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 PETITIONER

Team P5
Counsel for Petitioner

TABLE OF CONTENTS

TABLE OF AUTHORITIES

United States Supreme Court Cases

United States Circuit Court Cases

Constitution, Statutes, and Legislation Materials

Other Authorities

QUESTION PRESENTED

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

II. Whether the government's acquisitions pursuant to 18 U.S.C. § 2703(d) of three days of cell-site location information, one-hundred cumulative hours of cell-site location information over two weeks, and cell-site location information collected from cell tower dumps violate the Fourth Amendment of an individual in light of this Court's limitation on the use of cell-site location information in *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

OPINIONS BELOW

The opinion of the Fourteenth Circuit is reported at 1001 F.3d 1341. The district court opinion from the United States District Court of West Texas is unpublished.

CONSITUTIONAL PROVISIONS AND RULES

The Fourth Amendment to the U.S. Constitution provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The Stored Communications Act, 18 U.S.C. § 2703, provides in relevant part:

> (c) Records concerning electronic communication service or remote computing service. —
>
> (1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—
>
> (A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; [or]
>
> (B) obtains a court order for such disclosure under subsection (d) of this section;
>
> (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

INTRODUCTION

Brief for Petitioner

Petitioner Hector Escaton respectfully requests that this Court reverse the judgment of the United States Court of Appeals for the Fourteenth Circuit.

Jurisdiction

The Fourteenth Circuit issued its opinion on November 2, 2021. This Court granted Petitioner's Writ of Certiorari on November 22, 2022, and retains jurisdiction pursuant to 28 U.S.C. § 1254(1).

Standard of Review

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

Summary of Argument

Mr. Escaton's Fourth Amendment rights were violated when a forensic search was conducted on his electronic devices because reasonable suspicion is required to conduct a forensic search of electronic devices, even at the international border. While an individual's expectation of privacy is lower at an international border, it is not completely gone. Reasonable suspicion is required when a search invades an individual's privacy. Unlike a search of a vehicle, a forensic search is more comparable to a highly invasive internal body search. Many electronic devices contain data on every aspect of an individual's life, and forensic searches allow the searcher to see even deleted information. Requiring reasonable suspicion to conduct a forensic search does not impede the ability to protect the border and would be in keeping with current policies adopted by the Department of Homeland Security.

Additionally, the Government's acquisition of Mr. Escaton's three-day records, weekday records, and tower dumps contravened his reasonable expectation of privacy as announced by this Court in *Carpenter v. United States*, 138 S. Ct. 2206 (2018). The Government was provided an intimate window into Mr. Escaton's private life without having first satisfied the Fourth Amendment's warrant requirement. The Government ignored this Court's clearly demarked precedence when it failed to seek a warrant to acquire eleven days-worth Mr. Escaton's year old historical cell site location data.

For the aforementioned reasons, we respectfully request this Court reverse the Fourteenth Circuit's decision and find that (1) reasonable suspicion is required to conduct a forensic search of electronic devices at the border, and (2) that the Government's acquisition of Mr. Escaton's CSLI without a warrant was in contravention of his Fourth Amendment rights.

STATEMENT OF THE CASE

This case concerns the unlawful search and seizure of Petitioner Hector Escaton's property, and subsequent acquisition of his historical location data for a period of eleven days in contravention of his Fourth Amendment rights. The Fourth Amendment ensures that citizens be "secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. CONST. amend. IV.

Border searches are an exception to the Fourth Amendment that have been carved out since the creation of the United States. Before the First Congress even drafted the Fourth Amendment, they created the exception by passing the Act of July 31, 1789. *United States v. Ramsey*, 431 U.S. 606, 616 (1977). Border searches are considered reasonable simply because they occur at the border. *Id*. This Court has faithfully followed this longstanding principle and has not required warrants for searches at the border. *Id*. at 617. However, this doctrine was created while travelers

were only bringing items in luggage and not carrying around devices that contain the entirety of the personal, intimate details of their lives.

The ubiquity of cell phones, coupled with ever-expanding technological advancements make the acquisition of cell site location information (CSLI) equivalent to a search under the Fourth Amendment. In order to create a CSLI record, cell phones connect to nearby cell towers thereby recording the historical location data of a particular cell phone. The precision of this data is largely dependent on the amount of cell towers in a given area; generally, the denser the area, the more cell towers, and thus the more accurate data. Advancements in cell towers and cellular devices have only exacerbated the precision at which CSLI can be relayed. Accordingly, the volume and precision of CSLI will only continue advance and thus produce ever more revealing locational data.

Statement of Facts

The present controversy arose when Mr. Escaton was stopped at the United States (U.S.) – Mexico border for an extended period of time on September 25, 2019. (R. at 1342-43). Mr. Escaton is a U.S. citizen who resides in West Texas where he holds steady employment as a bartender at Mesa Hub. (R. at 1342; Hale Aff. ¶ 8). Mr. Escaton was attempting to reenter the U.S. when Customs and Border Protection (CBP) Officer Ashley Stubbs conducted a search of his vehicle. (R. at 1342). Officer Stubbs found three suitcases in Mr. Escaton's car and without reasonable suspicion searched them and their contents. (R. at 1342).

Upon Officer Stubbs' search she discovered an iPhone, laptop, three external hard drives, and four USB devices. (R. at 1342). An innocuous note reading "Call Delores (201)181-0981 $$$" was on the bottom panel of the laptop. (R. at 1342). Without any evidence of wrongdoing Officer Stubs seized and proceeded to search all nine devices. (R. at 1342-43). Officer Stubs manually searched both the laptop and iPhone; neither were connected to the internet at the time of the

search. (R. at 1342-43). Upon discovering that certain folders in Mr. Escaton's laptop were password protected, Officer Stubbs indefinitely seized the laptop, hard drives, and USBs but returned the iPhone after recording its number. (R. at 1342-43).

