federal magistrate judge issued an order directing Petitioner's wireless carrier, Delos Wireless, to disclose the cell site records that correspond to Petitioner's phone number for the period of October 11, 2018 to October 13, 2018. R. at 18. The records placed Petitioner in the area of affected Sweetwater ATMs on October 12, 2018 but did not place him in the area of the Escalante ATMs during that period. R. at 5.

This made the government suspect that the "Delores" identified on the paper note in Petitioner's laptop may have been party to Petitioner's criminal activity. R. at 5. Upon request the magistrate judge issued an additional order to Delos Wireless to disclose cell site information

for both Petitioner's and "Delores's" phone numbers for all weekdays between October 1 and 12 between the hours of 8 AM MDT and 6 PM MDT. R. at 5. The government also requested subscriber information for "Delores's" phone number and found that the number belongs to Delores Abernathy. R. at 5. Also revealed in the records was the fact that Abernathy was in the area of the Escalante ATMs in early October, and that she was in Petitioner's company during the same time period. R. at 5.

Abernathy had been convicted for ATM skimming previously, and a search of her home revealed cash and the same malware that Petitioner stored on his USB devices. R. at 5. She was arrested and entered a plea agreement, and cooperated with the government in its case against Petitioner. R. at 5.

Procedural History

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. Prior to the 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. *Id*. The District Court denied Escatons' Motion to Suppress. *Id*. Escaton appealed to the United States Court of Appeals for the Fourteenth Circuit. R. at 2. The Fourteenth Circuit affirmed the denial of Escatons' motion to suppress evidence. R. at 6. This Court granted certiorari.

ARGUMENT

I. The Fourteenth Circuit did not err in affirming the district court's decision to deny Escaton's Motion to Suppress because his Fourth Amendment rights were not violated since no reasonable suspicion is required to conduct a forensic search of electronic devices at the border.

The Fourth Amendment enumerates with precision the right of people to be secure in their "persons, houses, papers, and effects" against warrantless searches, and requires that

"no warrants shall issue, but upon probable cause, supported by Oath or affirmation." U.S. Const. amend. IV. Long established by this Court, warrantless searches are unreasonable unless a valid exception applies. *Katz v. United States*, 389 U.S. 347, 357 (1967). However, to determine the reasonableness of a border search[1], or of any search for that matter, courts weigh its intrusion on an individual's Fourth Amendment interests against its promotion of a legitimate governmental interests. *United States v. Alfaro-Moncada*, 607 F.3d 720, 727-28 (11th Cir. 2010). The Fourth Amendment does not require any suspicion for forensic searches of electronic devices at the border even though such devices could store vast quantities of records or effects and many people now own them. *United States v. Touset*, 890 F.3d 1228.

The border search exception to the search warrant requirement is not based on the doctrine of exigent circumstances, but rather is a long standing historically recognized exception to the Fourth Amendment's general principle that a warrant must be obtained. *United States v. Ramsey*, 431 U.S. 606, 607 (1977). There has never been any additional

[1] Border searches can also occur in places other than the actual physical border. Two different legal concepts authorize such searches: (1) searches at the functional equivalent of the border; and (2) extended border searches. These concepts allow federal officers to conduct border searches even in situations when it is not feasible to conduct the search at the actual point of entry (e.g., examining a person upon arrival at a U.S. airport rather than during a mid-flight crossing into the country). *See* CRS Report RL31826, *Protecting the U.S. Perimeter: Border Searches Under the Fourth Amendment*, by Yule Kim for an in depth analysis of this issue.

requirement that the reasonableness of a border search depended on the existence of probable cause. *Id*. The Supreme Court has also never required reasonable suspicion for a search of property at the border, however non-routine and intrusive. *United States v. Touset*, 890 F.3d 1227, 1233. The Fourteenth Circuit did not err in affirming the district court's decision to deny Escaton's Motion to Suppress, therefore not denying him of him Fourth Amendment rights.

A. Petitioner's Fourth Amendment rights were not violated with the search of his electronic devices because a person expects less privacy with international affairs.

