No. 10-1011

In the Supreme Court of the United States

HECTOR ESCATON,
PETITIONER

v.

UNITED STATES OF AMERICA,
RESPONDENT

ON WRIT OF CERTIORARI
TO THE SUPREME COURT OF THE UNITED STATES

BRIEF FOR THE RESPONDENT

Team Number P13

Attorneys for Respondent,
UNITED STATES OF AMERICA

TABLE OF CONTENTS

TABLE OF CONTENTS (CONT.)

TABLE OF AUTHORITIES

Page(s)

CASES

Supreme Court of the United States

TABLE OF AUTHORITIES (CONT.)

TABLE OF AUTHORITIES (CONT.)

QUESTIONS PRESENTED

I. Does the Fourth Amendment require that government officers have reasonable suspicion before conducting forensic searches of electronic devices at an international border?

II. In light of this Court's limitation on the use of cell-site location information in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), were the Government's acquisitions pursuant to 18 U.S.C. § 2703(d) of three days of cell-site location information, 100 cumulative hours of cell-site location information over two weeks, and cell-site location information collected from cell tower dumps a violation of the Fourth Amendment?

No. 10-1011

IN THE
SUPREME COURT OF THE UNITED STATES

HECTOR ESTACON,
PETITIONER,

v.

UNITED STATES OF AMERICA,
RESPONDENT

ON WRIT OF CERTIORARI
TO THE SUPREME COURT OF THE UNITED STATES

BRIEF FOR THE RESPONDENT

OPINION BELOW

The opinion of the United States Court of Appeals for the Fourteenth Circuit is reported at *Escaton v. United States*, 1001 F.3d 1341 (14th Cir. 2021).

CONSTITUTIONAL PROVISIONS AND RULES

The Fourth Amendment of the United States Constitution

The right of the people to be secure in their person, 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.

18 U.S.C. § 2703

The Stored Communications Act

. . .

(d) **Requirements for court order.** A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental

authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

INTRODUCTION

Summary of Argument

The Fourth Amendment does not require reasonable suspicion to conduct a forensic search on electronic devices at the border. There has never been a reasonable suspicion requirement for searches of property at the border. Furthermore, even if there was a routineness requirement for the border exception, the forensic search in the case at bar was routine. In addition, consistent with this Court's recent decision in *Carpenter*, the telecommunications records requested by the Government did not violate Petitioner's Fourth Amendment rights. This Court's recent decision in *Carpenter* highlighted several policy concerns in holding that government officers must obtain a warrant before requesting seven days of continuous historical cell-site location information. However, these policy reasons or factual underpinnings are not present in the case at bar, so *Carpenter* should not be extended. Therefore, this Court should affirm the United States Court of Appeals for the Fourteenth Circuit.

STATEMENT OF THE CASE

Statement of Facts

During October 2018, the Federal Bureau of Investigations ("FBI") began to investigate a series of ATM skimmings at the Mariposa Banks in the towns of Sweetwater and Escalante, West Texas, resulting in $50,000 of losses to the bank and hundreds of stolen identities of customers. (R. 3, 4). Five ATMs in Sweetwater, and three in nearby Escalante, were infected. (R. 3). Two of the Sweetwater ATMs had skimming devices overlaying the card readers, and the remaining three had been infected by plugging in a USB device. (R. 5). One of these three ATMs was even infected with sophisticated malware. (R. 4). The FBI used several investigative tools to probe into these crimes; one of the tools used was a "tower dump." (R. 4). A tower dump is a chronological list of every phone number that connected to a particular cell tower

during a short period of time, regardless of cellular service provider. (R. 4 n.3). When a cell phone makes this connection – often several times a minute – cell towers record a list of all cell phone numbers. (R. 4 n.4). Sweetwater is densely populated and contains many cell towers, which provides investigators with a large amount of data. (R. 22). Escalante is a smaller town with less cell towers, and therefore the accuracy of the data is less than that of Sweetwater, but still provides useful information for government officers. (R. 23). Both the Sweetwater and Escalante towers record information in five-to-ten minute increments. (R. 22, 23). Another investigative tool used by government officers is historical cell-site location information ("CSLI"). (R. 2). Cell phones operate by searching for and connecting to the nearest set of fixed radio antennas called cell-sites in order to obtain the best signal available. (R. 4 n.4). Each time a cell phone connects to a cell-site, it generates a time-stamped record known as CSLI. (R. 4 n.4).

Approximately one year later, on September 25, 2019, Hector Escaton ("Escaton") had his car searched by Customs and Border Protection ("CBP") Agent Ashley Stubbs ("Stubbs") at a border checkpoint between the United States and Mexico. (R. 2). Stubbs found an iPhone, a laptop, three external hard drives, and four USB drives. (R. 2). After a manual search of the devices, Stubbs discovered a piece of paper hidden beneath the laptop keyboard that read, "Call Delores (201) 181-0981 $$$." (R. 2). Delores had been previously convicted for ATM skimming. (R. 5). After turning off the network connectivity of all devices and returning the iPhone to Escaton, Stubbs attempted to access the contents of the laptop, hard drives, and USB drives, but some of the files were encrypted. (R. 2, 3). Stubbs then delivered the remaining electronics to Immigration and Customs Enforcement ("ICE") Senior Special Agent and Computer Forensic Examiner Theresa Cullen ("Cullen"). (R. 3). Cullen then used forensic software to search the encrypted files. (R. 3). Cullen uncovered that one of the encrypted files

held documents containing individuals' bank account information and pin numbers. (R. 3). Further examination uncovered malware on the USB devices. (R. 3).

