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 THE PETITIONER

TEAM P1

Counsel for Petitioner

TABLE OF CONTENTS

TABLE OF AUTHORITIES

QUESTIONS PRESENTED

I. Whether Agent Stubbs' suspicionless search of Petitioner's electronics at the nation's border violates the Fourth Amendment's prohibition of unreasonable search and seizure

II. Whether Agent Hale's multiple requests for Petitioner's historical cell-site location information (CSLI) and three tower dumps violate the Fourth Amendment's prohibition against warrantless searches considering this Court's holding in *Carpenter v. United States*, 133 S.Ct 2206 (2018).

OPINIONS BELOW

The opinion of the Fourteenth Circuit is reported at 1001 F.3d 1341. The district court opinion is unpublished.

CONSTITUTIONAL PROVISIONS AND RULES

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

> 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 relevant section of the Stored Communications Act, 18 U.S.C. § 2703, provides:

(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

This is a case that asks how emerging technology – laptop computers, large-scale storage devices, cell phones, etc. – that is being used by virtually all members of society in some form will be protected under the Fourth Amendment. On the one hand, the government has a compelling interest in gaining access to these devices as one of the greatest advances in criminal punishment in American history. On the other, private citizens have virtually all aspects of their life on these devices: financial, political, social, and on. The government should not have carte blanche to destroy one of the final vestiges of personal privacy – upon which the spirit of the Fourth Amendment rests – regardless of where or how this intrusion takes place.

Petitioner Hector Escaton had his Fourth Amendment rights violated when his electronic devices were seized and searched at the U.S.-Mexico border without a warrant, probable cause, or reasonable suspicion. This Court has recognized that electronic information is fundamentally different than traditional means of storage, and as such is subject to different protections under the Fourth Amendment. Because Petitioner's devices were searched without reasonable suspicion, it was in violation of the Fourth Amendment, and his motion to suppress should have been granted.

Petitioner's Fourth Amendment rights were also violated by the warrant-less collection of Cell-Site Location Information. The level of intrusion in collection a person's location at all hours for a certain number of days – of which they have a reasonable expectation of privacy – requires that the Government obtain a warrant to access this information. Petitioner had an expectation of privacy in his movements, and using his cell phone as a tracking device was in violation of the Fourth Amendment.

In both issues, the Government violated Petitioner's Fourth Amendment protections. Petitioner respectfully asks that this Court overturn the decision of the Fourteenth Circuit, and instruct the trial court to grant his motion to suppress.

STATEMENT OF THE CASE

Petitioner Hector Escaton, a citizen of the United States and the state of West Texas, lawfully crossed the border from Mexico into the United States. His vehicle was searched by agents of the United States Customs and Border Patrol, and the events that followed led to his arrest on charges of Bank Fraud, contrary to 18 U.S.C. § 1344; Conspiracy to Commit Bank Fraud, contrary to 18 U.S.C. § 1349; and Aggravated Identity Theft, contrary to 18 U.S.C. § 1028A.

A. THE INITIAL BORDER CROSSING AND SEARCH

On September 25, 2019, Petitioner Escaton returned to the United States from Mexico through a border checkpoint in West Texas. (R. at 2). At the checkpoint, Escaton was stopped and had his vehicle searched by an agent of Customs and Border Patrol. (R. at 2). The agent, upon searching the vehicle, came upon three pieces of Escaton's luggage. (R. at 2). Escaton was carrying several pieces of electronic equipment, including an Apple iPhone, a laptop, three hard drives, and four Universal Serial Bus (USB) storage devices.[1] (R. at 3). The agent seized the iPhone and, in order to keep the phone from connecting to the Internet, placed the iPhone in airplane mode.[2] (R. at 3). He took the same steps with the laptop, preventing it from connecting

[1] A USB storage device is substantially similar to an external hard drive in function, though typically with far smaller storage capacity.
[2] "Airplane mode" is a mode which disables a phone's Internet connectivity; so named because airplane passengers are regularly asked to disconnect all electronic devices from internet and cellular services.

to the internet. (R. at 3). He then searched both devices, manually going through files and other information stored on the devices. (R. at 3). The agent also copied a personal note Escaton had placed on the bottom half of the laptop, below the keyboard, which read "Call Delores (201) 181-0981." (R. at 3). The iPhone was returned, but the agent seized the laptop and storage devices, and attempted to access files on the laptop and devices, which were password protected. (R. at 3). At this point, the only information that the agent had was that Escaton – a U.S. citizen – was crossing from Mexico to the United States, and had these electronics in his possession. The agent retained the laptop and devices and delivered them to a Computer Forensic Examiner with United States Immigration and Customs Enforcement. (R. at 3). Still armed with only the knowledge of Escaton's possession of these items, the Examiner ran sophisticated forensic software to force decryption of the files of the laptop, and discovered documents containing banking information. (R. at 3). She then relayed her findings to the original Border Patrol agent, who notified the FBI of the decrypted data obtained. (R. at 3).

B. SUBSEQUENT INVESTIGATION AND ARREST

After being notified of the data seized from Escaton's electronics, the FBI began to investigate connections to that data. An investigation into ATM skimming was already underway on behalf of Mariposa Bank's Sweetwater and Escalante branches, which had recently been affected by skimming. (R. at 3). Mariposa Bank is large national chain that operates several branches in Sweetwater, a city in West Texas, and Escalante, a smaller suburb. (R. at 4). While there was forensic evidence of the skimming techniques used, as well as surveillance footage of an unidentified person, the investigation had as yet yielded no leads, let alone suspects. (R. at 4).

Even so, the FBI – in coordination with the U.S. Attorney for the District of West Texas – requested authorization for three cell tower "dumps" for periods during which the unidentified

person was near the banks in question. (R. at 4). A cell tower dump, essentially, compels tower operators to provide all cell phone numbers registered near a tower at a particular time. It was at this late stage that investigators discovered their first connection between the ATM skimming and Escaton: his phone number showed up as one of the hundreds acquired from the tower dump. (R. at 5). The investigators then requested and were granted an order compelling Escaton's cell service provider to provide them with Escaton's cell phone records. (R. at 5). Those records placed Escaton in the general area of one of the Sweetwater Mariposa ATM's during the time the skimming was thought to have occurred. (R. at 5).