Stationed at the border checkpoint was Special Agent & Computer Forensic Examiner Theresa Cullen with Immigration and Customs Enforcement (ICE). (R. at 1343). Officer Stubbs delivered the remaining eight devices to Special Agent Cullen to be thoroughly searched. (R. at 1343). Special Agent Cullen began the search by copying and scanning the contents of all devices, a process that took several hours. (R. at 1343). During Special Agent Cullen's search Mr. Escaton remained detained at the border while his property was in the Government's control. (R. at 1343). Special Agent Cullen's search revealed bank account numbers on the laptop, and traces of malware on the USBs. (R. at 1343).

Based on this modicum of suspicion Officer Stubs referred Special Agent Cullen's findings over to the Federal Bureau of Investigation (FBI). (R. at 1343). FBI Special Agent Catherine Hale immediately used these findings to paint Mr. Escaton as the lead suspect in a string of eight ATM robberies in two separate West Texas cities occurring almost a year prior to his seizure at the border.[1] (R. at 1343). Through Mariposa Bank data the FBI was able to deduce that five[2] of the eight ATM robberies occurred from October 11-13 in the city of Sweetwater.[3] (R. at 1343-44). (R.

[1] The FBI was made aware of the eight robberies in October 2018. (R. at 1344).

[2] Two robberies were conducted through use of an "ATM Skimmer," a device overlaying the debit card readers and copying a card's information when inserted. Another two were conducted through use of malware. The remaining robberies was conducted through use of *sophisticated* malware. (R. at 1345) (emphasis added).

[3] ATM maintenance records indicated that the ATMs were tampered with after a technician checked them on October 11, 2018, but before tampering was discovered on October 13, 2018. (R.

at 1343). The remaining three robberies occurred in the town of Escalante, however, the data from those ATMs was lost and Mariposa Bank could only make a determination that skimming did occur in early October 2018. (R. at 1343-44). Special Agent Hale was able to determine that the malware on Mr. Escaton's seized USBs was similar *but not identical* to the Malware infecting two Sweetwater ATMs. (R. at 1345) (emphasis added).

Special Agent Hale, in coordination with U.S. Attorney Elsie Hughes, requested tower dumps[4] of three cell sites in Sweetwater for thirty minutes before and as well as thirty minutes after a suspicious man loitered around three Mariposa Bank ATMs.[5] (R. at 1343; Hale Aff. ¶ 19). This request was made and approved on the grounds that there were "specific and articulable facts showing … reasonable grounds to believe" that Mr. Escaton skimmed the ATMs at eight banks, in two separate cities, over a span of less than three days. (R. at 1343); 18 U.S.C. § 2703(d). The detailed tower dumps revealed that Mr. Escaton was in Sweetwater at the time of the ATM skimmings. (R. at 1345).

Special Agent Hale did not seek a warrant based on probable cause for Mr. Escaton's CSLI between October 11-13, 2018 (hereinafter "three-day records"), but rather submitted an unsworn application pursuant to 18 U.S.C. § 2703(d) of the Stored Communications Act (SCA). (R. at 1345; Hale Aff. ¶¶ 21-22); 18 U.S.C. § 2701 *et seq*. As a result, the district court never made a probable cause finding before ordering Delos Wireless to disclose Mr. Escaton's historical cellular location.

---

at 1343-44; Hale Aff. ¶ 18).

[4] A "tower dump" is a list of all phone numbers, used in a given location. Generally, denser cities, such as Sweetwater, will have more cell sites thus providing a more precise location of the individuals enclosed in these tower dumps. (R. at 1344).

[5] Mariposa Bank turned over surveillance photographs that showed a man in a black sweatshirt near the skimmed ATMs during the time they were suspected to have been tampered with. (R. at 1344).

(R. at 17-18).[6] The application sought seventy-two hours of Mr. Escaton's CSLI when he was known to be in a part of Sweetwater that has enough cell towers to pinpoint an individual's exact location.[7] (R. at 1345; Hale Aff. ¶¶ 11, 20). The three-day records placed Mr. Escaton near a Mariposa Bank location in Sweetwater on October 12, 2018. (R. at 1345). However, the three-day records did not place him in Escalante.[8] (R. at 1345).

Since it was unlikely that Mr. Escaton accomplished all eight of the robberies by himself, and within a time span of less than three days, Special Agent Hale speculated that "Delores" must have abetted him.[9] (R. at 1345). In turn Special Agent Hale submitted another application pursuant to the requirements of the SCA for ten weekdays of Mr. Escaton's and Ms. Abernathy's CSLI from October 1-12 (hereinafter "weekday records").[10] (R. at 1345); 18 U.S.C. § 2703(c)(B), (d). Again, the district court never made a finding of probable cause before these records were disclosed. (R. at 1353). The acquired CSLI did reveal that Ms. Abernathy was near the Escalante ATMs, and that

---

[6] The District of West Texas's order cited in the record does not contain a page number or docket number but can be found on the two pages immediately following page 16 of the record.

[7] Sweetwater is a dense urban city with a population of over 1.4 million people. There are enough cell towers in Sweetwater to locate an individual within fifty feet. However, many of the buildings at the center of the city have smaller cell sites on them and thus have the potential to locate an individual's exact location. The five Mariposa Banks in Sweetwater are located in the center of the city. (R. at 1345; Hale Aff. ¶¶ 11, 20).

[8] Escalante is a suburban town with few cell sites, allowing CSLI to be accurate within 1000 feet. (Hale Aff. ¶¶ 12).

[9] Delores was later discovered to be Ms. Delores Abernathy. (R. at 1345).

[10] The application requested CSLI during the weekdays between October 1-12 from the times of 8 AM MDT to 6 AM MDT (hereinafter "business hours"). (R. at 1345).

Mr. Escaton was in Escalante with her prior October 11. (R. at 1345). A search warrant was obtained to search Ms. Abernathy's home where they found the same malware stored on Mr. Escaton's USBs. (R. at 1345). In total, the acquired CSLI allowed the Government to determine Mr. Escaton's location for the most relevant parts of an eleven day[11] span on a showing less than probable cause. (R. at 1344-45).