CBP then notified the FBI, and the case was assigned to Special Agent Catherine Hale ("Hale"). (R. 3). Hale began examining the forensic evidence uncovered from Escaton's devices in connection with the ongoing ATM skimming investigations in Sweetwater and Escalante. (R. 3). The malware found on the USB devices was similar to the sophisticated malware discovered by Mariposa Bank. (R. 4, 5). Using the forensic search information, surveillance photographs of the ATMs, and additional information provided by the bank, Hale and U.S. Attorney Elsie Hughes ("Hughes") requested three tower dumps pursuant to 18 U.S.C. § 2703(d). (R. 4). These tower dumps were taken from cell towers near three of the ATMs for the thirty-minute periods before and after the surveillance photos showed ATM tampering. (R. 4). 18 U.S.C. § 2703(d), also known as the Stored Communications Act ("SCA"), authorizes government officers to compel cellular service providers to disclose certain telecommunications data only if the Government can "offer specific and articulatable facts showing there are reasonable grounds to believe that the records sought are relevant and material to an ongoing investigation." 18 U.S.C. § 2703(d). Escaton's phone number was found to be near three of the five Sweetwater ATMs during this one-hour period. (R. 5).

Hale and Hughes then applied for, and received, a court order from a federal magistrate judge for Escaton's telecommunications records. (R. 20-25). These records compelled Escaton's cellular service provider to disclose CSLI corresponding to his cell phone number from October 11, 2018 through October 13, 2018 ("Three-day Records"). (R. 5). The Three-day Records showed Escaton's phone was near the fourth Sweetwater ATM around the time of the tampering. (R. 5). An additional order, pursuant to the SCA, requested Escaton's CSLI during the working hours of 8AM and 6PM between October 1, 2018 through October 12, 2018. (R. 5).

This data revealed that Delores and Escaton were near each other around the time of the tamperings. (R. 5). A warrant to search Delores's home was subsequently issued and executed; the search uncovered cash and copies of the malware found on Escaton's devices. (R. 5).

Procedural History

Petitioner was indicted 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, in the District of West Texas. (R. 6). Petitioner filed a motion to suppress the results of the forensic search of his devices and telecommunications records. (R. 6). The district court denied the motion, and Petitioner was subsequently convicted on all charges following a jury trial. (R. 6).

Petitioner appealed to the United States Court of Appeals for the Fourteenth Circuit ("Fourteenth Circuit") regarding the denial of his motion to suppress. (R. 6). The Fourteenth Circuit affirmed the district court's ruling. (R. 6). The court determined that there was no reasonable suspicion required to conduct a forensic search of electronic devices at the border, and the telecommunications records requested did not violate the Supreme Court of the United States' holding in *Carpenter*. (R. 13). Petitioner now appeals to the Supreme Court of the United States.

ARGUMENT

I. THE FOURTH AMENDMENT DOES NOT REQUIRE THAT GOVERNMENT OFFICERS MUST HAVE REASONABLE SUSPICION BEFORE CONDUCTING FORENSIC SEARCHES OF ELECTRONIC DEVICES AT INTERNATIONAL BORDERS.

The Fourth Amendment provides that "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." U.S. Const. amend. IV. This Court has stated that the "permissibility of a particular law enforcement practice is judged by 'balancing its intrusion of the individual's Fourth Amendment interests against its promotion of legitimate governmental interests.'" *United States*

v. Montoya de Hernandez, 473 U.S. 531, 537 (1985) (quoting *United States v. Villamonte-Marquez*, 462 U.S. 579, 588 (1983)). This Court has further provided that the "reasonableness" requirement of the Fourth Amendment generally requires a warrant; however, a search is reasonable if it falls within a specific exception to the warrant requirement. *Riley v. California*, 134 S. Ct. 2473, 2482 (2014). One of these exceptions is the border exception, where the "Fourth Amendment's balance of reasonableness is qualitatively different at the international border than in the interior." *Montoya de Hernandez*, 473 U.S. at 538. This Court has never found that reasonable suspicion is required for nondestructive property searches at the border. *See United States v. Flores-Montano*, 541 U.S. 149, 152 (2004).

The Government does not contest that the actions taken by Stubbs, Cullen, Hale, and the FBI fall within Fourth Amendment analysis. The case at bar is in regard to property: that of a laptop, USB drives, external hard drives, and an iPhone. (R. 2). The Government concedes that the act of a forensic examination of files constitutes a search within the meaning of the Fourth Amendment. Furthermore, no warrant was sought to conduct the forensic search because the search occurred at an area covered by the border exception – a checkpoint at the border itself. (R. 2, 3). However, the search was reasonable within the scope of the Fourth Amendment. The Government exercised its legitimate and plenary powers as sovereign by checking for unwanted contraband entering the country by performing a forensic search on the electronic devices. (R. 3). Because this Court has never required reasonable suspicion for searches such as the one in the case at bar, this Court should affirm the Fourteenth Circuit's decision below and hold that reasonable suspicion is not required for nondestructive searches of property at the border.

A. The Government's Interest Is So Great That It Does Not Require Probable Cause to Perform a Forensic Search on an Individual's Laptop Because There Is No Requirement for Routineness for the Search of Property at the Border.

The permissibility of a particular government officer's practice is judged by balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests. *Montoya de Hernandez*, 473 U.S. at 537. First, the Government has an expansive and long-founded interest in border security. Second, Petitioner has an individual interest in the files contained within his electronic devices. After balancing the two interests, the Government's interest is so much greater that it is not required to have reasonable suspicion for nondestructive property searches performed at the border.