The records did not place Escaton near any of the Escalante Mariposa ATM's during that time. (R. at 5). Investigators then turned to another piece of personal property seized from Escaton at the border – the note containing Delores' cell phone number. The FBI and U.S. Attorney again asked and were granted cell location data, this time for "Delores," who – as a result of these records requested from Escaton's note – was revealed to be Delores Abernathy. (R. at 5). Not only did the records reveal Abernathy's name, they also contained more than 100 hours of location information – the investigators' attempt to hit the proverbial bullseye with a shotgun. (R. at 5). Abernathy, who had previously been convicted of similar crimes, was arrested and accepted a plea deal in return for testifying against Escaton. (R. at 5-6).

C. PROCEEDINGS BELOW

Escaton was indicted in the District Court for the District of West Texas for Bank Fraud, Conspiracy to Commit Bank Fraud, and Aggravated Identity Theft. (R. at 6). Before the trial, Escaton moved to suppress the evidence obtained from both the forensic search of the seized electronics and the cell-site data. (R. at 6). The trial court denied the motion on both issues. (R. at 6). Escaton was convicted on all charges, and subsequently appealed to the Court of Appeals for

the 14th Circuit, alleging error in the trial court's denial of the motion to suppress. (R. at 6). The 14th Circuit affirmed the decision to deny the motion. (R. at 6). The 14th Circuit relied primarily in the reasoning in *United States v. Touset*, 890 F.3d 1227 (11th Cir. 2018) in finding that "no reasonable suspicion" is necessary for a forensic search at a border crossing, and primarily on the test outlined in *Carpenter v. United States*, 585 U.S. ___ (2018) (slip op.) in so affirming. (R. at 6).

ARGUMENT

I. ALTHOUGH THE GOVERNMENT IS GIVEN MUCH GREATER LATITUDE FOR SEARCHES AT AN INTERNATIONAL BORDER, THE SEARCH OF PETITIONER'S ELECTRONIC DEVICES WAS IN VIOLATION OF THE FOURTH AMENDMENT PROHIBITION OF ILLEGAL SEARCH AND SEIZURE.

It is well-settled that the government is afforded a much less stringent standard of unreasonableness under the Fourth Amendment's protection against "unreasonable searches and seizures" when the search in question takes place at an international border. However, that protection is not completely destroyed simply by virtue of the geographic location of the search. In this case, the government violated that Fourth Amendment protection by conducting an unreasonable search and seizure of the information stored on Petitioner's electronic devices, leading to his arrest and conviction. The Fourth Amendment is violated at the border (1) when a substantial intrusion of personal privacy and dignity occurs without reasonable suspicion; or (2) when the search amounts to an "extended border stop." In either of these situations, reasonable suspicion is required. Here, the search of Petitioner's electronic devices was a substantial invasion of his personal privacy and dignity without reasonable suspicion; and the stop was extended by virtue of the defendant having passed the cursory scan and having been admitted

into the country. For these reasons, the 14th Circuit was in error, and the trial court should be instructed to grant Petitioner's motion to suppress.

A. THE FORENSIC EXAMINATION OF PETITIONER'S DEVICES WAS SO SUBSTANTIAL AND INVASIVE THAT IT REQUIRED REASONABLE SUSPICION, WHICH WAS ABSENT.

The forensic examination of Escaton's laptops and USB devices was such an intrusion on his privacy because of the inherent nature of electronic storage devices that the search was in violation of the Fourth Amendment due to the lack of reasonable suspicion during the stop – despite the fact that it happened at the border.

This Court has repeatedly held that "searches made at the border … are reasonable simply by virtue of the fact that they occur at the border." *United States v. Ramsey*, 431 U.S. 606, 616 (1977). However, it also left the door open to the possibility that some border searches require some higher standard of suspicion in order to conform with the Fourth Amendment. *United States v. Flores-Montano*, 541 U.S. 149, 156 (2004) (holding that a particularly destructive search of property may require some level of suspicion). The widespread adoption of electronic devices has caused some consternation in this settled jurisprudence, however, saying modern electronics "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Riley v. California*, 573 U.S. ___ (2014) (slip op., at 20). 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. "The ultimate touchstone of the Fourth Amendment is reasonableness." *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006). That reasonableness is generally determined "by assessing, on the one hand, the degree to which [the search] intrudes upon an individual's privacy, and, on the other, the degree to which it is

needed for the promotion of legitimate governmental interests." *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999).

The opening left by this Court in *Flores-Montano* has given rise to differing opinions on how this technology, unimaginable in the time of the Founders, affects the protections offered by the Fourth Amendment. The Fourth and Ninth Circuits have both upheld a standard of reasonable suspicion for a border search of electronic information where it was able to be found by a mere cursory examination. *See United States v. Kolsuz*, 890 F.3d 133 (4th Cir. 2018) *and United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013).

In *Cotterman*, the defendant was charged and convicted as the result of a search of his electronic devices after crossing into the United States from Mexico in Arizona. *Cotterman*, 709 F.3d at 957-58. The evidence which would eventually prove incriminating was found in password-protected files that were accessed by a forensic specialist employed by U.S. Immigration and Customs Enforcement at a major city away from the border. *Id.* at 958. The Ninth Circuit said that "[i]t is the comprehensive and intrusive nature of a forensic examination – not the location of the examination – that is the key factor triggering the requirement of reasonable suspicion," in holding that "the forensic examination of [defendant's] computer required a showing of reasonable suspicion." *Id.* at 962 *and id.* at 968. The court went so far as to hold that a forensic search of a computer at the border is "a substantial intrusion upon personal privacy and dignity," and that forensic searches must be accompanied by reasonable suspicion. *Id.* at 968. The court reasoned that the "papers" protected from unreasonable search by the Fourth Amendment included those digital papers now maintained by virtually all members of society in electronic devices. *Id.* This reasoning follows this Court's reasoning in *Riley* – namely that before the introduction of these modern, massive storage devices, a Fourth Amendment

exception search "was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy." *Riley*, 573 U.S. at ___ (slip op., at 34). This Court went on to say that "the possible intrusion on privacy is not physically limited in the same way when it comes to cell phones," and went on to list several concerns that are now present when considering searches of electronic devices (*Riley* was concerned primarily with cellular phones, but the reasoning is applicable to all modern electronic storage devices):

> "First, a cell phone collects in one place many distinct types of information – an address, a note, a prescription, a bank statement, a video – that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs … the same cannot be said of a photograph tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. … Finally, there is an element of pervasiveness that characterizes cell phones but not physical records. Prior to the digital age, people did not typically carry a cache of sensitive information … Allowing the police to scrutinize such records on a routine basis is quite different from allowing them to search a personal item or two in the occasional case."