A person expects less privacy upon entering and exiting the United States than in his movements and affairs within the United States. At the border, an individual has a lesser expectation of privacy, the government a greater interest in searching, and the balance between the interests of the government and the privacy right of the individual is struck more favorably to the government. *See United States v. Alfaro-Moncada*, 607 F.3d 721. Although it may intrude on the privacy of the owner, a forensic search of an electronic device is a search of property that does not require border agents to touch a travelers body, to expose intimate body parts, or to use any physical force. See *United States v. Touset*, 890 F.3d 1228. Those lawfully within the country have a right to free passage without interruption or search unless it is known to a competent official authorized to search, or he has probable cause. *United States v. Ramsey*, 431 U.S. 618.

For many reasons, the expectation of privacy is less at the border than it is in the interior. *United States v. Flores Montano*, 541 U.S. 149, 154-55 (2004). In *Flores Montano*, customs officials seized 37 kilograms of marijuana from respondent's gas tank by removing and disassembling the tank. *See id* at 150. This Court held that defendant did not have a privacy

interest in his vehicle's fuel tank and the disassembly of a gas tank as part of a border search did not require reasonable suspicion. *Id* (noting that Congress has always granted the Executive plenary authority to conduct routine searches and seizures at the border, without probable cause or a warrant, in order to prevent the introduction of contraband into the country). This Court relied on what is characterized as the United States' longstanding right as a sovereign "to protect itself by stopping and examining persons and property crossing into [the] country…" *Id*. at 152-153 (quoting *Ramsey*, 431 U.S. at 616). This court further highlighted that travelers may be so stopped in crossing an international boundary because of national self-protection reasonably requiring one entering the country to identify himself as entitled to come in and his belongings as effects which may be lawfully brought in. *See id* at 154 (noting that that it is difficult to imagine how the search of a gas tank, which should be solely a repository for fuel, could be more of an invasion of privacy than the search of the automobile's passenger compartment). Although the interference with a motorist's possessory interest is not significant, it nevertheless is justified by the Government's paramount interest in protecting the border. *Id*. at 155. Therefore, because the court found no invasion of privacy, there was no violation of respondent's Fourth Amendment rights.

Similarly, in *United States v. Touset*, it was held that the Fourth Amendment does not require any suspicion for forensic searches of electronic devices at the border and in determining whether the information supporting the government's application for a search warrant is impermissibly stale, courts consider the length of time as well as discrete crimes, habits of the accused, character of the items sought, and nature of the premises to be searched. 890 F.3d 1229 (11th Cir. 2018); *see also United States v. Montoya de Hernandez*, 473 U.S. 531 (holding that it is reasonable to detain an individual for the period of time necessary to verify or dispel the

suspicion of the agents in the circumstances). The defendant, a United States traveler, was stopped upon entering an Atlanta airport from an international flight. *Id*. at 1230. Defendant was placed on a "lookout" list and after the defendant deplaned, officials from Customs and Border Protection searched him, manually inspected his electronic devices, found no child pornography, and returned the iPhones and camera to the defendant. *Id*. The officer retained his two laptops, external hard drives, and two tablets for forensic examination. *Id*. Child pornography was then found on the devices. *Id*. The 11th Circuit held that in contrast with the diminished privacy interests of travelers, the government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border. *Id* at 1235. The Court further highlighted that electronic devices should not receive special treatment because so many people own them or because they can store vast quantities of records. *Id*. at 1233; *see also United States v. Arnold*, 533 F.3d 1003 (9th Cir. 2008) (holding that there was no material difference between the search of an electronic storage device and the search of a briefcase, purse, pocket or pictures and thus, like any border search of a "closed container", reasonable suspicion is not required) . Therefore, because the search of defendant's electronic devices did not require any reasonable suspicion and the government's interest was higher than the privacy interest of the defendant, there was no violation of his Fourth Amendment right.

Border searches never require probable cause or a warrant, and the Court requires reasonable suspicion for a search of the border only for highly intrusive searches of a person's body. *United States v. Vergara*, 884 F.3d 1309 (11th Cir. 2018) (noting that highly intrusive searches of a person's body consist of a strip search or an x-ray examination). In *Vergara*, Vergara returned to Tampa, Florida on a cruise ship from Cozumel, Mexico. *Id*. at 1311. Officer Christopher Ragan, an officer with Customs and Border Patrol, identified Vergara and searched