1. Since the founding of the nation, the Government's interest in border security has been well-recognized.

"The Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border." *Flores-Montano*, 541 U.S. at 152. Time and time again, this Court has stated that searches made at the border, pursuant to the longstanding right of the sovereign to protect itself, are reasonable simply by virtue of the fact that the searches occur at the border. *Id*. at 152-53. The Government's interest is "at its zenith at the international border" because there is a substantial interest in preventing unwanted persons and effects from entering or leaving the country. *Id*. at 152. In effect, there is no other time where the Government's Fourth Amendment interest is higher.

In *United States v. Flores-Montano*, this Court outlined the Government's interest in performing extensive searches of property at the border, and ruled that the nondestructive but complete disassembly and reassembly of an automobile's gas tank did not require any level of suspicion. *Id*. at 153, 155-56. Since the First Congress, American jurisprudence has recognized the sovereign's inherent and paramount interest in protecting its territorial integrity. *Id*. at 153. Furthermore, this Court articulated the importance of protecting the border due to the attempted

smuggling. *Flores-Montano*, 541 U.S. at 153. At the time this case was decided, approximately one quarter of all drug seizures came from searching gas compartments at the border. *Id*.

Similarly, electronic devices are capable of bringing in massive amounts of contraband and illegal materials. *Riley*, 134 S. Ct. at 2484. The oldest still-supported iPhone can contain a minimum of hundreds of thousands of text files and thousands of photographs, in addition to other software and stored information. *See generally* Orin S. Kerr, *Foreword: Accounting for Technological Change*, 36 Harv. J.L. & Pub. Pol'y 403, 404 (2013). Petitioner was able to cross the border with a USB drive – an object smaller than a deck of cards – containing multiple files of contraband. (R. 2-3, 5). Electronic devices are the only place where this digital contraband can be found. Whereas in *Flores-Montano*, approximately one quarter of drug seizures came from searching automobile gas tanks, searching external hard drives has uncovered contraband or illegal materials the Government does not want entering the country. 541 U.S. at 153; (R. 2). Because the Government's interest in protecting itself at the border is at its zenith, this Court should affirm the lower court's decision and rule that forensic searches of electronic devices at the border do not require any reasonable suspicion.

2. Petitioner has a privacy interest from a forensic search of his computer and files contained within.

In order to determine if an individual has a privacy interest meriting Fourth Amendment protection, this Court has provided that the individual must have exhibited an actual, subjective expectation of privacy which "is one that society is prepared to recognize as reasonable." *Katz v. United States*, 389 U.S. 347, 361 (1967). There is a reasonable expectation of privacy in one's cell phone. *Riley*, 134 S. Ct. at 2484. In *Riley v. California*, this Court reasoned that because modern cell phones are such a pervasive and insistent part of daily life, a proverbial visitor from Mars could conclude they were an important feature of human anatomy. *Id*. This Court went on to discuss whether or not society should recognize cell phones as having a privacy interest that

society is prepared to recognize. *Riley*, 134 S. Ct. at 2484. Its reasoning included that a cell phone collects many distinct types of information in one place, that, in combination, allows for the sum of an individual's private life to be reconstructed through a thousand photographs. *Id*. at 2489. This Court therefore reasoned that there was no practical ability of a person to choose what to include on their person. *Id*. at 2490.

3. Balancing the interests of the Government with the interests of an individual crossing the border, reasonable suspicion is not required for a nondestructive search of property.

In *United States v. Ramsey*, this Court provided that border searches "have been considered to be 'reasonable' by the single fact that the person or item in question entered into our country from outside. There has never been any additional requirement that the reasonableness of a border search depended on the existence of probable cause." 431 U.S. 606, 619 (1977). In addition, in *Flores-Montano,* this Court looked to see if suspicionless border searches of a vehicle were constitutional. 541 U.S. at 155. In both cases, this Court held that the searches were constitutional because the Government interest is so great at the border. *Id*.; *see also Ramsey*, 431 U.S. at 623. This Court reasoned that although it may be true that some searches of property are "so destructive" as to require a level of suspicion at the border, these did not. *Flores-Montano*, 541 U.S. at 155-56.

The most poignant reasoning by this Court in *Flores-Montano* was their derision of the Ninth Circuit's reasoning below. *Id*. at 151.

> [The Ninth Circuit] seized on the language from. . . *United States v. Montoya de Hernandez*. . . in which [this Court] used the word 'routine' as a descriptive term in discussing border searches. . . The [Ninth Circuit] took the term 'routine,' fashioned a new balancing test, and extended it to searches of vehicles. But the reasons that might support a requirement of some level of suspicion in the case of highly intrusive searches of the person--dignity and privacy interests of the person being searched--simply do not carry over to vehicles. Complex balancing tests to determine what is a 'routine' search of a vehicle, as opposed to a more 'intrusive' search of a

> person, have no place in border searches of vehicles. *Flores-Montano*, 541 U.S. at 152.

The instant case included no destruction to property and was not highly intrusive to the person. There is no question what was searched was property: a laptop, iPhone, USB drives, and external drives. (R. 2). Even though some of the files were encrypted, Cullen was able to discover the files containing bank account information, pin numbers, and ATM malware without damaging the devices. (R. 2, 3). Therefore, the search was not only not "so destructive" of the property, it was not destructive at all.