Id. (slip op., 35-37). In short, this Court held that because of the inherent nature of electronic information, traditional Fourth Amendment jurisprudence is inapplicable: "The United States asserts that a search of all data stored on a cell phone is 'materially indistinguishable' from searches of these sorts of physical items. That is like saying a ride on horseback is indistinguishable from a flight to the moon." *Id*. (slip op., at 33). It is clear that the jurisprudence of this court is to treat traditional property from electronic property.

While the Fourth and Ninth Circuits have both recognized this Court's different treatment of electronic information, the court below relied on *United States v. Touset*, 890 F.3d 1227 (11th Cir. 2018). In *Touset*, the facts are materially similar to *Cotterman*, but with the defendant arriving to the U.S. via plane rather than automobile. *Id.* In *Touset*, the 11th Circuit mischaracterizes the holdings of this Court: "The Supreme Court has never required reasonable

suspicion for a search of property at the border, however non-routine and intrusive, and neither have we." *Id.* at 1233. While technically true, this Court has chosen to leave an opening for possible unreasonable searches, particularly for "extended border searches" (*see, e.g., United States v. Montoya de Hernandez*, 473 U.S. 531 (1985)), or for "highly intrusive searches," (*Flores-Montano*, 541 U.S. at 152). Clearly, this Court envisioned a border search that would require reasonable suspicion.

Further, the court in *Touset* unnecessarily expanded their holding beyond the question raised on appeal. The parties at trial "agreed that the government 'needed reasonable suspicion of criminal activity in order to lawfully detain for further analysis and search [Touset's] electronic devices." *Touset*, 890 F.3d at 1231. The parties only disagreed that there was reasonable suspicion, as defendant argued that the specific knowledge used to justify the reasonable suspicion was "stale." *Id.* Even though there was no controversy over whether reasonable suspicion was necessary, the Fourth Circuit decided the question anyway, with a subheading titled "The Fourth Amendment Permits Forensic Searches of Electronic Devices at the Border Without Suspicion." *Id.* at 1232. This entire section is, in essence, dicta, as it does not answer a question raised on appeal.

However, even if it is accepted as black-letter law, it is still incorrectly decided. The court in *Touset* based their holding on the idea that they saw "no reason why the Fourth Amendment would require suspicion for a forensic search of an electronic device when it imposes no such requirement for a search of other personal property…. And it does not make sense to say that electronic devices should receive special treatment because so many people now own them or because they can store vast quantities of records or effects." *Id.* at 1233. The 11th Circuit dismissed this Court's holding that electronic storage and personal property are fundamentally

different, and subject to different degrees of protection under the Fourth Amendment. The *Touset* court, relying on its previous decision in *United States v. Vergara*, 884 F.3d 1309 (11th Cir. 2018), explained that "our decision in *Vergara* made clear that *Riley* … does not apply to searches at the border." *Touset*, 890 F.3d at 1234. While it is clear that the 11th Circuit does not believe *Riley* signals differing standards for electronic and non-electronic property, that is counter to this Court's holding in *Riley*.

The court below outlined two rationales for choosing the 11th Circuit's approach over that of the 4th and 9th Circuits. First, they say, there is a "significant national security interest in using the border to screen for risks to the United States," and "to hold [that some level of suspicion is necessary] would allow digital contraband a pass, no matter how potentially dangerous, while physical property still remains subject to penetrating searches." (R. at 8). However, the risk to national security is minimal – the primary concern of national security would be an immediate one, such as "detonat[ing] a bomb" or having information about an abducted child. *See Riley*, 2014 U.S. ___ (slip op., at 49). *Riley* makes clear that, in those circumstances, there is nothing in the holding that prevents "other case-specific exceptions [from] justify[ing] a warrantless search of a particular phone." *Id.* National security is not compromised by the imposition of a reasonable suspicion standard in a search of electronic devices at an international border. Indeed, in many of the cases cited herein, the defendants were already under some kind of suspicion from surveillance by the national security apparatus.

Second, the court below states that "a person expects less privacy upon entering and exiting the United States." [cite below]. It is well-settled that "the expectation of privacy is less at the border than it is in the interior." *Flores-Montano*, 541 U.S. at 154-55. While it is true that the expectation of privacy is less at the border, there is some expectation of privacy. *See, e.g.,*

Montoya de Hernandez, 471 U.S. 531. A reasonable suspicion standard is far less than the unabridged requirements of the Fourth Amendment, requiring only "specific and articulable facts which … reasonably warrant that intrusion." *Terry v. Ohio*, 392 U.S. 1, 21 (1968). Where the normal 'man-on-the-street' is entitled to the full protection of the Fourth Amendment, there are nevertheless situations in which those protections are outweighed by a governmental interest, such as the interest in "preventing the entry of unwanted persons and effects" into the country. *Flores-Montano*, 541 U.S. at 152. Given that this Court has never established that the Fourth Amendment does not apply at a border, there must be some level of protection. As in *Terry*, where the court held that an intrusion with reasonable suspicion that the man or woman in question had a potentially dangerous weapon was not in violation of the amendment (*Terry*, 392 U.S. 1), a reasonable suspicion standard at the border strikes the balance between the government's interest in keeping potential wrongdoers from entering the country, and the entrant's (though somewhat lessened) expectation of being free from unreasonable searches and seizures.

In this case, both Petitioner and the government agree that there was no reasonable suspicion when Petitioner was searched at the border. Petitioner was simply one of thousands of citizens who make their way across United States' borders on a daily basis.