his luggage. *Id*. He then discovered a Samsung phone, an LG phone, and an iPhone. *Id*. Officer Ragan asked Vergara to turn the Samsung phone on and looked through the contents for 2-5 minutes. *Id*. During this searched, Officer Ragan found two videos of two topless minors and notified investigators for the Department of Homeland Security. *Id*. A special agent with the Department of Homeland Security decided to have all three phones forensically examined, which revealed more than 100 images and videos of child pornography. *Id*. The Court highlighted that neither the manual searched nor the forensic examinations damaged the phones. *Id*. The Court further highlighted the Supreme Court has consistently held that border searches are not subject to the probable cause and the warrant requirements of the Fourth Amendment. *Id*. at 1312 (citing *United States v. Vega-Barvo*, 729 F.2d 1341, 1344 (11th Cir. 1984)). Instead, border searches are simply subject to the Fourth Amendment's more amorphous reasonableness standard. *Id*. (citing *United States v. Villabona-Garnica*, 63 F.3d 1051, 1057 (11th Cir. 1995)). Vergara was then convicted of possessing child pornography. *Id*. Therefore, because this search occurred at the border and neither the manual or forensic searches of the cell phones required reasonable suspicion or a warrant, Vergara's Fourth Amendment right to privacy was not violates.

Unlike the above cases, in *Riley v. California*, Riley was stopped for a traffic violation, which eventually led to his arrest on weapons charges. 573 U.S. ___ (slip op., at 2477) An officer seized Riley's cell phone and noticed the repeated use of a term associated with a street gang. *Id* at ___ (slip op., at 2477). A detective further examined the phone's contents and charged Riley with a shooting that had occurred earlier. *Id* at ___ (slip op., at 2477). It was then held that the police generally may not, without a warrant, search digital information on a cell phone seized from an individual who has been arrested (noting that cell phones differ in both a quantitative and a qualitative sense from other objects that might be carried on an arrestee's

person). *Id*. at ____ (slip op., at 2477-78). The Court explained that the rationales that support the search-incident-to arrest exception, namely the concerns of "harm to officers and destruction of evidence", did not have much force with respect to digital content on cell phones. *Id*. at ____ (slip op., at 2484). It was further explained that the concerns of the possibility of remote whipping of data when phones "locked" , but those concerns were distinct from arrestees destroying evidence within their reach. *Id*. at ___ (slip op., at 2475) Because Riley was within the United States, was already arrested, and not at an international border, his Fourth Amendment right to privacy was violated.

Here, Escaton's Fourth Amendment rights were not violated because he possesses less of a privacy interest at an international border. He was returning to the United States from Mexico through a West Texas border checkpoint, similar to *Touset*. R. at 2. Customs and Border Protection Officer Ashley Stubbs conducted a routine border search of Escaton's vehicle. *Id*. Through the search, Officer Stubbs found and iPhone, a laptop, three external hard drives, and four USB devices. *Id*. Stubbs noticed a message with multiple money signs. *Id*. Stubbs returned the iPhone back to Escaton, but detained the remaining electronic devices. *Id*. at 3 Stubbs discovered that there were no passwords required and delivered the electronics to ICE. *Id*. at 3. Similar to *Vergara*, both a manual and a forensic search was conducted on his computer, and it was discovered that Escaton's laptop held documents containing individuals' bank account numbers and pins, as well as the USB devices containing traces of malware, which related to an ongoing crime of "ATM skimming"[2]. R. at 3. Similar to *Touset*, Escaton had this criminal

[2] ATM skimming is a criminal activity that costs U.S. banks hundred of millions of dollars annually and affects thousands of bank customers. It can be done by "shoulder surfing" –

activity on his electronic devices, not protected by any right, allowing the government the ability to prevent it from coming into the country. Similar to the disassemble of the gas tank that was entering into the country in *Flores Montano,* the inspection of Escaton's electronic devices pose a parallel situation in which the government is allowed to identify the objects that are coming into the country. The case at hand is unlike *Riley,* in the fact that *Riley* occurred within the United States along with the Court addressing a different question, whether the police may, without a warrant, search digital information on a cell phone seized from an individual that was arrested, rather than the one at hand, whether reasonable suspicion is required for electronic devices at the border for an individual that is not arrested. Since Escaton's search was a routine search at an international border and he was not under arrest, his Fourth Amendment rights were not violated.

B. Petitioner's Fourth Amendment rights were not violated with the search of his electronic devices because there is a significant national security interest.