In addition to its nondestructive nature, the search in the case at bar was not highly intrusive as to require any level of suspicion at the border. Government officers were searching for contraband by searching property, not a person. (R. 2). Therefore, the fact that property was being searched and not a person means that a complex balancing test is an inappropriate extension of the current understanding of the border exception to the Fourth Amendment. Furthermore, CBP and the FBI uncovered contraband and clear evidence of a crime; the agents did not go on a fishing expedition by reading every file and looking through each picture. (R. 4). Instead, the forensic software they used highlighted specific documents and malware. (R. 4). Because the software was not a dragnet or manual inspection of each and every file and the search was limited to uncovering contraband, it cannot be said to be so highly intrusive. Therefore, in conjunction with the nondestructive nature of the forensic search, the dignity and privacy interests of the individual are paled in comparison to the Government's interest in preventing contraband from entering the country. Because the Government's interest is so great, this Court should affirm the lower court and hold that there is no reasonable suspicion required for nondestructive searches of property at the border.

B. Even if "Routineness" Is Required for a Forensic Search of a Laptop, the Search in the Case at Bar Was Routine and Therefore Did Not Require Probable Cause.

This Court has, beyond general guidance, not determined precisely what makes a search nonroutine. *United States v. Kolsuz*, 890 F.3d 133, 144 (4th Cir. 2018). This Court has held that the highly-intrusive x-ray and anal cavity searches are considered nonroutine, but the complete disassembly and reassembly of a vehicle gas tank was considered routine. *See Montoya de Hernandez*, 473 U.S. at 532-36; *see also Flores-Montano*, 541 U.S. at 155. The Circuit Courts, specifically the Fourth, Ninth, and Eleventh, have split over whether a forensic search of an electronic device is routine.

1. A forensic search of a laptop is routine as long as there is no connection to cloud or other over-the-air capabilities.

The Circuit Courts' split on the issue of forensic searches of electronic devices at the border can illuminate the proper determination for when a search is or is not routine. A search of a laptop should be considered routine as long as the Government does not access cloud data or other over-the-air capabilities, and is otherwise nondestructive. This rule would strike the proper balance between the various Circuits.

The Ninth Circuit included language in its decision in *United States v. Cotterman* that the ubiquity of cloud computing complicates the issue; the devices act as a conduit to retrieving information from the cloud in an often-seamless manner. 709 F.3d 952, 965 (9th Cir. 2013). By limiting the Government's searches to local files on a computer or hard drive, the Government is prevented from having a traveler's entire life history just a click away. *Id*.

The Fourth Circuit expressed similar concerns. For example, in *United States v. Kolsuz*, it determined that the use of software to search an iPhone's data was a nonroutine search. 890 F.3d at 152. The Fourth Circuit reasoned that it is "difficult to conceive of a property search more invasive or intrusive" because the digital search of a cell phone is essentially "a body

cavity search" of the cell phone. *Kolsuz*, 890 F.3d at 140 (citing *United States v. Saboonchi*, 990 F. Supp. 2d 536, 569 (D. Md. 2014)) (internal quotations omitted). A phone contains many sensitive records, even more than that of the constitutionally protected home. *Id*. at 145.

2. The Fourth Circuit's reasoning that a forensic search of an iPhone as nonroutine is incorrect because it erred by applying *Riley*.

The Fourth Circuit has held that a forensic search of an iPhone is nonroutine. *Id*. at 144. The Fourth Circuit reasoned that this Court's decision in *Riley* appears to indicate that cell phones deserve the highest level of Fourth Amendment protection. *See generally id*. at 144-47. However, *Riley* is not applicable to the case at bar; that case determined if a forensic search of a cell phone needed reasonable suspicion for a *search incident to arrest*, not a border search. *Riley*, 134 S. Ct. at 2482. With a different history in American jurisprudence, the search incident to arrest doctrine is primarily aimed at discovering evidence on the arrestee's person, preventing the evidence's destruction, and disarming the arrestee. *See generally id*. at 2482-84. A border search, on the other hand, is based on the Government's interest in preventing the unwanted entry of persons and effects, and "is axiomatic that the United States, as sovereign, has the inherent authority to protect, and a paramount interest in protecting, its territorial integrity." *Flores-Montano*, 541 U.S. at 153.

Furthermore, even if *Riley* did indicate that a forensic search of a cell phone was nonroutine because of the privacy and dignity interests involved, those same interests do not apply to a laptop. *Riley*, 134 S. Ct. at 2484. In *Riley*, this Court reasoned that modern cell phones are "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude that they were an important feature of human anatomy." *Id*. This Court further went on to enumerate several factors that indicated whether or not society should recognize cell phones as having a privacy interest that society is prepared to recognize. *Id*.

However, laptops and external memory devices are very different in many ways despite the seeming similarities. While a laptop *can* have the same amount and type of information on it, it frequently does not. Cell phones are a uniquely singular technological device in modern society. First, cell phones include all forms of communication, from text messages to email, in addition to countless social media software. Kerr, *Foreword*, *supra*, at 405. Second, cell phones often contain or have access to every picture taken by its owner, especially since the recent introduction of cloud technology. *Id*. Finally, cell phones are always with their owner, regardless of the owner's physical location. *Id*.

Laptops, on the other hand, do not typically have the same communication abilities as cell phones, besides email and website-based software abilities. *Id*. Additionally, laptops require manual effort to load and store pictures on the device, whereas cell phones do not. Orin S. Kerr, *Essay: Digital Evidence and the New Criminal Procedure*, 105 Colum. L. Rev. 279, 284-85 (2005). Finally, laptops are much larger than cell phones and require the owner to make a conscious decision to keep the device on their physical person. Kerr, *Foreword*, *supra*, at 407. Therefore, the qualitative differences between a cell phone and laptop demonstrate that the level and amount of intrusion by a forensic search of a laptop is routine.