Procedural History

Mr. Escaton was indicted in the District of West Texas for bank fraud[12], conspiracy to commit bank fraud[13], and aggravated identity theft.[14] (R. at 1346). Before trial, Mr. Escaton filed a motion to suppress the results of the forensic search conducted on his devices during his detention at the border, and the CSLI acquired from Delos Wireless. (R. at 1346). The district court denied his motion, and rejected his arguments that the border search was conducted without reasonable suspicion and that a warrant was required in order for the Government to obtain his CSLI. (R. at 1346). A jury eventually found Mr. Escaton guilty on all counts. (R. at 1346).

On appeal, a three judge panel found that reasonable suspicion is not required to conduct forensic examinations of electronic devices at border crossings. However, the court was divided in finding that the Government's request for CSLI did not violate Mr. Escaton's Fourth Amendment rights. (R. at 1346). Writing for the court, Judge Ford concluded that border searches are categorically different from other searches, and requiring the Government to have reasonable suspicion to conduct searches at the border would place too heavy a burden on our national

[11] Totaling 152 hours of CSLI.

[12] 18 U.S.C. § 1344

[13] 18 U.S.C. § 1349

[14] 18 U.S.C. § 1028A

security. (R. at 1346-49). He then opined that the Government's requests and acquisition of the tower dumps, three-day records, and weekday records were proper under *Carpenter v. United States*, 138 S. Ct. 2206 (2018), and not in contravention of Mr. Escaton's Fourth Amendment right. (R. at 1350-54). Judge Ford reasoned that refining *Carpenter* would result in the lower courts continuously laboring to construct judicial rules for fact specific situations. (R. at 1351-52)

Judge Weber disagreed, dissenting in judgement only on the three-day and weekday record requests. (R. at 1354). Judge Weber explained that the majority's interpretation of *Carpenter* was too narrow and did not follow the Court's intent. (R. at 1354-55). Judge Weber argued that the CSLI requests made here mirror the concerns the Court in *Carpenter* outlined, and due to CSLI's potential to disclose private information the Government's acquisition of such violated Mr. Escaton's Fourth Amendment rights. (R. at 1354-56)

ARGUMENT

I. THE FOURTEENTH CIRCUIT'S HOLDING THAT NO REASONABLE SUSPICION IS REQUIRED TO CONDUCT FORENSIC EXAMINATIONS OF ELECTRONIC DEVICES AT THE BORDER CROSSINGS SHOULD BE REVERSED.

While there is a lessened expectation of privacy at the international border, it cannot be interpreted to mean that border patrol agents have unchecked power to search at the international border. *United States v. Montoya de Hernandez*, 473 U.S. 531, 541 (1985). The reasonable suspicion standard is a way to keep the power in check while allowing for less than probable cause. *Id*. Unlike a manual search of electronic devices, a forensic search is a nonroutine search, and thus invasive. The more invasive the search is of an individual's privacy, the greater likelihood that the search is nonroutine. *United States v. Kolsuz*, 890 F.3d 133, 144 (4th Cir. 2018). Due to the massive amount of personal data electronic devices can store, a search of an electronic device is highly invasive. *Riley v. California*, 134 S. Ct. 2473, 2489-90 (2014). Highly invasive, nonroutine searches require reasonable suspicion. *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004).

A. Reasonable suspicion must be based on objective measurements and particularized suspicion.

Reasonable suspicion requires a totality of the circumstances analysis based on objective measurements that yield particularized suspicion. *United States v. Cortez*, 449 U.S. 411, 418 (1981). In *Cortez*, this Court decided a case involving Border Patrol agents in Arizona who noticed footprints and tire tracks of what they believed to be a guide leading aliens across the Mexico border. *Id*. at 413. The officers stopped Cortez's vehicle and found his shoeprint matched the one they had seen in the sand. *Id*. at 415. This Court then defined reasonable suspicion. *Id*. at 418. Reasonable suspicion has two elements, both of which are necessary. *Id.* The assessment must be based on the totality of the circumstances. *Id*. This includes using objective measurements, such as police reports and considerations of the "modes or patterns of operations of certain kinds of lawbreakers." *Cortez*, 449 U.S. at 418. The totality of the circumstances must then lead to the second element; particularized suspicion that the individual is engaged in wrongdoing. *Id*. Thus, objective facts can be combined with inferences to lead to reasonable suspicion by a trained, skilled officer. *Id*. at 419.

The parties here agree that there was no reasonable suspicion at the time of the border search. (R. at 1346). However, even if they were not in agreement, there would be no reasonable suspicion. The nondescript note on Mr. Escaton's laptop and password protected folders on his iPhone are hardly circumstances that lead to particularized suspicion of wrongdoing.

B. While routine searches do not require reasonable suspicion, nonroutine searches are highly invasive and require reasonable suspicion.

A search of a vehicle, including removal and disassembly of the gas tank, is a routine search because it is not highly invasive of an individual's privacy. *Flores-Montano*, 541 U.S. at 154. Flores-Montano was stopped and his vehicle inspected. *Id*. at 150. An officer tapped on the gas tank and believed it sounded solid. *Id*. at 151. A mechanic removed and disassembled the gas tank

and found 37 kilograms of marijuana bricks. *Id*. Ultimately, this Court held that no reasonable suspicion was required to remove and disassemble the gas tank of a vehicle. *Id*. at 155. While the "dignity and privacy interests of the person being searched" at the border demands "some level of suspicion in the case of highly intrusive searches," this requirement does not carry over into a vehicle. *Id*. at 152. The Court recognized long ago that a car seeking to enter the country may be searched. *Flores-Montano*, 541 U.S. at 154. Therefore, the search of the gas tank is no more "an invasion of privacy than a search of the automobile's passenger compartment." *Id*.

In contrast, an internal search of an individual's body is highly invasive, requiring reasonable suspicion prior to an officer conducting the search. *Montoya de Hernandez*, 473 U.S. at 541. Montoya de Hernandez arrived in the United States from Bogota, Colombia. *Id*. at 533. While going through customs, officers suspected she was smuggling drugs via balloon swallowing. *Id*. at 534. Subsequently, she was detained for sixteen hours and, once a court order was obtained, x-ray examination revealed balloon's containing a foreign substance. *Id*. at 535. This Court held that a search beyond the ordinary, routine border search is justified if the officers have reasonable suspicion that the traveler is smuggling contraband internally. *Id*. at 541. At the border, the Fourth Amendment balance between government interests and privacy rights weighs more heavily in favor of the government. *Id*. at 540. Thus, requiring reasonable suspicion to conduct an internal search of an individual's body evens out the balance between the two interests. *Montoya de Hernandez*, 473 U.S. at 541. Therefore, requiring reasonable suspicion to conduct an internal body search requires a "particularized and objective basis for suspecting the particular person." *Id*. (quoting *Cortez*, 449 U.S. at 417).