First, Petitioner was not a threat to national security, and was thereby not under any reasonable suspicion during the stop. In *Cotterman*, the defendant was already on a watch-list; indeed, that was why his devices were searched at the border checkpoint at all. Here, Petitioner was not on any watch-list or other database. In fact, the government agent did not even have knowledge of the crimes that were being investigated by the FBI at the time of the stop. It appears that the entirety of the agent's rationale was a flight of whimsy that there was no

prohibition against searching Petitioner's documents. This comes perilously close to the general warrants issued by agents of King George that allowed for a search of any person's home and effects, hoping to turn up some evidence of wrongdoing – the very thing that the Fourth Amendment was included to protect against. Allowing this sort of search may serve governmental interests in catching all criminals (though even that assertion is questionable given the enormity of time and resources it would take to search all of every country-entrant's electronic information), but it cannot reasonably be said to benefit the security of the nation. The sheer amount of information obtained would take more time than was practicable, allowing those plotting against the nation or its citizens to carry out their crimes before being able to act on any information obtained. The only feasible action would be to detain everyone while their articles were searched, which cannot possibly be the correct interpretation of the Fourth Amendment. Further, if the concern is to prevent electronic crime, there are a myriad of other ways the government is able to advance their interest – firewalls, counter-intelligence, and anti-spyware are all used by the government for precisely this purpose, and manually searching the files adds nothing.

Nor can this be hand-waved away by saying that there is less of an expectation of privacy at the border. If the holding of the court below is accepted, it can safely be said that there is *no* expectation of privacy at the border. As noted in *Riley*, the ubiquity of possession and nigh infinite storage capacity of these devices has fundamentally affected the way that people store and carry their information. Gone are the days of people carrying address books that list only contact information; instead, their "address book" also contains health information, evidence of political affiliation, and personal financial information. The modern convenience of this having this information at one's fingertips also means that one cannot store private information in a safe

place, away from prying eyes. The fundamental assumption of Fourth Amendment jurisprudence is that the more cursory a scan is, the less protection is afforded. Electronic information stores very nearly the entirety of person's life now, and should be treated as such for purposes of protection against unreasonable search and seizure.

If it is accepted that the right to privacy at the border is lessened by virtue of the government's interest in controlling who and what comes into the country, a standard of reasonable suspicion is the only practicable solution. A border agent must have specific and articulable facts that lead to an inference that criminal activity is afoot. It is an extremely standard to meet, but it is still a standard. A reasonable suspicion standard would balance the government interest in protecting the country from undesirable entrants by allowing agents to do forensic searches of anyone who they believed to be criminally active in some way, while also maintaining the fundamental right to privacy afforded by the Fourth Amendment.

B. THE SEARCH OF PETITIONER AMOUNTED TO AN EXTENDED BORDER STOP, AND THUS REASONABLE SUSPICION WAS NECESSARY.

The forensic search of Petitioner's electronic devices was an extended border search, and as such, reasonable suspicion – which was lacking in this case – was necessary. An extended border search takes place when there is attenuation in the time or location of the search from the border crossing such that the subject has regained an expectation of privacy. Because Petitioner had gained access to the country, and the search took several hours, reasonable suspicion was necessary and as it was lacking, the search was in violation of the Fourth Amendment.

The doctrine of extended border search is both limited in use, and not well defined. This Court has only used the term "extended border search" once in its decisions, as part of the basis for issuing a stay of judgment in a border search case. *Harris v. United States*, 400 U.S. 1211

(1970) (Douglas, J., staying judgment of 9th Circuit) (cert. denied). It is primarily used by the 9th Circuit, though its existence has been impliedly accepted by the 6th Circuit. *See, e.g., United States v. Abbouchi*, 502 F.3d 850 (9th Cir. 2007) *and see United States v. Stewart*, 729 F.3d 517 (6th Cir. 2013) (finding that the search in question was not an extended border search). Extended border searches are those that "usually occur near the border, but after the border has already been crossed." *United States v. Villasenor*, 608 F.3d 467, 471 (9th Cir. 2010). The crux of the reasoning for the extended border stop doctrine is that once an individual has cleared the border, the individual has "regained an expectation of privacy in accompanying belongings." *Cotterman*, 709 F.3d at 961. The court in *Cotterman* held that the extended border search was not applicable as the laptop did not clear customs, although the defendant did. *Id.* However, the same court has held that the extended search doctrine applied to a package shipped by Federal Express before the border crossing, so this cannot be the accurate dispositive factor. *United States v. Cardona*, 769 F2d 625 (9th Cir. 2013). Instead, the question must be whether the search, taking into account factors like time of the search, distance from the border, and whether the search "intrude more on an individual's normal expectation of privacy" that they had regained after clearing the border. *Cotterman*, 709 F.3d at 990 (Smith, J. dissenting).

In this case, the search did intrude after Petitioner had regained an expectation of privacy. Petitioner had cleared the border; only his laptops and USB devices were detained (R. at 3). It does not appear from the record that Petitioner was informed that his devices were going to be submitted to a more extensive search, and it is reasonable to conclude that he believed he had cleared the border, and that the government would need either to obtain a warrant to search the devices (in the absence of reasonable suspicion), or return them to Petitioner. Neither of those happened, and Petitioner's devices were searched without reasonable suspicion (R. at 6). Further,

the devices were transported away from actual border crossing (presumably into some office space near the crossing), and were held for several hours after Petitioner had entered the country (R. at 3). From the totality of these circumstances, the search of the electronic devices was an extended border search, subject to a reasonable suspicion standard, and in violation of the Fourth Amendment.

II. THE ACQUISITION OF HISTORICAL CELL SITE LOCATION INFOMRATION IS A SEARCH.

The Fourteenth Circuit erred by holding that requests for fewer than seven days of historical cell site location information (CSLI) do not violate the Fourth Amendment protection against unreasonable search and seizures. The decision is incompatible with this Court's holding in *Carpenter v. United States* and the requirements of the Fourth Amendment. *Carpenter v. United States,* 138 S. Ct. 2206 (2018). In *Carpenter,* this Court held that law enforcement's access of seven days of CSLI constituted a Fourth Amendment search and required a warrant backed by probable cause. *Id.* The Court declared that, generally, law enforcement must obtain a warrant supported by probable cause before acquiring CSLI and held that individuals maintain a legitimate expectation of privacy in the record of their physical movements. *Id* at 2221.

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend IV. To establish a Fourth Amendment violation, petitioner must show that there was government action that constitutes a search and that the search was unreasonable. *Smith v. Maryland*, 442 U.S. 735, 740 (1979).