3. The Ninth Circuit's reasoning for why a forensic search of a laptop is nonroutine is flawed because it fails to take into account the gravity of the Government's interest at the border.

The Ninth Circuit has held that the forensic search of a laptop was nonroutine because it was akin to "reading a diary line by line looking for a mention of criminal activity." *Cotterman,* 709 F.3d at 962-63. The court reasoned that even though a traveler has a diminished expectation of privacy at the border, the dignity and privacy interests will, on occasion, demand some level of suspicion in the case of highly-intrusive searches of the person. *Id*. at 963. Likewise, the Ninth Circuit explained that some searches of property are so destructive, particularly offensive,

or overly intrusive in the manner in which they are carried out, that they are determined to be nonroutine. *Cotterman,* 709 F.3d at 963. The court went on to reason that the "nature of the contents of electronic devices differs from that of luggage" because they are "simultaneously offices and personal diaries." *Id*. at 964. "When packing traditional luggage, one is accustomed to deciding what papers to take and what to leave behind. When carrying a laptop, tablet or other device, however, removing files unnecessary to an impending trip is an impractical solution given the volume and often intermingled nature of the files." *Id*. at 965.

While noble in its goal of protecting individual rights, the Ninth Circuit has misconstrued the balance of the Government's interests and the privacy interests of the individual. Searches found not routine in the interior are qualitatively different at the border. *Ramsey*, 431 U.S. at 621. For example, it would very likely be considered nonroutine for a local police officer to completely tear down a car and reassemble it; however, this is considered routine in the context of border searches despite the privacy interests of the individual remaining the same. *Id*. Furthermore, the Government's interests are at its zenith at the border. *Flores-Montano*, 541 U.S. at 152. If the Ninth Circuit's decision was adopted in the case at bar, it would severely hamper government officers from preventing unwanted persons and contraband from entering the country. The Ninth Circuit is correct that the amount and type of information that can be brought on a laptop is far beyond what could have been imagined fifty, thirty, or even twenty years ago. *Cotterman,* 709 F.3d at 962-64. But that amount and type of information only increases the Government's interest in preventing unwanted contraband from entering the country. By the same reasoning, the Government can look at this vast potential of contraband to ensure that none is entering. In addition, a forensic search is necessary because of the sophistication and difficulty government officers have in actually finding contraband on a computer; locked folders and hard drives, firewalls and self-destructing software, and many other

cybersecurity measures easily can prevent an onsite, quick glance at data from being effective at preventing contraband. Therefore, because the search in the case at bar would be considered routine and probable cause is not required, this Court should affirm the Fourteenth Circuit.

II. THE GOVERNMENT'S ACQUISITIONS OF HISTORICAL CELL-SITE RECORDS AND TOWER DUMP INFORMATION DID NOT VIOLATE PETITIONER'S FOURTH AMENDMENT RIGHTS.

The Fourth Amendment ensures "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches" conducted by the Government. U.S. Const. amend. IV. Historically, Fourth Amendment search doctrine focused on whether the Government obtained information by physically intruding on a constitutionally protected area. *Olmstead v. United States*, 277 U.S. 438, 466 (1928) (holding that wire-tapping did not amount to a search within the meaning of the Fourth Amendment because there was no "actual physical invasion"). More recently, taking into account advancements in technology, this Court has expanded the scope of the Fourth Amendment to protect certain reasonable expectations of privacy in addition to traditional property rights. *See Katz*, 389 U.S. at 351 (establishing that the Fourth Amendment is not limited to trespass of a physical space, but also includes particularized privacy interests of an individual). Technological developments, including location tracking in cell phones, have required courts to assess the boundaries of Fourth Amendment protections. *See generally Kyllo v. United States*, 533 U.S. 27 (2001).

Three sets of telecommunications records obtained by the Government, pursuant to the SCA, did not violate Petitioner's Fourth Amendment rights against unreasonable searches as established in *Carpenter v. United States*, 138 S. Ct. 2206 (2018). This Court should not undermine its narrow holding in *Carpenter* by dramatically expanding it to include historical CSLI requests of six days or fewer and to different methods of requesting CSLI information. The factual circumstances underlying the Government's CSLI requests do not implicate the

concerns articulated by this Court in *Carpenter*. Furthermore, because there is no bright-line rule, government officers are unable to benefit from the guidance of this Court. *See* Dylan Bonfigli, *Get a Warrant: a Bright-Line Rule for Digital Searches Under the Private-Search Doctrine*, 90 S. Cal. L. Rev. 307, 335-36 (2017) (discussing how a bright-line rule provides law enforcement with clarity, prevents courts from wading into difficult factual inquiries, and promotes responsible investigative techniques). Therefore, this Court should affirm the United States Court of Appeals for the Fourteenth Circuit, and hold that the Government's acquisitions of tower dump information, Three-day Records, and Weekday Records from Petitioner's cellular service provider were constitutional.

A. In *Carpenter*, This Court Held that the Government Is Required to Obtain a Warrant Before Requesting Seven Days of Historical Cell-Site Location Information.