When Mr. Escaton was stopped at the checkpoint and a search of his vehicle was conducted, this search was in keeping with this Courts' decision in *Flores-Mantano* and no reasonable suspicion was needed. However, upon discovery of Mr. Escaton's iPhone, laptop, three

hard drives, and four USB devices, any search other than a manual search takes it outside the scope of the *Flores-Montano* holding. The Government's internal search of the electronic devices using forensic software is akin to the internal body search in *Montoya de Hernandez*. *See id*. at 541. Like the x-ray used to find the balloons in Montoya de Hernandez, the forensic search copied and scanned the devices, which gave Special Agent Cullen the ability to see all personal information stored by Mr. Escaton. (R. at 1343).

C. Like an x-ray of an individual, a forensic search of an electronic device yields all personal information stored on the device, whether or not it has been deleted.

Unlike luggage, which can be left behind to avoid a search, the necessity of electronic devices means that absent a requirement of reasonable suspicion, they will always be subjected to a forensic search, revealing an individuals' intimate details. *Kolsuz*, 890 F.3d at 145. When Kolsuz entered the country, customs agents searched his luggage, and found firearm parts. *Id*. at 139. Kolsuz was detained and a manual search was conducted on his iPhone, which confirmed he did not have the necessary licenses to export firearms. *Id*. Next, a forensic search was done on his iPhone. *Id*. Despite being on airplane mode, one month's worth of data was extracted, which created an 896-page report comprised of Kolsuz's contacts, emails, conversations, web browsing history, phone logs, and a history of his location with precise GPS coordinates. *Id*. The court held that a forensic search must be treated as nonroutine and is permissible only on a showing of reasonable suspicion. *Id*. at 144. To decide whether a search is nonroutine, courts focus on how deeply the search intrudes into an individual's privacy. *Kolsuz*, 890 F.3d at 144.

Luggage, which is always subject to routine border searches, only allows the carrier to bring limited items, including personal information. *Id*. at 145. Comparatively, the amount of highly personal information that can be stored on a phone absolutely dwarfs what can be carried in luggage. *Id*. Aside from the quantity of information, cell phones and laptops contain unique, personal information, the quality of which yields the intimate details of an individual's life. *Id.* at

145. Additionally, electronic devices can return information that may be stored remotely. *Id*. Taken together, this information can provide a picture of a person's "familial, political, professional, religious, and sexual associations." *Id*. (quoting *United States v. Jones*, 565 U.S. 400 (2012) (Sotomayor, J., concurring). To avoid revealing personal information in a luggage search, that particular item can simply be left at home. *Id*. However, it is impractical to expect individuals traveling abroad to leave behind electronic devices, which are most likely their primary means of communication. *Kolsuz*, 890 F.3d at 145. The ubiquity and necessity of electronic devices, coupled with the intimate details they contain make it obvious that a forensic search constitutes a nonroutine border search. *Id*.

A forensic search is highly invasive due to the comprehensive amount of information gathered about an individual, which amounts to a "computer strip search." *United States v. Cotterman*, 709 F.3d 952, 966 (9th Cir. 2013). Cotterman was stopped while returning to the United States from Mexico. *Id*. at 957. Within the vehicle were two laptops and three digital cameras. *Id*. Upon a forensic search, seventy-five images of child pornography were found on the laptops, in the space where deleted files are kept. *Id*. at 958. The court found that even at the international border the Fourth Amendment still requires that the nature and the scope of the search be reasonable, thus reasonable suspicion was needed to conduct a forensic search. *Id*. at 962-63.

A forensic search copies a computer's hard drive and analyzes not only current data, but data that has been deleted, which is the equivalent of searching a diary for criminal activity, including anything that has been erased. *Id*. The information stored on an electronic device is an individual's "papers" that the Fourth Amendment seeks to protect, which is vastly different than impersonal property, such as a vehicle, that does not require reasonable suspicion for a search. *Cotterman*, 709 F.3d at 964. The nature of electronic devices and the "attendant expectation of privacy" are the determining factors for the reasonableness of the search. *Id*. A car completely

filled with sensitive documents could not come close to holding the number of documents that can be stored within an electronic device. *Id.* Electronic devices also keep information beyond the user's deletion of it, making it impossible for the user to determine what information will be subjected to a border search. *Id*. Because a forensic search can find even these "deleted" files, it is the same as a border agent being able to search a bag for its contents and all the contents it has ever carried. *Id*. at 965. Differences in property must be accounted for during searches at the border. *Id*. While searches of vehicles have little implication after the search, the exposure of confidential information on an electronic device cannot be undone. *Cotterman*, 709 F.3d at 964. International travelers may expect their property to be searched at the border, but they do not expect agents to "mine every last piece of data on their devices." *Id*. at 967. Therefore, requiring reasonable suspicion to conduct a forensic search of an electronic device will provide for travelers' privacy and will not impede the ability to secure the border. *Id*. at 966.

Given how many electronic devices of Mr. Escaton were searched forensically, his entire life was subjected to Special Agent Cullen's pervasive eyes. Effectively, Special Agent Cullen read through every page of Ms. Escaton's electronic diary. While it is true that Special Agent Cullen found documents on the laptop containing bank account numbers and pin numbers, the record also states she found no incriminating information on the hard drives. (R. at 1343). However, the record is silent as to what information about Mr. Escaton's personal life she had access to during the several hours it took to scan the devices. Mr. Escaton was carrying three external hard drives with him when crossing the border, all of which were forensically searched. (R. at 1343). External hard drives are used solely to hold information, typically vast amounts. Details of Mr. Escaton's familial, political, or sexual decisions were all potentially subjected to scrutiny while Special Agent Cullen scanned his devices. Moreover, the other information on Mr. Escaton's laptop could yield even more intimate details of his personal life.