While this Court has noted that there may be a limited period for which law enforcement may access CSLI without implicating Fourth Amendment rights, this Court should declare today that all access to CSLI requires a warrant supported by probable cause. Alternatively, this Court

should declare that law enforcement's actions in acquiring 10 days of weekday CSLI, three days of continuous CSLI, and one hour of tower dump CSLI violate petitioner's Fourth Amendment rights.

The first step in the Fourth Amendment search analysis is determining whether a reasonable expectation of privacy exists and that the government's actions intrude on that privacy. *Smith*, 442 U. S. at 740. The test to determine whether government action constitutes a search is whether government agents intrude upon an expectation of privacy that society is prepared to recognize. *Kyllo v. United States,* 533 U.S. 27 (2001); *Katz v. United States,* 389 U.S. 347, 361 (1967) (Harlan, J., concurring). When determining if a reasonable expectation of privacy exists, this Court examines the mindset of the individual to determine if the expectation of privacy exists and the opinion of society at large to determine whether society is prepared to recognize that expectation. *Kyllo,* 533 at 34. The latter part of this inquiry requires the court to determine whether the expectation of privacy is such that it can be classified as one of "the everyday expectations of privacy that we all share." *Minnesota v. Olson*, 495 U.S. 91, 98 (1990) Further, when examining new or relatively new technology, the court has noted that this test must ensure the same degree of privacy protection against the government exists now that would have existed before the new technology existed. *Kyllo*, 533 U.S. at 34.

A. THIS COURT SHOULD HOLD THAT INDIVIDUALS HAVE A REASONABLE EXPECTATION OF PRIVACY IN THEIR HISTORICAL CELL PHONE LOCATION RECORDS AND THAT GOVERNMENT ACQUISITION OF THESE RECORDS IS A PER SE FOURTH AMENDMENT SEARCH.

This Court's jurisprudence indicates that individuals have a reasonable expectation of privacy in their historical cellphone location information. In *Carpenter,* this Court held that individuals have a reasonable expectation of privacy in seven days of historical cell site

location information. *Carpenter,* 138 S. Ct. 2206. *Carpenter* remains the binding precedent on this Court, however the Court should take the opportunity to clarify its holding in *Carpenter* and to provide a more explicit rule regarding the government's intrusion on the individuals' privacy by acquiring CSLI. The Court should declare that individuals have a reasonable expectation of privacy in their historical cell phone location records regardless of the time frame being considered because these records track the whole of an individual's movements.

This Court has consistently held that individuals have a reasonable expectation of privacy that society is willing to recognize in the whole of their physical movements. In *United States v. Jones*, a case involving GPS tracking of a vehicle, this Court concluded that there was a reasonable expectation of privacy that the government could not monitor and catalogue an individual's every movement. *United States v. Jones*, 565 U.S. 400 (2012). *Jones* is an example of this Court's acknowledgment that new technology often requires greater judicial protections to ensure that the level of privacy that existed before the technology was invented. See *Id.* This Court took the *Jones* conclusion one step further in *Carpenter* by affirmatively declaring that individuals have a reasonable expectation of privacy in the whole of their physical movements. *Carpenter,* 138 S. Ct. at 2219.

In *Carpenter*, the court provided the framework to analyze the acquisition of historical cell site location information (CSLI) and its impact on an individual's reasonable expectation of privacy. In *Carpenter,* the court held that the acquisition of seven days of CSLI was a significant enough intrusion to violate an individual's reasonable expectation of privacy in the whole of his physical movement and thus constitute a search under the Fourth Amendment. *Id.* The majority stated, "we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI." *Id* at 2217. In coming to this conclusion, the

court set forth two guideposts for applying the Fourth Amendment, "securing the privacies of life against arbitrary power, and placing obstacles in the way of a too permeating police presence." *Id* at 2214. The court then reasoned that the acquisition of CSLI violated the reasonable expectation of privacy because CSLI can monitor a person's every movement (something police were incapable of doing in the past), CSLI allows investigators to travel back through history to reconstruct every movement "the suspect has effectively been tailed every moment of every day for five years.", CSLI is collected on every device across the nation (which leads to effectively a dragnet of policing), and perhaps most importantly CSLI disclosure is overly intrusive and can reveal the privacies of life. See generally *Id.* Finally, the court hit on the fact that CSLI is remarkably easy and cheap compared to traditional investigative tools. *Id* at 2218.

In the present case, the Fourteenth Circuit, while acknowledging the *Carpenter* decision affirming an individual's reasonable expectation of privacy in the whole of his physical movements, misapplies the majority's decision concludes that this expectation is only implicated by government agents accessing seven days or more of CSLI. R. at 11-12. To reach this conclusion, the Fourteenth circuit relied on a footnote in the *Carpenter* decision which stated:

> "As part of its argument, the Government treats the seven days of CSLI requested from Sprint as the pertinent period, even though Sprint produced only two days of records. Contrary to JUSTICE KENNEDY's assertion, post, at 19, we need not decide whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be. It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search."

Carpenter, 138 S.Ct at 2217 n.3. (The Fourteenth Circuit announces that this Court has not determined whether there is a limited period of time that the government may acquire CSLI without implicating the Fourth Amendment, yet then declares that this Court had established a

bright-line rule in *Carpenter*: the acquisition of seven days or more of CSLI is a Fourth Amendment search, and anything less is not. (R. at 11-12).

The Fourteenth Circuit erred in its reasoning and conclusion that this Court's holding in *Carpenter* announced this Court's judgment merely restricted, while affirming, law enforcement's ability to request CSLI under the SCA to requests of fewer than seven days. As Judge Weber notes in his dissent:

> "The Court decided the case on the facts before it. It did not indicate—much less hold that a shorter period of time would not violate an individual's expectation of privacy. And, it affirmatively stated that the 'government must generally obtain a warrant supported by probable cause before acquiring such records.'"