There is a significant national security interest in using the border to screen for risks to the United States. In order to regulate the collection of duties and to prevent the introduction of illegal aliens and contraband into this country, Congress has granted the authority to conduct routine searches of persons and their personal belongings at the border without reasonable

---

standing behind a customer when they enter their pin, or through "skimmers reading information from debit cards as the enter ATM card readers. Criminals may also infect ATM terminals by uploading malware from USB devices, which collece customer bank numbers and pins. R. at 3.

suspicion, probable cause, or a warrant[3]. Because the Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border, border searches are generally deemed reasonable simply by virtue of the fact that they occur at the border. *Cotterman*, 709 F.3d 952 (9th Cir. 2013) (en banc) (quoting *Ramsey*, 431 U.S. at 616 and *Flores-Montana*, 541 U.S. at 152). Border searches have been reasonable by the single fact that the person or item in question had entered into our country from the outside. *Ramsey*, 431 U.S. 606. The sovereign has an elevated interest in screening for illegal contraband, and the increasing sophistication of technology only heightens the need of the government to search property at the border unencumbered by judicial second-guessing. *Touset*, 890 F.3d at 1235.

The United States' interest in national security at the border is not new. In *Ramsey*, customs officials opened for inspection incoming international letter-class mail without first obtaining a search warrant. 431 U.S. 610; *see also United States v. Seljan*, 547 F.3d 993, 996 (9th Cir. 2008) (holding that an envelope containing personal correspondence is not uniquely protected from a search at the border). Ramsey and Kelly jointly commenced in a heroin-by-mail enterprise in Washington, D.C. which involved the procuring of heroin which was then being

---

[3] *See, e.g.*, 8 U.S.C. § 1357(c) (authorizing immigration officials to search without a warrant persons entering the country for evidence which may lead to the individual's exclusion); 19 U.S.C. § 1496 (authorizing customs officials to search the baggage of person entering the country); 19 U.S.C. § 1582 (authorizing customs officials to detain and search all persons coming into the United States from foreign countries). *See also United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985).

mailed in letters from Bangkok, Thailand and sent to various locations in the District of Columbia area for collection. *See id* at 608. A United States customs officer inspected incoming mail, all which were rather bulky, from Thailand, a known source of narcotics, and suspected that the envelopes might contain contraband. *Id*. at 609. The officer weighed the envelopes, found that they weighed 6 times the normal envelop weight, and opened them finding the contents were identical and all contained heroin. *Id*. Ramsey was indicted on a 17 count indictment. *Id*. at 611. The Fourth Amendment does not denounce all searches or seizures, but only such as are unreasonable (recognizing the distinction between searches within the United States requiring probable cause and border searches, which do not). *Id*. at 1979. It was held that the border-search exception is grounded in the recognized right of the sovereign to control who and what may enter the country (noting there should be no different constitutional standard simply because the envelopes were mailed and not carried). *Id*. at 620. The historically recognized scope of the border-search doctrine suggests no distinction in constitutional doctrine stemming from the mode of transportation across our borders (noting that a port of entry is not a traveler's home and his right to be left alone neither prevents the search of his luggage nor the seizure of unprotected, but illegal, materials discovered during a search). *Id*. at 620-621. The longstanding recognition that searches at our borders without probable cause and without a warrant are nonetheless reasonable has history as old as the Fourth Amendment itself. *Id*. at 619. (citing *United States v. Carroll*, 267 U.S. 132, 149 (1925)). Therefore, because of the national security interest in what is entering into the United States, the Fourth Amendment right of Ramey was not violated.

Allowing digital contraband through the borders could create dangerous situations. Because of the United States' strong interest in national self protection, it was held in *United*