Like the court in *Cotterman*, this Court should find that the nature of electronic devices and the "attendant expectation of privacy" are the determining factors for reasonableness of a forensic search. *Cotterman*, 709 F.3d at 964. As the court pointed out in *Cotterman*, these devices can retain information far longer than the user realizes. Special Agent Cullen had access to not only the current information on the devices, but also any deleted information. Additionally, the record is silent as to whether Special Agent Cullen also conducted the forensic search while disconnected from wireless services. Therefore, had the devices been connected to wireless service, the information that could be gathered on Mr. Escaton is virtually limitless. Like *Montoya de Hernandez*, where this Court found that an internal search required reasonable suspicion, a forensic search is an internal search into all the private, intimate details of a person's life and should also require reasonable suspicion. *Montoya de Hernandez*, 473 U.S. at 541.

D. Evolving technology creates a need for reasonable suspicion prior to conducting a forensic search.

A cell phone is fundamentally different than containers such as wallets and bags traditionally subjected to government search. *Riley*, 134 S. Ct. at 2489. In *Riley*, the police made a stop and subsequently arrested Riley. *Id*. at 2480. During a search incident to the arrest, the officer found gang related items and Riley's cell phone, which he seized and searched. *Id*. This Court ultimately held that police may not search a cell phone without a warrant as a search incident to arrest. *Id.* at 2485. The immense storage capacity of cell phones distinguishes it from other items found upon an individual during an arrest and creates a privacy problem, as a search gives the searcher a complete picture of the owner's life. *Id*. at 2489. Additionally, the information held on a cell phone can allow for the reconstruction of an individual's private life. *Id*. The information can date back to the purchase of the phone, which could be many years' worth of information. *Riley*, 134 S. Ct. at 2489. Cell phones are pervasive in today's society, which means they have the potential to reveal the most intimate details of their users' lives. *Id*. at 2490. Furthermore, even the

apps on a cell phone can reveal a "montage" of the user's life. *Id*. Technology holds the intimate details of the user's life but the fact that this information can now be carried "in [his] hand does not make the information any less worthy of the protection for which the Founders fought." *Id*. at 2495.

Lastly, a requirement of reasonable suspicion prior to conducting a forensic search of an electronic device would be in line with what is required by the Department of Homeland Security. *See* U.S. CUSTOMS AND BORDER PROT., CBP DIRECTIVE NO. 3340-049A, BORDER SEARCH OF ELECTRONIC DEVICES (2018) (hereinafter "Directive"). Section 5 of the Directive discusses the procedures for border searches. *Id*. First, the officer must not access any information that may be stored remotely by turning the device on airplane mode. *Id*. Futhermore, there are two types of searches, a "basic search" and an "advanced search." *Id*. *Id*. An advanced search is "any search in which an Officer connects external equipment, through a wired or wireless connection, to an electronic device." *Id*. The basic search is defined by not being an advanced search and can be performed with or without suspicion. *Id*. Additionally, an "advanced search" includes reviewing, copying, or analyzing the contents on the device. *Id*. An officer may conduct an "advanced search" when there is reasonable suspicion. *Id*. Reasonable suspicion has many factors, such as "the existence of a relevant national security-related lookout in combination with other articulable facts." *Id.*

Here, it is clear that Special Agent Cullen conducted what is described as an "advanced search" by using forensic software to search Mr. Escaton's electronic devices. (R. at 1343). Therefore, Special Agent Cullen, pursuant to the Directive, should have had reasonable suspicion before conducting the search. There were no articulable facts shown in the record indicating that Special Agent Cullen nor Officer Stubbs had reasonable suspicion to conduct the forensic search. (R. at 1342-43). Under the Directive's guidelines, the forensic search should not have happened.

An internal search of an individual's body requires reasonable suspicion, due to the invasiveness of the search. Given the pervasiveness and usage of electronic devices, a search of one reveals so much of an individual's private life as to be invasive. Thus, a forensic search of an electronic device is comparable to an internal search of an individual's body and requires reasonable suspicion for the search.

II. THE GOVERNMENT'S ACQUISTION OF THREE-DAY RECORDS, WEEKDAY RECORDS, AND TOWER DUMPS WERE NOT SUPPORTED BY PROBABLE CAUSE AND THUS AMOUNT TO AN UNLAWFUL SEARCH UNDER THE FOURTH AMENDMENT.

If this Court reaches the issue, it should hold that warrants were required to conduct the searches for Mr. Escaton's cell site location information (CSLI) based on the normative principals announced by this Court in *Carpenter v. United States*, 138 S. Ct. 2206 (2018).[15] The Fourteenth Circuit held – and the Government argues – that a warrant need only be sought to acquire CSLI for more than seven-days or 168 hours. *Escaton v. United States*, 1001 F.3d 1341, 1350-54 (14th Cir. 2021). If the Court were to accept this argument, law enforcement will be gifted the capability to discover an individual's most personal information at a standard less than what is constitutionally required. *See Escaton*, 1001 F.3d at 1356 (Weber, J., dissenting) (arguing that the majority's holding would allow the Government to request one hour of CSLI a day for 168 days); *see also Carpenter*, 138 S. Ct. at 2221. That sweeping proposition is irreconcilable with Fourth Amendment requirements; thus, this Court must find the CSLI acquired here contravened Mr. Escaton's reasonable expectation of privacy.

[15] A finding that Officer Stubs' and Special Agent Cullen's search at the border contravened Mr. Escaton's Fourth Amendment rights would mean that the Government's request for CSLI under the SCA did not rest on specific and articulable facts and thus improper even under the lesser standard. 18 U.S.C §2703(d).