This Court's recent decision in *Carpenter* created a narrow, policy-driven, and factually specific rule for when CSLI triggers the Fourth Amendment. This Court held that accessing seven days of historical CSLI constitutes a search under the Fourth Amendment, and therefore, government officers must obtain a warrant in order to request more than six cumulative days of CSLI. *Carpenter*, 138 S. Ct. at 2217 n.3. This Court heavily based its reasoning on the facts of the case. *See id*. at 2220.

Due to the incriminating proof found in CSLI obtained by the Government, Timothy Carpenter was convicted and sentenced to more than one-hundred years in prison for his role in a series of nine armed robberies that occurred during a four-month span. *Id*. at 2213. Government officers were able to obtain CSLI records without a warrant by applying for a court order under the SCA. *Id*. at 2212. The SCA permits government officers to compel cellular service providers to disclose certain telecommunications records only if they offer "specific and articulable facts showing that there are reasonable grounds to believe" that the records "are

relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). Federal magistrate judges issued the disclosure of Carpenter's CSLI during the four-month period when the robberies occurred in order to identify whether he was in the vicinity. *Carpenter*, 138 S. Ct. at 2212. One order requested 152 days (3,648 hours) of CSLI, and the other order requested seven days (168 hours) of CSLI. *Id*. The data confirmed that Carpenter's cell phone was in the general vicinity of four of the nine robberies at the times those robberies occurred. *Id*. at 2213.

On appeal, this Court resolved the issue of whether the CSLI obtained by the Government constituted a "search" under the Fourth Amendment. *Id*. at 2211. In a 5-4 decision, this Court reversed the Sixth Circuit, and set forth the rule that accessing seven days, or 168 hours, of historical CSLI constitutes a search. *Id*. at 2217 n.3. Furthermore, because no exceptions to the warrant requirement applied, a warrant was required for the search to be reasonable under the Fourth Amendment. *Id*. at 2221.

This Court made it clear that its holding was limited to seven days of continuous CSLI. *See id*. at 2217 n.3. In reaching this decision, this Court articulated several important policy concerns in reaching its decision. First, this Court was concerned that 168 hours of continuous CSLI "provides an intimate window into a person's life." *Id*. at 2217. Second, this Court was concerned with the Government's accessibility to CSLI, because with "just the click of a button, the Government can access. . . historical location information." *Id*. at 2218. Finally, this Court was concerned with the accuracy and "GPS-level precision" of CSLI that could further compound the potential intimacy of the data. *Id*. at 2219.

Carpenter did not articulate a test for when less than seven days of CSLI may require a warrant; now, this Court should adopt a bright-line rule that less than seven days of CSLI does not require the Government to obtain a warrant. There is a considerable benefit to government officers and the judicial system in having a bright-line rule for when a warrant is required

regarding CSLI. Bonfigli, *supra*, at 335-36. It is well established that having a clear rule supports predictability of result and avoids inconsistent police and judicial determinations. *See State v. Storm*, 898 N.W.2d 140, 156 (Iowa 2017). Clear, bright-line rules are especially beneficial when officers have to make quick decisions as to what the law requires. *Id*. Requiring a warrant every time a government officer wishes to access these records would only serve to slow down and frustrate their efforts. *See* Kyle Malone, *The Fourth Amendment and the Stored Communications Act: Why the Warrantless Gathering of Historical Cell Site Location Information Poses No Threat to Privacy*, 39 Pepp. L. Rev. 701, 744 (2012) (discussing the value of cell phone records to law enforcement). This Court should therefore adopt the rule that less than seven days of CSLI does not require the Government to obtain a warrant, not because *Carpenter* compels it, but because the underlying policy rules make it a sound policy decision.

B. The Policy Concerns Implicated in *Carpenter*'s Narrow Holding Do Not Apply to the Case at Bar.

This Court's decision in *Carpenter* was "a narrow one" and this Court did not express a view on matters not before it. *Carpenter*, 138 S. Ct. at 2220. It did not rule on whether collection of CSLI for less than seven days implicated the same Fourth Amendment concerns. *Id*. Furthermore, this Court did not apply its holding to other government collection techniques such as tower dumps. *Id*. In fact, this Court invoked Justice Frankfurter's warning from 1944 that courts must tread carefully in cases involving new innovations so as not to "embarrass the future." *Id*. (quoting *Northwest Airlines, Inc. v. Minnesota*, 322 U.S. 292, 300 (1944) (internal quotations omitted). The explicit language in *Carpenter* demonstrates that this Court's narrow decision should not be expanded to include the telecommunications data in the case at bar.

Looking beyond this Court's strong warning not to extend its holding, the policy concerns discussed in *Carpenter* are not of concern in the present case. This Court was concerned that 168 continuous hours of CSLI holds private information because it provides an

"intimate window" into a person's life, is easily accessible by the Government, and has great accuracy and precision. *See Carpenter*, 138 S. Ct. at 2217-20. Consistent with this Court's holding in *Carpenter*, the tower dump information, Three-day Records, and Weekday Records at issue serve compelling security interests at little cost to Petitioner's privacy.

1. This Court should not expand *Carpenter* to include tower dump information because of the Government's interest in accessing efficient investigatory tools, and lack of personal information contained within.