States v. Alfaro-Moncada, 607 F.3d 720 (11th Cir. 2010), routine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant (quoting *Montoya de Hernandez*, 473 U.S. at 538, 105 S.Ct. at 3309; see also *Denson* 574 F. 3d 1318 (11th Cir. 2009) ("Entrants, therefore, are subject to search even in the absence of reasonable suspicion, probable cause, or a warrant")). To hold otherwise would allow digital contraband to pass no matter how potentially dangerous, while physical property still remains subject to penetrating searches. *Id*. at 728. Here, a foreign cargo ship docked at the Antillean Marine inside Miami, Florida after traveling from the Dominican Republic. *Id*. at 723. The United States Customs and Border Protection went on board to inspect the ship for prohibited agricultural materials. *Id*. The specialist went below the ship to inspect the crew members quarters and searched particularly Alfaro-Moncada's desk which contained DVD covers that contained images of young girls engaging in a variety of sex acts. *Id*. at 725. Alfaro-Moncada was indicted with possession of child pornography. *Id*. Suspicionless searches of a cargo ship cabin described at the defendant's home on vessels entering into the United States are reasonable simply by virtue of them happening at the border. *Id*. at 728. The United States' paramount interest in conducting searches at its borders it in itself national self-protection. *See Flores-Montano*, 541 U.S. at 153, 124 S.Ct. at 1585 ("It is axiomatic that the United States, as sovereign, has the inherent authority to protect, and a paramount interest in protecting its territorial integrity). It was further highlighted that to determine the reasonableness of a border search, the intrusion on an individual's Fourth Amendment interests is weighed against its promotion of legitimate governmental interests. *Id*. at 727. Therefore, defendant's Fourth Amendment rights were not violated due to the national security interest with the ship coming back from international seas along with the governmental interest weighing higher than the

intrusion on an individual's Fourth Amendment, the defendant's Fourth Amendment right was not violated.

Unlike the above cases, in *United States v. Cotterman*, it was held that reasonable suspicion is required for the search of electronic devices (noting that although border searches are generally deemed "reasonable" by virtue of the fact that they occurred at the border, this does not mean that at the border "anything goes"). 709 F.3d 952. The Ninth Circuit reasoned that because of the "ubiquity of cloud computing" and that cloud data "may appear as a seamless part of the digital device when presented as the border", border agents will be able to access that information without reasonable suspicion as well. *Id*. at 965. It was further held that the forensic examination of the defendant's computer that analyzed his hard drive required the showing of reasonable suspicion. *Id*. at 952. Here, Cotterman and his wife were driving home to the United States from Mexico when they reached a port of entry. *Id*. at 957. During the primary investigation, it was discovered that Cotterman was a registered sex offender which resulted in him and his wife being instructed to exit their vehicle and leave all their belongings in the car. *Id*. The agents searched the vehicle and retrieved two laptop computers and three digital cameras. *Id*. The agents seized Cotterman's laptop in response to an alert based on a fifteen-year-old conviction for child molestation. *Id*. at 956. The officer inspected the electronic devices and found family photographs along with other password protected files. *Id*. at 958. The laptop was shipped 170 miles away and subjected to a comprehensive forensic examination. *Id*. at 956. The agent used a software on Cotterman's computer to examine copies of the laptop hard drives which displayed seventy five images of child pornography. *Id* at 958. The Court viewed computer forensic examinations as a powerful tool that is capable of unlocking password protected files, restoring deleted material, and retrieving images viewed on web sites. *Id*. at 957.

Cotterman was indicted for a host of offenses related to the child pornography. *Id*. at 959. Due to the vast array of information that an electronic device can hold, the Ninth Circuit held that the Fourth Amendment right of Cotterman was violated during the search of his electronic devices.

In the case at hand, upon finding the electronic devices, Stubbs was sure to place the iPhone on airplane mode, ensured the laptop was disconnected from wireless service, and manually searched the devices without assistive technology. This is unlike *Cotterman* because the agents were careful to disconnect Escaton's iPhone and laptop from cell and internet service prior to conducting the searches. R. at 9. This disconnects the electronic device from the iCloud and what information the agents are capable of retrieving. There were also no passwords needed to open the devices. R. at 3. The information that Escaton was carrying is unable to be seen by the physical eye due to the fact that it is electronic information, which deserves the same holding as in *Alfaro-Moncada* because in this case, if electronic information was able to be passed through the borders, this could be a very dangerous situation for the country from situations such as child pornography to terrorism. Therefore, because the electronic information stored in Escaton's computer is unable to be detected to the naked eye, along with a high national security interest, his Fourth Amendment rights were not violated.

II. The government's request for historical cell-site location information is not a violation of Petitioner's Fourth Amendment rights and comports with the Court's decision in *Carpenter*.

Pursuant to the Stored Communications Act 18 U.S.C. § 2703(d) the government obtained access to Petitioner's cell-site data through a court order. The Court held in *Carpenter v. United States*, 138 S. Ct. 2206 (2018) that the retrieval of this information by law enforcement is not a search if what is gathered amounts to fewer than seven days of historical data or does not contain information that would provide intimate details of a person's movements. This means the

government's collection of three-day records, weekday collection of cell-site information, and request for a tower dump was not a search and thus not a Fourth Amendment violation.