(R. at 15). Judge Weber notes that, by stating that generally to acquire CSLI records law enforcement must obtain a warrant, this Court is not stating that only by acquiring seven days of CSLI will the Fourth Amendment be implicated. *Id.*

This Court should take this opportunity to declare that law enforcement engages in a Fourth Amendment search when acquiring historical any amount of historical CSLI because any collection of this data intrudes on a reasonable expectation of privacy. By attempting to interpret this Court's *Carpenter* decision as a bright-line rule, the Fourteenth Circuit creates an arbitrary distinction between requests for 7 days of CSLI and requests for 6 days and 23 hours of historical CSLI. The Fourteenth Circuit notes that without this Court determining a rule, the lower courts are likely to be involved in judicial line drawing on iteratively smaller scales. However, any acquisition of historical CSLI implicates the same privacy concerns noted in *Carpenter*. As the inquiry would theoretically be based on a difference of degree, rather than a difference of kind, any judicial line drawing would be completely arbitrary. The line drawing would result in the judiciary determining that, even though the same concerns (cataloguing every individual's historical movements, law enforcement's ability to rewind history, the overly

intrusive and revealing nature, and the low cost) are raised by any collection of historical CSLI, the court has decided not to protect the reasonable expectation of privacy because law enforcement effectively dodged the *Carpenter* ruling.

Finally, the Fourteenth Circuit expressed concern about narrowing the *Carpenter* holding because of an active senate bill. (R. at 12). The lower court's majority suggested it would be wise to defer to Congress in this situation. *Id.* However, this court has explained that there are a variety of tenable inferences that may be drawn from congressional inaction and thus congressional inaction lacks significance. *Pension Ben. Guar. Corp. v. LTV Corp.*, 496 U.S. 633, 650 (1990) As such, any judicial holding should not be based on what actions congress may or may not make in the future to protect the Fourth Amendment rights of individuals, but rather on this Court's precedent.

B. ALTERNATIVELY, THIS COURT SHOULD HOLD THAT LAW ENFORCEMENT'S ACQUISITION OF THE THREE-DAY RECORDS AND WEEKDAY RECORDS CONSTITUTES A FOURTH AMENDMENT SEARCH.

Ensuring that the line between short-term and long-term CSLI does not allow law enforcement to evade any durational protection is paramount. As Justice Sotomayor noted in her concurrence in *Jones*, not only does long-term GPS monitoring raise privacy concerns, but short-term GPS monitoring raises concerns under the *Katz* reasonable expectation of privacy test as well. 565 U.S. 400, at 415 (Sotomayor, J., concurring). Justice Sotomayor's observation is just as applicable to historical CSLI as it was to GPS monitoring. The concerns that are raised by short-term and long-term requests for CSLI are identical in kind and thus the judiciary is forced to draw lines based on differences of degree rather than differences of kind.

Notably, very few courts have attempted to draw these lines. Before *Carpenter,* the circuit courts elected to apply the third-party doctrine to historical CSLI. As such, only one court

that has attempted to draw a line defining short-term and long-term historical CSLI. *Commonwealth v. Estabrook,* 38 N.E.3d 231 (Mass. 2015). The court in *Estabrook* held that any requests for historical CSLI beyond six hours constituted a request for long-term CSLI and thus were a Fourth Amendment search requiring a warrant. *Id.* at 234. If this Court insists on drawing these lines, this Court may wish to follow that court's lead. However, even if this Court does not draw such a line, the Court should still determine that law enforcement's actions here are a Fourth Amendment search and violate petitioner's reasonable expectation of privacy.

1. LAW ENFORCEMENT'S ACQUISITION OF THE THREE-DAY RECORDS CONSTITUTES A FOURTH AMENDMENT SEARCH.

The privacy concerns articulated by the *Carpenter* majority are still applicable to the request for the three-day records and as such, the accessing the records constitutes a Fourth Amendment search. The reasonable expectation of privacy in the whole of one's physical movements cannot disappear simply because those movements are tracked for a shorter period. Ensuring the level of privacy remains the same as before the technology was implemented was key to the *Carpenter* decision. *Carpenter,* 138 S.Ct. at 2214. As such, the differences in degree of intrusion based on how many days or hours of CSLI law enforcement accesses should not determine the constitutionality of those acquisitions.

In *Carpenter* the court expressed concerns about the very nature of CSLI allowing law enforcement to access CSLI without a warrant supported by probable cause. *Id.* The court noted that these requests allowed law enforcement to travel back in time and retrace a suspect's whereabouts, something previously impossible to achieve. *Id.* at 2218. Essentially, every suspect (or cell phone owner) had been tailed by law enforcement every moment of every day. *Id.* Additionally, the court acknowledged that CSLI is deeply revealing about the happenings of a person's life and can give law enforcement an intimate view into the privacies of life. *Id.* at 2222.

Finally, the relative ease, low cost, and efficiency of CSLI gave law enforcement a cheap, efficient, and powerful form of surveillance that would permeate throughout society without most individuals realizing that they were being tracked. *Id.* The sum of these factors resulted in the Court declaring that the acquisition of historical CSLI constituted a Fourth Amendment search. Notably, while law enforcement requested seven days in *Carpenter*, Carpenter's cell phone carrier only provided 2 days of CSLI. *Id.* at 2217 n.3.

Here, the Fourteenth Circuit maintains, without providing any evidence, that the three days of records are not enough time to give an intimate view into the privacies of life nor amount to near-perfect surveillance. (R. at 13). On its face this may seem valid, as the time frame is shorter than the time frame in *Carpenter*, but the same concerns are raised no matter length of the time period of CSLI requested. In the instant case, Agent Hale's request for the 2703(d) court order is telling. In her request, Agent Hale expressly states, "law enforcement officers can use historical cell site information to analyze the past use of Subject Phone 1 and thereby obtain information about the subject's whereabouts, and activities, as well as patterns of behavior." Hale Aff. at 20. One cannot possibly conclude that technology that would allow law enforcement to glean information pertaining to a "subject's whereabouts, and activities, as well as patterns of behavior" do not provide an intimate view into the privacies of life. If the law enforcement officer requesting the information acknowledges its power, it seems erroneous for the Fourteenth Circuit not to do so as well.

Additionally, the historical CSLI collected in the three-day records request is likely to be more accurate than even GPS. In her request, Agent Hale confirms this theory when identifying that Sweetwater is a large, densely populated city with many buildings that have small towers attached to provide cellular service. Hale Aff., at 11. Agent Hale concludes that because of the

vast number of towers, CSLI can locate individuals on particular floors, or in particular rooms, of buildings and is often more accurate than GPS. *Id.* The accuracy of CSLI in the instant case gives rise to greater privacy concerns than typical CSLI. Essentially, because of the accuracy of CSLI in Sweetwater, law enforcement was able to rewind history and track Petitioner's movements which could reveal a particular bar he frequented, a religious establishment he visits, the exact location of his bedroom in his house, or the location of a private sexual encounter without his knowledge.