Carpenter's narrow holding should not apply to tower dump information because a long list of all phone numbers that connected to a particular cell tower within a short, one-hour period of time does not reveal detailed information about a person's life. A tower dump is a chronological list of every single phone number that used a tower for any purpose, regardless of cellular service provider, for a very short period of time. *United States v. Pembrook*, 876 F.3d 812, 816 (6th Cir. 2017) (vacated on other grounds). In *Carpenter*, this Court explicitly refused to "express a view on" tower dumps or "call into question conventional surveillance techniques." *Carpenter*, 138 S. Ct. at 2220. Because of the compelling governmental interest in ensuring the efficiency of current law enforcement practices, and because a tower dump does not reveal more than a location and phone number, *Carpenter* should not be extended to include tower dump information.

a. <u>The Government has a substantial interest in the need for efficient tools during the initial stages of criminal investigations.</u>

There is a governmental interest in having probative investigatory tools that do not require a warrant. Malone, *supra*, at 743-44. There is no dispute that the SCA's "specific and articulable" facts standard is less than the probable cause standard required for a search warrant. 18 U.S.C. § 2703(d); *United States v. Davis*, 785 F.3d 498, 505 (11th Cir. 2015). Courts have held that initial applications for tower dump information that "briefly informed the magistrate judge about the particulars" of the crime being investigated were sufficient under the SCA.

Pembrook, 876 F.3d at 823-24. Government officers need access to investigative tools under a lower standard because it allows them to create a list of potential suspects at the initial stages of investigations where they otherwise would not be able to. (R. 14).

For example, the Sixth Circuit held that government officers may access and obtain tower dump information without a warrant under the SCA. *See generally Pembrook*, 876 F.3d 812. In *United States v. Pembrook*, an FBI agent began his investigation of two jewelry store robberies by acquiring a tower dump for the cell phone towers near the two stores, pursuant to the SCA. *Id*. at 816, 822. The agent found the same phone number had used towers near each of the robberies around the times they occurred. *Id*. at 816. The tower dump information guided the FBI to further examine the suspect, and obtain other evidence which eventually led to the conviction of four co-defendants. *Id*. The Sixth Circuit held the use of the tower dump information under the SCA was constitutional. *Id*. at 823.

Similarly, in the case at bar, the first type of telecommunications records requested by the FBI were three tower dumps from the cell sites near three of the Sweetwater ATMs. (R. 4). After Mariposa Bank discovered the ATM tampering, it turned its findings over to the FBI. Hale Aff. ¶¶ 18-19. It was only after receiving the information from Mariposa Bank that the FBI requested tower dumps for thirty minutes before and after a suspicious man approached and tampered with the ATMs, pursuant to the SCA. Hale Aff. ¶ 19. Moreover, in her affidavit submitted in support of an application for a Section 2703(d) court order, Hale declared under penalty of perjury that there was a reasonable ground to believe that the tower dump information was relevant and material to the ongoing investigation. Hale Aff. ¶ 21. The tower dump information was crucial to the FBI discovering potential suspects, such as Petitioner. The SCA allows the FBI to access this information at the initial stages of criminal investigations, and Hale's affidavit made under penalty of perjury provided additional support. *See In re U.S. for*

Historical Cell Site Data, 724 F.3d 600, 602 (5th Cir. 2013) (in which the Government provided the court with evidence detailing its cell-site records in the form of an affidavit). Tower dump information is a legitimate investigatory tool, and if a higher standard was imposed by this Court as Petitioner requests, the FBI would no longer have access to this effective and essential mechanism.

b. Tower dump information does not provide an intimate window into a criminal suspect's life.

First, because tower dumps only provide a list of numbers, they do not provide the Government with personal information worthy of Fourth Amendment protection. This Court has held that records containing a limited amount of personal information, specifically information that lacks any content, do not implicate privacy concerns. *See Smith v. Maryland*, 442 U.S. 735 (1979). In *Smith v. Maryland*, this Court addressed law enforcement access to the criminal suspect's outgoing call data, and held that government officers did not require a warrant to use a pen register because it did not show the content of the calls. *Id*. at 746. Similar to the pen register data in *Smith*, tower dump information does not provide a "detailed and comprehensive record of the person's movements" because it only provides a list of cell phone numbers. *Carpenter*, 138 S. Ct. at 2217. Government officers should not be required to obtain a warrant before accessing tower dump information because it has a limited ability to reveal sensitive information.

Second, the limited time period during which the tower dump information was requested is not extensive enough to implicate the policy concerns articulated by this Court in *Carpenter*. In *Carpenter*, CSLI was requested for an extended period of seven days, which amounted to 168 hours of continuous tracking. *Id*. at 2212. This large volume of tracking information provided an intimate window into Carpenter's life because it had the ability to show his familial, political, professional, religious, and sexual associations. *Id*. at 2217. On the other hand, the tower dump

requests in the case at bar were only for a limited one hour period of time – the thirty minutes before and thirty minutes after bank surveillance footage caught a man in a black sweatshirt tampering with ATMs. (R. 4). Three brief, relevant windows of time cannot be compared to the 168 hours of continuous CSLI.

Finally, the extensive lists taken from tower dumps do not provide particularized information about an individual because of the vast amount of other cell phone numbers contained within. Sweetwater is a densely populated city in the most populous state in the Fourteenth Circuit, West Texas. (R. 2 n.1). Tower dumps taken from cell towers in Sweetwater contain a long list, as compared to tower dumps from less populous cities. Hale Aff. ¶ 11. Longer lists lack specificity because the percentage chance that a given number on the list belonged to the criminal is very low. Therefore, this Court should not extend *Carpenter* to include tower dump information because the governmental need for this investigatory tool is great, and the records do not provide an intimate window into a suspect's life.

2. *Carpenter* should not be dramatically extended to include the Three-day Records because three days is not enough time to invade any reasonable expectation of privacy.