The narrow holding in *Carpenter* affirms that the government's action in gathering a three-day record and the weekday CSLI was congruent with the Fourth Amendment because less than seven days of data was collected. *Carpenter*, 138 S. Ct. at 2220 (2018). The Court did not declare 18 U.S.C. § 2703(d) of the Stored Communications Act unconstitutional, but instead placed limits upon the government's abilities under it. That limit is seven days of data. *Carpenter*, 138 S. Ct. at 2220. While a person does have an expectation to privacy as it relates to a record of his physical location and movements, that expectation is not limitless. *Id.* at 2215, 2220. The Court took time to clarify that historical cell-site location information is not subject to the third-party doctrine, but also acknowledged that its opinion did not apply to or preclude law enforcement from obtaining information from tower dumps. *Id.*

A. Government collection of three-day records and historical cell-site location information that amounts to fewer than seven total days of information on Petitioner does not violate the Fourth Amendment.

Acquisition of seven days of historical CSLI is an unreasonable search under the Fourth Amendment. *Carpenter,* at 2220-2221. This leaves the three-day record of Petitioner's data both within the scope of the SCA and makes it reasonable under the Fourth Amendment. In determining the reasonability of a search, the Court pointed to two guiding principles: first that the Fourth Amendment ought to protect against the use of arbitrary power to intrude upon the "privacies of life," and second that the Fourth Amendment ought to serve as an obstacle to omnipresent police surveillance. *Id*. Three days of information falls well short of these two concerns in *Carpenter.*

In *Carpenter*, police officers arrested four men who were suspected of executing a series of robberies of Radio Shacks and T-Mobile stores in Detroit. *Carpenter,* at 2212. During interrogations officers learned that the men robbed a total of nine stores in Michigan and Ohio. *Id.* Once a list of accomplices had been identified, prosecutors obtained court orders under the SCA to obtain cell phone records for several suspects, including Timothy Carpenter. *Id.* The order allowed law enforcement to obtain fourth months of CSLI, and Metro PCS provided records spanning 127 days. *Id.* Two days of records were collected from Sprint, which cover the period when Carpenter's phone was roaming in Ohio, pursuant to a court order for seven days of records. *Id.* The Court expressed concern for law enforcement being able to obtain five years of historical CSLI – the amount of time for which cell service providers maintain records – without a warrant. *Id.* at 2218. Emphasizing that point throughout the opinion, the Court held that for the specific set of facts in the case using a court order to obtain seven days or more of CSLI is an unconstitutional search and a warrant is required. *Id*. at 2223.

An officer cannot gain meaningful insight into the intimacies of a person's life from three days of information. Three days of information is only useful when the requestor knows which three days to look for. In Petitioner's case, the government had reliable and articulable facts that allowed them to gain a court order for records for very specific days. Those days were the ones that fell between the day of the last ATM maintenance at Mariposa Bank and the day the customer noted an oddity at the ATM. R. at 13. While the Court has held that a person maintains a legitimate interest in his movements, even when they are public, that privacy interest is not without limit. *See generally, United States v. Jones,* 565 U.S. 400 (2012) (determining that the placement of a GPS tracker on a car after the warrant expired was an unreasonable search); *United States v. Knotts*, 460 U.S. 276 (1983) (ruling that placement of a beeper in a container for

the purpose of using that beeper's signal to track the container to its destination was not an unreasonable search).

A factor in determining whether law enforcement has unreasonably uncovered the intimacies of someone's life in violation of the Fourth Amendment is whether that person sought to preserve that activity as private. *Carpenter,* at 2213. In *Carpenter* the Court did not need to address whether Carpenter intended to keep his movements private; the incredible amount of information that law enforcement was able to acquire is a clear intrusion of Carpenter's privacy interests. *Id.* Yet, when the amount of information collected is under the threshold established in *Carpenter,* the Court should look to the manifestation of an expectation of privacy. *See, e.g.*, *California v. Ciraolo,* 476 U.S. 207, 211 (1986); *Katz v. United States,* 389 U.S. 347, 360 (1967) (Harlan, J. concurring). Here, three-day records fall within the seven-day threshold and Petitioner has done nothing to manifest his interest in keeping his CSLI private. An individual who does not want their phone to automatically and constantly ping cell towers has the option to place his phone in "airplane mode" or to turn off data entirely. To assuage concerns about being able to gain emergency assistance if necessary, service providers have made it possible to place 911 calls while phones are in these states of operation. Petitioner could have hidden his location, but he did not.