Finally, as noted, while the request in *Carpenter* was for seven days, law enforcement was only able to acquire two days' worth of CSLI. *Carpenter*, 138 S.Ct at 217 n.3. The Three-day Records acquired in this case are longer than the two days of CSLI in *Carpenter*. Here, the fact that they acquired more information than was acquired in *Carpenter* may very well prove dispositive. However, if it does not, the fact that the privacy concerns are nearly identical no matter the amount of CSLI requested, the accuracy of CSLI in Sweetwater, and law enforcement's acknowledgement of the value of CSLI should. The court should thus determine that accessing the Three-Day Record of CSLI constituted a Fourth Amendment search.

2. LAW ENFORCEMENT'S ACQUISITION OF THE WEEKDAY RECORDS CONSTITUTES A FOURTH AMENDMENT SEARCH.

The privacy concerns in the weekday records request may be lower, but the request still violates petitioner's expectation of privacy in the record of his physical movements. This reasonable expectation of privacy is one that society, and this Court, has already recognized. *Carpenter,* 138 S.Ct at 219; *Jones,* 565 U.S. 400. The Court must then weigh the intrusion based on the Fourth Amendment principle of securing individuals' privacies of life against arbitrary power and the Fourth Amendment's purpose of creating an obstacle to a permeating police presence. *Carpenter,* 138. S.Ct. at 2214. Finally, the Court must ensure that the degree of privacy

protection against the government is the same as it was before the new technology existed. *Jones,* 565 U.S. at 406.

Here, law enforcement's attempts to lower the degree of intrusion by asking for fewer days of CSLI is merely an attempt to scurry around the *Carpenter* decision. (R. at 16). While the concerns about intrusion into the privacies of life may be lower with these records, the practical effect results in constant surveillance of all activity during business hours. In the past, a comprehensive list of activities an individual is involved in, and the location of those activities, would have been unknowable to law enforcement. *Carpenter*, 138. S.Ct at 218-19. With the advent of historical CLSI, law enforcement's request for historical CSLI pertaining to petitioner's weekday business hours locations still is akin to tracking him every moment of that time period. As Judge Weber noted in his accessing these limited records is the equivalent of having petitioner retroactively wearing an ankle monitor. (R. at 16). While the Fourteenth Circuit claims that this is completely possible in every day policing, the historical nature of the CLSI makes it impossible because law enforcement cannot travel back in time to track a suspect.

Additionally, the requests for weekday hours is a blatant violation of *Carpenter* and law enforcement attempted to side-step the seven-day requirement articulated in *Carpenter* by limiting the number of hours they requested. (R. at 16). The request was for a 10-day period which was then limited to business hours, a clear attempt to avoid *Carpenter*. *Id.* To allow requests such as these, this Court would be approving of this deliberate attempt by law enforcement officers to dodge the law. Theoretically, by the logic offered by the Fourteenth Circuit, law enforcement could request up to 167 hours and 59 minutes of CSLI without violating the Fourth Amendment.

As such, this Court should clarify that law enforcement's strategy of dodging the law is unacceptable and hold that the weekday records request constituted a search.

3. ALTERNATIVELY, LAW ENFORCEMENT'S COMBINED ACQUISITION OF THE THREE-DAY RECORDS AND WEEKDAY RECORDS CONSTITUTES A FOURTH AMENDMENT SEARCH.

If the court does not consider each request individually or determines that one of the previous requests is not a search, the Court should consider the cumulative effect of multiple requests and determine that combination of these requests violate petitioner's expectation of privacy. This mosaic theory has been advocated by different justices on the Court, with at least 5 joining in concurrences that mention the theory. *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring); *Jones*, 565 U.S. at 428-31 (Alito, J., concurring in the judgment). The theory posits that, while one act of law enforcement may not be a search, the Court should look at the collective whole of the actions to determine if those actions would constitute a search. Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 Mich. L. Rev. 311, 320 (2012).

If the Court believes that the hour measurement pursued by the government is proper, then the Court must consider the requests jointly. In this case, the three-day request and the weekday records request combined amount to 152 hours of surveillance, admittedly fewer than the 168 hours of surveillance in *Carpenter*, but are we really to believe that 16 hours or less than 10% of the request amounts to any lower degree of surveillance or intrusion into the privacies of petitioner's life? In the past, this level of surveillance may have been possible, but the expensive and time-consuming nature would limit its viability. Additionally, when officers are conducting traditional surveillance, there is every opportunity for the suspect to detect the surveillance. Here, no such opportunity existed because the surveillance didn't begin until nearly a year after the crime was committed. (R. at 5).

By refusing to consider these requests jointly, the court would allow for law enforcement to simply make multiple requests for 6 days of CSLI. Obviously, this negates the purpose of any restriction this Court established in *Carpenter*. In his dissent, Judge Weber notes that the majority's logic would allow for them to request 1 hour each day for 168 days. (R. at 16). By allowing these requests, this Court would be allowing law enforcement to avoid playing by the rules and essentially be endorsing law enforcement's attempts to violate the Fourth Amendment protections that are guaranteed the citizens of this country.

C. IF THE COURT DOES NOT DETERMINE THAT ALL ACQUISITIONS OF HISTORICAL CLSI ARE FOURTH AMENDMENT SEARCHES, THE COURT SHOULD DETERMINE THAT TOWER DUMPS ARE FOURTH AMENDMENT SEARCHES.

In each instance the Court must consider whether the expectation of privacy is one that society is willing to recognize. *Smith,* 442 U. S. at 740. The Court must then weigh the intrusion based on the Fourth Amendment principle of securing individuals' privacies of life against arbitrary power and the Fourth Amendment's purpose of creating an obstacle to a permeating police presence. *Carpenter*, 138 S.Ct. at 2214. Finally, the Court must ensure that the degree of privacy protection against the government is the same as it was before the new technology existed. *Kyllo*, 533 U.S. at 34.