A. Cell site location information is by default subject to the warrant requirement.

An individual maintains a legitimate expectation of privacy in his historical location data such that "the Government must obtain a warrant supported by probable cause before acquiring" CSLI. *Carpenter*, 138 S. Ct. at 2217-21. Under this Court's longstanding test, government agents engage in a Fourth Amendment search when they intrude on an expectation of privacy that society is prepared to recognize as reasonable. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). The Court affirmed this test in *Carpenter,* finding that petitioner had a reasonable exception of privacy in his CSLI and the Government should have sought a warrant if it wished to acquire such data. *Carpenter*, 138 S. Ct. at 2220-21. *Carpenter* drew a clear line that CSLI should by default be subject to the warrant requirement due to its precision, indiscriminate nature, low acquisition cost, and intrusiveness. *See id*. at 2216-20.

The Court in *Carpenter*, although not explicitly, announced a multi-factor analysis that must be considered when questions concerning acquisition of CSLI arise. The Court expressed concerns about "CSLI [] rapidly approaching GPS-level precision." *Id*. at 2219. Cell site location information has the potential to retrospectively reveal an individual's exact location by effectively surveilling him "every moment of every day for [] years." *Id*. at 2218. The threat of the Government acquiring precise historical location data without a warrant was an irreconcilable proposition to the Court in *Carpenter*. *Id*. at 2218-21.

The Fourth Amendment was in part inspired to prevent the indiscriminate nature of the King's assignment of general warrants and writs of assistance. *See* Henry F. Fradella et al., *Quantifying Katz: Empirically Measuring "Reasonable Expectations of Privacy" in the Fourth Amendment Context*, 38 AM. J. CRIM. L. 289, 326–27 (2011). Comparably, CSLI "is continually logged for all of the 400 million devices in the United States — not just those belonging to persons who might happen to come under investigation." *Carpenter*, 138 S. Ct. at 2217. This data will

indiscriminately reveal innocent information which should reasonably be expected to remain private. In accord with the Framers ideas, the "all-encompassing" nature of CSLI requires that the warrant be obtained when the requested data has the potential to indiscriminately reveal private information. *Id*.

Further, CSLI is relatively inexpensive and easy to obtain under 18 U.S.C. § 2703(d) of the SCA. The Court in *Carpenter* expressed concern about these truths, stating that CSLI is "remarkably easy, cheap, and efficient compared to traditional investigative tools." *Id*. at 2218. The ease at which CSLI can be obtained under the SCA allows the Government to request private historical location data with limited resources and evidence offered in support of such a request. *Id.*

The Court's biggest concern was the potential intrusiveness of CSLI disclosed to the Government pursuant to its requests under 18 U.S.C. § 2703(d) of the SCA. Under the SCA the Government is given free rein to discover information about an individual's family, politics, religion, health, profession, and intimate partners. *See id.* at 2217. When requested CSLI has the potential to disclose "deeply revealing" information about an individual's private life it must be considered so intrusive as to be subject to the warrant requirement. *See id.* at 2217 (cautioning against the Government being allowed "an intimate window into a person's life" without satisfying the warrant requirement).

The Government's acquisition of Mr. Escaton's CSLI through 18 U.S.C. § 2703(d) of the SCA fell "well short of the probable cause required for a warrant." *Carpenter*, 138 S. Ct. at 2221. When this Court is asked to determine whether an individual has a reasonable expectation of privacy in his data it considers the degree to which that data may potentially reveal intimate details about his private life. *See, e.g., Riley v. California*, 134 S. Ct. 2473, 2490 (2014); *United States v. Jones*, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring); *Kyllo v. United States*, 533 U.S. 27, 34-36 (2001); *United States v. Karo*, 468 U.S. 705, 715 (1984). The potential for the requested

CSLI at issue to reveal a substantial amount of Mr. Escaton's private life indicates that the Government should have complied with the warrant requirement. Acquisition of CSLI at any lesser standard would contravene Mr. Escaton's Fourth Amendment rights.

1. **Mr. Escaton's legitimate expectation of privacy was contravened because the Government was supplied an intimate window into his personal life through the cell site location information it acquired without satisfying the warrant requirement.**

The Government's acquisition of Mr. Escaton's historical movement through CSLI violated his Fourth Amendment rights due to its potential to provide the Government an intimate window into his personal life at a standard less than what is constitutionally required. *See Carpenter*, 138 S. Ct. at 2217. This Court has made a particular effort to protect individuals' Fourth Amendment rights when threatened with advancing technology employed by law enforcement. *See, e.g., id.* at 2217; *Kyllo,* 533 U.S. at 36 (extending Fourth Amendment protection to use of a thermal imaging camera to observe heat emanating from a house); *Jones*, 565 U.S. at 430 (2012) (Alito, J., concurring in the judgment) (individuals, even in the public sphere, have a reasonable expectation of privacy in their GPS location); *Riley*, 134 S. Ct. at 2490 (requiring a warrant to search contents of cell phones seized incident to arrest in order to preserve degree of privacy enjoyed). Here, each of the Government's three separate requests for Mr. Escaton's CLSI under the provisions enumerated in 18 U.S.C. § 2703 of the SCA likely violated *Carpenter*, however, when considered together there is no doubt that his Fourth Amendment rights were violated.

The Government's acquisition of Mr. Escaton's weekday records violated his Fourth Amendment rights because it had the potential to provide a detailed mosaic of his personal life in contravention of his reasonable expectation of privacy. The standard at which CSLI is acquired should be dictated by the normative understandings that underline *Carpenter*. 138 S. Ct. at 2216-20; *see also United States v. White*, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting) (arguing that *Katz* requires a normative judgement on what should be labeled as private). Acquisition of CSLI for

a ten or even two-day period should be predicated on the potential for the requested information to reveal "familial, political, professional, religious, and sexual associations," not a bright line rule. *Id.* at 2217 (quoting *Jones, 565 U.S. at 415 (2012)* (Sotomayor, J., concurring)); *see also Riley*, 134 S. Ct. at 2490 (declining to announce a bright line rule relating to Fourth Amendment searches in the digital age). Here, the Government's request of Mr. Escaton's year old weekday records provided an intimate view into his day-to-day life particularly because it was tailored to reveal moments relevant to his private life.