Because three days of information cannot give an officer insight into the intimate details of a person's life, it cannot be determined to be establishing a surveillance state. The SCA combined with the limitation established in *Carpenter* provide a significant obstacle to omnipresent police surveillance. Depending on which three days are collected, law enforcement may not be able to see where a person works or prays, and certainly would not be able to

determine what establishments that person frequents. A random selection of three days of historical CSLI without context would not give law enforcement any actionable information.

B. Government collection of 100 hours of historical cell-site location information does not violate the Fourth Amendment.

Just as a three-day record does not violate the rule established in *Carpenter,* the collection of 100 hours of weekday CSLI does not. 100 hours amounts to fewer than five days, still falling short of the seven-day requirement set by *Carpenter*. In addition, the government did not request 100 consecutive hours, but instead asked for Petitioner's CSLI records during regular working hours. Without information on what Petitioner does "after hours" the Court does not need to worry about the government intruding upon Petitioner's private life, or about the government attempting to maintain an unreasonable surveillance state. *See, United States v. Knotts*, 460 U.S. 276, 284 (1983) (ruling that a person has no Fourth Amendment privacy interest in information that could be discovered from a public thoroughfare).

The Court in *Carpenter,* takes care to note that the protection of the Fourth Amendment should extend to "a detailed log of a person's movements over several years." *Carpenter,* 138 S. Ct. at 2222. In this case, we are looking at less than five days of information collected only during regular working hours. This is hardly a detailed log of Petitioner's life. It is only a detailed log of Petitioner's crimes. The Court went on to say that, under the decision in *Carpenter,* the government "will be able to use subpoenas to acquire records in the overwhelming majority of investigations." *Id.* This is one of those investigations. This Court has held that a person does not have a reasonable expectation of privacy in anything that an officer could observe from a public thoroughfare. *Ciraolo,* 467 U.S. at 213. In *Ciraolo,* law enforcement received an anonymous tip that marijuana was growing in respondent's backyard. *Id.* at 209. While police could not see the marijuana from the ground level because of a series of fences, the

highest being 10 feet tall, enclosed the yard, they flew over the property and identified marijuana plants. *Id.* The Court ruled that this was not a search in violation of the Fourth Amendment because the police do not need a warrant for what is visible to the naked eye. *Id.* at 215.

Instead of obtaining Petitioner's historical CSLI, law enforcement could have tailed him during working hours. They would have been able to go home every night, see their families, get a full night of rest, and then wake up the next day to continue surveillance. And that visual surveillance would provide them with far more detail that the CSLI information in this case, which was accurate only within 1,000 feet of Petitioner due to the scarcity of cell towers in the area. R. at 23. Like in *Ciraolo,* law enforcement had access to all of Petitioner's collected movements from a public thoroughfare. If an anonymous tip is enough to allow the government to overcome a 10-foot fence within the curtilage of a man's home, then specific and articulable facts establishing the justification for a court order are enough for the government to acquire historical CSLI in this case.

The Court in *Carpenter* also states that the government's position does not contend with the shifts in digital technology that make the tracking of a person's movements through CSLI possible. *Carpenter*, 138 S. Ct. at 2219. But these shifts in technology are exactly what enabled Petitioner to commit his crimes. As technology becomes more advanced law enforcement struggles to keep up. *See, e.g.*, Marc Goodman, "Crime has Gone High-Tech, and The Law Can't Keep Up," *Wired* (March 21, 2015) (found at: https://www.wired.com/2015/03/geeks-guide-marc-goodman/). To deny law enforcement reasonable access to technology and digital information is to ignore the realities of the digital age.

Collection of 100 hours of CSLI during specified hours does not violate the rule established in *Carpenter* because it does not provide a complete picture of Petitioner's personal

life. *Carpenter,* 138 S. Ct. 2206. As established in *Knotts,* there is no privacy interest in information that can be discovered from public thoroughfares, and the information collected here was nothing more than Petitioner's public movements. *Knotts,* 460 U.S. 276, 284.