Tower dumps are less intrusive to each individual, but more intrusive to society as a whole than collection of individual CLSI. As such, they create the exact fears that caused the framers to create the Fourth Amendment. The framers created the Fourth Amendment to prevent arbitrary invasions of an individual's privacy and security by the government. *Camara v. Municipal Court of City and County of San Francisco*, 387 U. S. 523, 528 (1967). This amendment was crafted to protect against the general warrants and writs of assistance which granted British army officers in the Framers' time to search for evidence of criminal activity

without rules or restraints. *Riley v. California,* 573 U.S. ___ (2014) (slip op., at 27). These concerns were later articulated in *United States v. Knotts*, where the Court feared "dragnet type law enforcement policies" that would allow the police to have surveillance of every citizen, every moment, of everyday. *United States v. Knotts*, 460 U.S. 276, 283-84 (1983).

While the Fourteenth Circuit contends that *Carpenter* should not apply to tower dumps, the court neglected to consider the wide ramifications of allowing these requests without Fourth Amendment protections. Tower dumps are the definition of the dragnet law enforcement policies expressed in *Knotts*. Tower Dumps allow law enforcement to see where any person is, at any point in time, throughout the recorded history of that tower and are only limited in this discovery by the time period of the request. (R. at 4 n.3). While the privacy concerns of each individual are lowered, when considering the potential to use tower dumps as a form of mass surveillance they cannot avoid Fourth Amendment scrutiny.

Law enforcement will advocate for tower dumps as an effective tool for police, but they offend our basic notions of security, privacy, and our expectation that big brother is not always watching. Law enforcement's support of tower dumps is understandable; even when there is no identifiable suspect to a crime, law enforcement can request tower dumps from the towers around that crime and identify potential suspects. However, our citizens do not have the expectation that they are constantly being watched and that is what tower dumps enable law enforcement to effectively accomplish. Tower dumps give law enforcement knowledge of everyone in an area at a specified time in history, they can tell law enforcement where those people are visiting, who they are visiting with (as was the case here), and allow law enforcement to peer, if ever so briefly, into the privacies of life for each of the individuals who were unfortunate enough to be in the area of a crime when it was committed.

In the present case, Agent Hale requested three tower dumps with no suspect identified. (R. at 4). Her hope was that she would simply find one phone number that was listed on all of the tower dumps and that would create a suspect. While Agent Hale identified a suspect, the greater cause for concern is the fact that these tower dumps disclosed a countless number of individuals' location information nearly a year after those individuals were in those locations. Essentially, the government was allowed to rewind history and track each of the individuals for an hour a year after they had cause for concern. These results are untenable with the privacy that was expected before the use of tower dumps became possible. In the past, the only way for the government to receive this information would be to magically conjure up a list of everyone that was in the vicinity of each of these crimes and then ask them each individually to recall their location at the precise date and time associated with the crime. Allowing these tower dumps allows law enforcement officers, like agent Hale, to track every individual regardless of whether they present a criminal threat.

Even if this Court does not wish to use the *Carpenter* analysis, harking back to the basic purpose of the Fourth Amendment and the concerns articulated in *Knotts* requires that tower dumps be considered Fourth Amendment searches and require a warrant backed by probable cause. Tower dumps create the opportunity for law enforcement to use tactics which amount to dragnet policing, constant surveillance, and a permeating police presence, all of which the Fourth Amendment seeks to prevent.

III. THE ACQUISTION OF HISTORICAL CELL SITE LOCATION INFORMATION REQUIRES A WARRANT AND NO WARRANT EXCEPTIONS ARE APPLICABLE IN THIS CASE.

The collection of each of these forms of CSLI constituted a search and thus required a warrant backed by probable cause. Contrary to the Fourteenth Circuit's assertion that the Stored

Communications Act (SCA) is still applicable to this case, and as noted in *Carpenter*, the collection of CSLI will generally require a warrant, absent some exigent circumstance. *Carpenter,* 138 S.Ct at 2222. While there are various exceptions to the warrant requirement, the only one that could potentially be at play in this situation is the exigent circumstances exception and it is inapplicable.

The general test about the warrant requirement is the reasonableness of a search, but warrantless searches are generally unreasonable unless it falls within one of the specified exceptions to the warrant requirement. *Arizona v. Gant*, 556 U.S. 332, 338 (2009). In *Carpenter*, the court lists some possible circumstances that could result in the inapplicability of the warrant requirement. *Carpenter*, 138. S.Ct. at 2223. ("Such exigencies include the need to pursue a fleeing suspect, protect individuals who are threatened with imminent harm or prevent the imminent destruction of evidence."). "While police must get a warrant when collecting CSLI to assist in the mine- run criminal investigation, the rule we set forth does not limit their ability to respond to an ongoing emergency." *Id.*

In this case, neither party disputes that the orders were acquired based upon a reasonable belief that the information may be relevant and material to a criminal investigation. (R. at 10 n.11). This showing falls well short of probable cause. Further, there is little room for argument that the situation is one of the exigent circumstances that would allow for a warrantless search. Petitioner was not a current threat to harm anyone, he was not fleeing, and there is no evidence that he was likely to destroy evidence. The fact that these searches happened almost a year after the crimes points to the fact that these were not exigent circumstances. There is every indication that this investigation is one of the mine-run cases identified by the majority in *Carpenter*. This

court should re-affirm established precedent and announce that the collection of CSLI required a warrant in this case.

CONCLUSION

For the foregoing reasons, Petitioner respectfully requests that this court recognize the self-evident fact that electronic devices are fundamentally different from other material, and rule that they are subject to the Fourth Amendment protections which they should be afforded. Even though the search took place at the border – where the government has a greater ability to control who and what enters the nation – a reasonable suspicion standard balances the compelling governmental interest with a citizen's expectation of privacy.

In addition, Petitioner urges this Court to re-affirm its holding in *Carpenter* that the collection of CSLI constitutes a Fourth Amendment search and requires a warrant. In the alternative, the facts of this case show that each of law enforcement's requests for CSLI intruded on petitioner's Fourth Amendment reasonable expectation of privacy and, consequently, were unreasonable searches that required a warrant backed by probable cause.

Accordingly, Petitioner respectfully requests that this Court overturn the holding of the 14th Circuit, and instruct the trial court to grant Petitioner's motion to suppress.

Respectfully submitted,

Attorneys for
Petitioner