Individuals are more likely to participate in their most intimate encounters during business hours from Monday to Friday. We are more prone to the engage in encounters with family, doctors, or political organizations during weekday business hours because that is generally the time when people are most active. Accordingly, any request for CSLI made by the Government specifically tailored to learn the movements of an individual during these hours over an extended period of time should be treated with extreme sensitivity. Here, the Government's weekday record request was potentially more detrimental than a request for a continuous 100 hours of CSLI because it allowed the Government to track Mr. Escaton over an extended period when he was more likely to reveal details about his private life.

While the Government's three-day request may facially be within the bounds of *Carpenter*, it nonetheless violated Mr. Escaton's Fourth Amendment rights due to the precision at which it relayed his location. Due to the numerous cell sites in Sweetwater, the Government was supplied with "near perfect surveillance" of Mr. Escaton's location for a seventy-two-hour period. *Escaton*, 1001 F.3d at 1355 (Weber, J., dissenting) (quoting *Carpenter*, 138 S. Ct. at 2218). The Government also had knowledge that Mr. Escaton was in Sweetwater for the requested time period, yet still declined to get a warrant despite knowing that they would be provided with Mr. Escaton's precise location history in Sweetwater pursuant to its request. (R. at 1345; Hale Aff. ¶¶ 11, 20) (Special

Agent Hale was aware that Mr. Escaton was in Sweetwater from October 11-13 due to the previously requested tower dumps, and was aware of the high amount of cell towers in Sweetwater). The Government was reckless in its requests for Mr. Escaton's three-day records as it gave no regard to the warrant requirement despite knowing the likely sensitivity of the information to be relayed.

The three Sweetwater tower dumps should have been subject to the warrant requirement because of their potential to precisely reveal Mr. Escaton's "familial, political, professional, religious, and sexual associations." *Carpenter*, 138 S. Ct. at 2217 (quoting *Jones, 565 U.S. at 415 (2012)* (Sotomayor, J., concurring)). In total, the three tower dumps amounted to a modest one-hour worth of information. (R. at 1343). However, it is the precision and potential intrusiveness of the acquired CSLI to wit the *Carpenter* Court was concerned. 138 S. Ct. at 2217-19. Sweetwater is populated with enough cell towers to pinpoint what floor or even room an individual is located. (Hale Aff. ¶ 11). The request for these tower dumps and the precision at which they were relayed is even more troubling when coupled with the fact that the Government had little to no nexus between Mr. Escaton and the crimes alleged. (R. at 1344; Hale Aff. ¶ 19) (the Government was merely aware of similar malware and a suspicious man loitering around the skimmed ATMs). These facts do not supply the requisite probability that Mr. Escaton was involved with criminal activity. *See Illinois v. Gates*, 462 U.S. 213, 235 (1983) (holding for the probability requisite to conduct a search). This type of fishing expedition is not permitted under "intermediate standard" enumerated in 18 U.S.C. § 2703(d), let alone the heightened requirements of the Fourth Amendment. H.R. REP. NO. 827, 103d Cong., 2d Sess. Pt. 1, at 31 (1994) (noting that the Section 2703(d) standard was intended to "guard against 'fishing expeditions' by law enforcement" while allowing access only in appropriate circumstances).

The Government's use of the SCA allowed them easy access to a breathtaking amount of data gathered on Mr. Escaton over a vast spectrum of time in contravention of his reasonable expectation of privacy. The Fourteenth Circuit held that the Government's acquisition of CSLI did not contravene Mr. Escaton's reasonable expectation of privacy because the 152 requested hours were within the bounds of *Carpenter's* narrow holding. *Escaton*, 1001 F.3d at 1350-54. However, the Court in *Carpenter* noted "[i]t is *sufficient for our purposes today to hold that accessing seven days* of CSLI constitutes a Fourth Amendment search." 138 S. Ct. at 2217 n.3 (emphasis added). In fact, this Court routinely declines to prescribe mechanical Fourth Amendment rules. *Id.* ("We need not decide whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be."); *Kyllo*, 533 U.S. at 35 (the Court declined to announce a mechanical interpretation of the Fourth Amendment because doing so would leave reasonable expectations of privacy "at the mercy of advancing technology."). The refusal to announce mechanical Fourth Amendment rules should be taken as tacit invocation that the application of the warrant requirement for CSLI is dependent upon the sensitivity of the information, not the amount at which it is requested.

Affirming the Fourteenth Circuit would allow the Government to "reconstruct someone's specific movements down to the minute" without a warrant over an extended period of time, so long as the request remains within a rigid set of parameters. *See Riley*, 134 S. Ct. at 2490. The logical end to this holding is the creation of a legal matryoshka doll; whereby the government would be allowed to incrementally request CSLI as permitted by a set threshold until the total requests amounted to a detailed mosaic of an individual's private life. The Government utilized this tactic – making individual requests for Mr. Escaton's CSLI that together amounted to a detailed window into his personal – in contravention of his of his Fourth Amendment rights.

2. The Government's acquisition of Mr. Escaton's cell site location information was unlawful pursuant to the plain language of *Carpenter v. United States*, 138 S. Ct. 2206 (2018) and should have been subject to the Fourth Amendment's Warrant Requirement.

The Government's acquisition of eleven days-worth of CSLI, at a standard less than probable cause, violated Mr. Escaton's Fourth Amendment right pursuant to this Court's holding in *Carpenter*. 138 S. Ct. at 2217 n.3 ("accessing seven days of CSLI constitutes a Fourth Amendment search."). This Court was clear in *Carpenter* to hold that accessing "*seven days*" of CSLI constitutes a search, and thus is subject to the warrant requirement. *See id.* (emphasis added). At no point has this Court suggested that law enforcement may attempt substitute the stated seven day threshold for 168 hours. Despite this clearly defined threshold, the Government made three invalid requests for Mr. Escaton's year old CSLI; one request alone demanding Mr. Escaton's CLSI over a ten-day period. In total, the Government acquired eleven days of Mr. Escaton's personal location history. The Government's request and subsequent acquisition of Mr. Escaton's CSLI were outside the parameters of already established law, thus violating his legitimate expectation of privacy in his historical location data.