Carpenter's holding was based on factual underpinnings that are not present in the case at bar. This Court reasoned that seven days of time-stamped data can reveal an individual's familial, political, professional, religious, and sexual associations. *Carpenter*, 138 S. Ct. at 2217. "A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales." *Id*. at 2218. Because cell phone users carry their phones with them everywhere, seven days of nonstop CSLI allows the government to achieve "near perfect surveillance, as if it had attached an ankle monitor to the phone's user." *Id*.

To the contrary, a mere 72 hours is not an amount of time that allows police to conduct a fishing expedition into a person's life, and CSLI taken from this extremely limited window is only useful when government officers can link a suspect to a relevant time frame. (R. 13). Here, the maintenance records of the bank and the customer complaint of ATM tampering created a small three-day window when the crime was likely committed. (R. 3). A brief 72 hours of CSLI was necessary for the Government to know whether Petitioner was in the location of the ATM tamperings during the relevant times.

Although three days of CSLI may provide essential incriminating information, it does not necessarily follow that it also provides an intimate view of an individual's life, which is a primary concern with seven days of CSLI. Three days does not amount to the same level of "depth, breadth, and comprehensive reach" as seven days. *Carpenter*, 138 S. Ct. at 2223. Three days creates a brief, incomplete snapshot, which substantially limits government officers' surveillance of an individual's life. Consistent with this Court's holding in *Carpenter*, the Government's request for the Three-day Records did not violate Petitioner's Fourth Amendment rights, and this Court should adopt the rule that requests for less than seven days of CSLI can be made without a warrant.

3. This Court's rationale in *Carpenter* does not apply to the Weekday Records because the quantity and quality of the data is insufficient to warrant the same privacy concerns as seven days of nonstop cell-site location information.

100 hours of CSLI over the course of ten weekdays does not implicate the policy concerns articulated in *Carpenter*. The Weekday Records were the last set of telecommunications records requested by the Government. (R. 5). They were only requested after the Three-day Records placed Petitioner's cell phone in the area of the Sweetwater ATMs, making Petitioner more likely to be criminally liable for the tamperings. (R. 5). This Court's

policy concerns articulated in *Carpenter* are not at issue regarding the Weekday Records because of the extremely limited quantity and quality of the data.

First, 100 hours of CSLI does not provide enough quantity of data to invoke Fourth Amendment protection. 100 hours amounts to less than five days of hours for a relevant time frame and is much less than the 168 hours of CSLI at issue in *Carpenter*. (R. 13). Under the same logic used to determine that 72 hours of CSLI does not provide enough data to violate *Carpenter* or implicate the same concerns as 168 hours, five days does not either.

Second, in addition to the small quantity of data provided by the Weekday Records, the quality of data is not nearly as all-encompassing as the CSLI in *Carpenter*. Limiting the request to working hours diminishes the privacy concern that a "cell phone faithfully follows its owner beyond public thoroughfares and into private residences." *Carpenter*, 138 S. Ct. at 2218. The Weekday Records only contain CSLI between the hours of 8AM and 6PM, Monday through Friday, which is during the typical workweek. (R. 5). This Court has articulated that information that could be discovered from a public thoroughfare does not constitute a search under the Fourth Amendment. *United States v. Knotts*, 460 U.S. 276, 284 (1983). If an individual is in a public place, there is a lesser expectation of privacy than if an individual is in a private place, such as in a private home. *See generally id*.

The privacy interest in the Weekday Records is similar to this Court's determination in *United States v. Knotts* because the CSLI was only taken during the normal business hours of 8AM through 6PM, when people are typically out in the public domain performing a limited range of public activities. *See generally id*. Records taken during working hours do not show intrusive information because the information would be in the public domain regardless. The Government's request for only 100 hours of CSLI recorded during limited working hours does not implicate the concerns voiced by this Court in *Carpenter*. Therefore, this Court should

affirm the lower court and hold that the Government's acquisitions of tower dump information and historical CSLI did not violate Petitioner's Fourth Amendment rights.

CONCLUSION

Petitioner's Fourth Amendment rights were not violated by the Government officers' actions in the case at bar. First, the forensic search of Petitioner's electronic devices at the border fell within the well-recognized exception to the warrant requirement because the search occurred at the border. This Court has never held that nondestructive searches of property at the border be "routine." In fact, this Court has never required reasonable suspicion for searches of property at the border because the Government's security interest is so great. Even if "routineness" is required for searches at the border, the search in the case at bar was routine. Therefore, no reasonable suspicion was required to conduct the forensic search of Petitioner's electronic devices.

Second, the Government's acquisitions of historical CSLI and tower dump information, pursuant to the SCA, also did not violate Petitioner's Fourth Amendment rights. In *Carpenter*, this Court articulated an intentionally narrow holding in requiring the Government to obtain a warrant before requesting seven days or more of historical CSLI. This Court's rationale was fact-based, and the policy concerns implicated in *Carpenter* do not apply to the facts of the case at bar. In weighing the Government's substantial security interest with the lack of personal information contained within the records at issue, this Court should not expand *Carpenter*. Moreover, this Court should adopt a bright-line rule for when access to telecommunications records requires a warrant, in the best interest of government officers and the judicial system. This Court should affirm the Fourteenth Circuit's ruling and provide government officers with the rule that they are not required to obtain a warrant to request tower dump information or less than seven days of historical CSLI. In sum, the Government respectfully requests that this Court

affirm the Fourteenth Circuit and hold that Petitioner's Fourth Amendment rights were not violated.

Dated: February 8, 2019

Respectfully submitted,

Attorneys for Respondent