C. Government collection of CSLI records from tower dumps do not provide insight into the intimate details of a person's movements and thus do not violate the Fourth Amendment.

A tower dump provides "a download of information on all the devices that connected to a particular cell site during a particular interval." R. at 13. *Carpenter* does not apply to the government's request for CSLI records from a tower dump as it does not provide a diary of Petitioner's movements. No detailed information is revealed by the government asking which devices connected to which tower on a given day. The information collected is the same is what a security camera collects, and there are not significant Fourth Amendment concerns with the lawful placement of routine security cameras. *See, e.g., Carpenter,* 138 S. Ct. at 2220-21.

Instead the Court should apply the standards established in *Smith v. Maryland* and *United States v. Miller,* two of the cases that established the third-party doctrine. *Smith v. Maryland*, 442 U.S. 735, 743 (1979); *United States v. Miller*, 425 U.S. 435, 443 (1976). In *Smith,* a woman was robbed and being harassed by the perpetrator of the crime, Petitioner in the case. *Id.* at 737. After the police discovered the name of the Petitioner, they asked that the phone company install a pen register at its central office and record the numbers dialed from the phone in Petitioner's home. *Id.* The register revealed that the Petitioner had called the woman, so he was arrested and charged. *Id.* Petitioner sought to suppress "all fruits derived from the pen register" because the police did not obtain a warrant for its installation. *Id.* However, the pen register tape and the evidence stemming from it were admitted at trial and Petitioner was convicted. *Id.* at 738. This Court determined that a warrant was not necessary for the police to order the installation of the

pen register because Petitioner did not have a reasonable expectation of privacy to the numbers he dialed on his phone. *Id.* at 742.

In *Miller*, police received a tip that lead them to stop a truck occupied by two of respondent's co-conspirators. *Miller,* 425 U.S. at 437. The truck contained materials used for distilling whiskey. *Id.* The following month a warehouse rented to respondent caught fire, and in the course of addressing the blaze law enforcement discovered a distillery, nontax-paid whiskey, and related paraphernalia. *Id.* Two weeks later agents from the Alcohol, Tobacco and Firearms Bureau presented subpoenas to the bank where respondent maintained accounts and obtained several records related to his accounts. *Id.* at 437-438. Respondent in *Miller* was convicted of possessing an unregistered still and with carrying on the business of a distillery with intent to defraud the Government of whiskey tax in the District Court, after his motion to suppress was overruled. *Id.* at 436. This Court found that there had not been an intrusion into an area in which respondent had a protected Fourth Amendment interest because the documents collected were not his private papers. *Id.* at 440.

In this case, the tower dump is more similar to the collection of information in both *Smith* and *Miller* because it does not contain any personal information and is simply a business record. R. at 14. While pen registers may still have their use, a tower dump today is its modern equivalent. In 1979 the Court found in *Smith* that there was no privacy interest in the numbers a person dials from his or her phone, given its limited capabilities. *Smith*¸ 442 U.S. 735, 742. A tower dump is equally limited in its capabilities. It shows only what phone numbers have connected to a given tower during a specific period. If it is not a search to discover which numbers are dialed, it stands to reason that it is not a search to find out how the call was connected.

Bank records are significantly more private than a phone number, and this Court has ruled that an individual does not have a reasonable expectation of privacy for those records. *Miller*, 425 U.S. 435, 442. Here, all the tower dumps produced were lists of phone numbers that used the towers, regardless of service provider. R. at 4. Record of the interaction is more similar to exchange of information at a bank, as in *Miller*, than it is something that the Petitioner would have an expectation of privacy in. *Miller*, 425 U.S. 435.

The Court should apply the third-party doctrine as established in *Smith* and *Miller* to the tower dumps in this case because the records recovered were related to business and Petitioner did not have an expectation of privacy in them. *Smith v. Maryland*, 442 U.S. 735, 743 (1979); *United States v. Miller*, 425 U.S. 435, 443 (1976). *Carpenter* does not apply because no detailed information is revealed from a tower dump.

CONCLUSION

For the aforementioned reasons, Escaton respectfully requests this Court AFFIRM the judgment of the Fourteenth Circuit and apply the decision of the District Court.

Dated: February 10, 2019

Respectfully Submitted,

Attorneys for
Respondent