Alternatively, this Court should not accept the Fourteenth Circuit's erroneous interpretation of *Carpenter's* holding given its potential to be taken advantage of by clever law enforcement. The Fourteenth Circuit read into *Carpenter* that 168 hours-worth of CSLI is allowable even if it were to span over weeks or months. *See Escaton*, 1001 F.3d at 1343. This interpretation is not only inconsistent with the plain language of *Carpenter*, but invites Government action that would be inconsistent with Fourth Amendment principles. *See id*. at 1356 (Weber, J., dissenting); *see also Carpenter,* 138 S. Ct. at 2217 n.3.

A pillar of the Fourth Amendment is "to place obstacles in the way of a too permeating police surveillance." *Id*. at 2214 (quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)). Here, the Government's ability to work around *Carpenter's* narrow holding amplifies the need for an

obstacle to be in the way of creative law enforcement. The Fourteen Circuit rejected the idea of further defining the boundaries of *Carpenter*, as it may cause the judiciary to repeatedly answer the same questions surrounding the acquisition of CSLI. *Escaton*, 1001 F.3d at 1351-52. However, the opposite is true; this Court should feel persuaded to dispense with the ambiguity lower courts have created, and likely will create in light of *Carpenter*, in an effort to prevent cumulative judicial labor on issues like the one at bar. This Court should affirm the precedence set by *Carpenter* and find that "no Warrants shall issue, but upon probable cause" when the Government attempts to acquire potentially sensitive CSLI. U.S. CONST. amend. IV.

3. Because the Fourteenth Circuit did not decide whether the good faith exception to the exclusionary rule applies, this case presents a clean vehicle for this Court to consider the issue at bar.

This Court should not consider whether application of the good faith exception to the exclusionary rule applies, but rather leave that task for the court of appeals on remand. The issue at bar presents a question of public importance that must be resolved despite any good-faith action by the Government to adhere to the provisions of the court-order for CSLI. *See Illinois v. Krull*, 480 U.S. 340, 347 (1987) (application of the exclusionary rule is restricted to only those circumstances where its remedial purpose is effectively advanced.) This Court should only consider the issues raised on appeal and decline to consider whether the Government's officers acted in good faith in order to refine Fourth Amendment precedence. *See Davis v. United States*, 564 U.S. 229, 247 (2011) ("[T]he good-faith exception in this context will not prevent judicial reconsideration of prior Fourth Amendment precedents.").

Application of the good faith exception to the exclusionary rule would effectively insulate most decisions by law enforcement to obtain CSLI without seeking a warrant from appellate review. Simply, if the good-faith exception were to apply "the government would be given carte blanche to violate constitutionally protected privacy rights, provided, of course, that a statute [or

court order] supposedly permits them to do so. The doctrine of good-faith reliance should not be a perpetual shield against the consequences of constitutional violations." *United States v. Warshak*, 631 F.3d 266, 282 n.13 (6th Cir. 2010).

B. Any excessive narrowing of *Carpenter v. United States*, 138 S. Ct. 2206 (2018) will negate Fourth Amendment protection to a wide array of privacy interests in a digital age.

"It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology." *Kyllo*, 533 U.S. at 33-34. This Court has attempted to keep pace with the unavoidable march of technological progress by adapting Fourth Amendment protections. *See, e.g. id*. at 36*; Jones*, 565 U.S. at 430 (Alito, J., concurring); *Riley*, 134 S. Ct. at 2490; *Carpenter*, 138 S. Ct. at 2217-21. This Court should follow its precedence to ensure that Fourth Amendment protections adapt contemporaneously with the concerns that may arise from digital progress. *See Packingham v. North Carolina*, 137 S. Ct. 1730, 1736 (2017) ("courts must be conscious that what they say today might be obsolete tomorrow."). It is thus important that this Court not craft a mechanical Fourth Amendment prescription concerning the acquisition of CSLI in order to preserve the flexibility necessary to address future digital privacy concerns. *See Kyllo*, 533 U.S. at 35 (declining to announce a "mechanical interpretation of the Fourth Amendment.").

C. Potential Congressional action is irrelevant here.

"It is emphatically the province and duty of the judicial department to say what the law is." *Marbury v. Madison*, 5 U.S. 137, 153 (1803). The Fourteenth Circuit argued that courts are wise to defer to congress to determine the appropriate standards relating to the Government's acquisition of CSLI. *Escaton*, 1001 F.3d at 1352. While this sentiment does come with some wisdom, the judicial department may not relinquish their duty to decide "what the law is." *Marbury*, 5 U.S. at 153. Where individuals' rights and freedoms are threatened by too permitting police powers, it is the

Court's responsibility to curb those powers. *See Di Re*, 332 U.S. at 595.

Congressional action concerning too permitting police powers is not new and does not absolve the courts of their responsibility. As Justice Alito chronicled in *Jones*, Congress instituted legislation curbing the Government's ability to wiretap following the Court's opinion in *Katz*. 565 U.S. at 427 (2012) (Alito, J., concurring). However, the fact that Congress promulgated rules concerning wiretapping did not prevent the Court from subscribing to and developing the longstanding principles encompassed within *Katz*.

Further, previous attempts by Congress to adequately address issues concerning the acquisition of CSLI under the SCA have routinely failed. *See, e.g.*, Email Privacy Act, H.R. 699, 114th Cong. (2015) (House passed by a unanimous vote, but the Senate never considered the bill). Recently, Congress recognized the sensitivity of CSLI in the Telecommunications Act. 47 U.S.C. § 222(f). However, that recognition cannot be considered meaningful as serious issues, such as the one at bar, are want to continually appear under current law. This Court should decline being a passive onlooker to Congress's frequent attempts to update the SCA. Absent meaningful legislation, this Court should feel compelled to enforce the requirements of the Fourth Amendment by preserving the reasonable expectation of privacy that Americans have long enjoyed in the details of their location over a significant amount of time.

CONCLUSION

For the foregoing reasons, Petitioner requests this Court REVERSE the Fourteenth Circuit's decision denying Petitioner's motion to suppress on both grounds.

Dated: February 10, 2019

Respectfully Submitted,

Attorneys for Petitioner