Case No. 10-1011

In the

SUPREME COURT OF THE UNITED STATES

HECTOR ESCATON,
Petitioner,

v.

UNITED STATES OF AMERICA,
Respondent.

On Writ of Certiorari from the
United States Court of Appeals
for the Fourteenth Circuit

BRIEF FOR THE PETITIONERS

Team 15
Counsel for Petitioner

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES:

QUESTIONS PRESENTED

I. Whether reasonable suspicion is required under the Fourth Amendment to conduct forensic searches of electronic devices at the border.

II. Whether the Government's acquisition of three days of cell-cite location information, one-hundred hours of of cell-cite location information over two weeks, and cell-cite location information collected from cell tower dumps violate the Fourth Amendment of an individual in light of Carpenter v. United States, 585 U.S. (2018).

OPINION BELOW

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

CONSTITUTIONAL PROVISIONS AND RULES

The Fourth Amendment of the United States Constitution ensures:

"The right of people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall be issued, 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."

INTRODUCTION

This case is about Petitioner's Fourth Amendment rights being violated when reasonable suspicion was not applied to a forensic search of Petitioner's electronic devices, which led to Petitioner's criminal charges of Bank Fraud, Conspiracy to Commit Bank Fraud, and Aggravated Identity Theft. This court is presented with the opportunity to establish policy that strikes a greater balance when it comes to governmental interests and privacy interests at the border, as well as correct the violations of Fourth Amendment rights committed in the over-reaching searches of Petitioner's cell cite information.

STATEMENT OF FACTS

On September 25, 2019, Hector Escaton, a twenty-eight-year-old West Texas citizen and resident, returned to the United States from Mexico through a West Texas border checkpoint. (R. at 2). Customs and Border Protection (CBP) Officer Ashley Stubbs conducted a border search of Escaton's vehicle and found three suitcases in the back of Escaton's car. (R. at 2). Through the search, Stubbs found an iPhone, a laptop, three external hard drives and four USB devices. (R. at 2). The iPhone was placed on airplane mode and the laptop was disconnected from wireless service, and Stubbs manually searched both devices without the use of assistive technology. (R. at 2). A paper note was attached to the bottom of the computer, indicating to call a person by the name of Dolores with $$$. (R. at 2).

Stubbs returned the phone to Escaton, but retained the laptop, hard drives, and USB devices. (R. at 3). The devices did not need passwords. (R. at 3). Stubbs discovered that on the laptop, there were certain folders that could not be opened and needed a password. (R. at 3). Stubbs then inserted the USB drives in the computer and found that he could not access the

contents. (R. at 3). Stubbs sent the electronics to Immigration and Customs Enforcement (ICE) Special Agent & Computer Forensic Examiner Theresa Cullen at the checkpoint. (R. at 3). Cullen used forensic software to copy and scan the devices, which takes several hours. (R. at 3).

The forensic examination found that the laptop contained documents containing individual bank account information, and the USB drives contained traces of malware. (R. at 3). Cullen found not incriminating evidence on the hard drives and deleted those scans. (R. at 3). CBP notified the FBI of the findings, which had been investigating "ATM skimming" of Mariposa Bank ATMs in Sweetwater during October of 2018. (R. at 3). Special Agent Catherine Hale began examining connections between the forensic evidence provided by Stubbs and Cullen and that reported by Mariposa Bank. (R. at 3). There were different methods used to obtain the information from the ATMs that included: foreign skimmers overlaying debit card information, malware installed through the ATMs USB port, and malware that allowed the skimmer to empty out cash from the ATM. (R. at 4).

Stubbs reported Escaton's information, including the telephone number which he found in Escaton's phone, and details to the FBI for potential bank fraud and identity claims. The malware found on his hard drive, which was not identical, was similar to the malware that was used at Mariposa ATMs in Sweetwater. (R. at 5). At trial, Escaton was convicted for Bank Fraud, Conspiracy to Commit Bank Fraud, and Aggravated Identity Theft. (R. at 6). Escaton filed a motion to suppress the results of the forensic search and the cell-site data requested from Delos Wireless. (R. at 6). The District Court denied the motion on both issues and Escaton was convicted on all charges, and now appeals. (R. at 6).

ARGUMENT

The court incorrectly denied Petitioner's motion to suppress evidence, finding that the forensic search of Petitioner's electronic devices did not violate his Fourth Amendment rights. The Fourth Amendment ensures "the right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures…" U.S. Const. amend. IV. The Court will adopt the de novo standard of review. United States v. Cotterman, 709 F.3d 952, 968 (9th Cir. 2013). The previous court's legal conclusions and factual determinations will be reviewed for clear error. Id. Since there is clear error in the legal conclusions determining that no reasonable suspicion is required to forensically search electronic devices at the border, an ordeal that Petitioner was subjected to twice, this Court should reverse the lower court's decision, finding that reasonable suspicion is required to conduct forensic searches at the border.

I. THE COURT INCORRECTLY FOUND THAT NO REASONABLE SUSPICION IS REQUIRED TO MANUALLY SEARCH PETITIONER'S CELL PHONE OR LAPTOP WHEN SUCH A SEARCH SUBJECTS PETITIONER TO SUFFER GREAT INDIGNITY, AND WAS NOT CONDUCTED FOR A PARTICULAR OR OBJECTIVE REASON.

The court incorrectly found that reasonable suspicion is not required to conduct a search of electronic devices at the border. The Fourth Amendment commands that searches and seizures be reasonable, and what is reasonable depends upon all of the circumstances surrounding the search or seizure and the nature of the search itself. U.S. v. Montoya De Hernandez, 105 S.Ct. 3304, 3308 (1985); The permissibility of a particular law enforcement practice is judged by balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interest. Id. at 3308. However, reasonable suspicion has been required for searches at the border for highly intrusive searches of a person's body, and intrusiveness has

been defined in terms of the indignity that will be suffered by the person being searched, in contrast with whether one search will reveal more than another. U.S. v. Touset, 890 F.3d 1227, 1234 (11th Cir. 2018).

As in U.S. v. Ortiz, the court held that reasonable suspicion was required in order to search vehicles at the border. 95 S.Ct. 2585, 2588 (1975). Border Patrol agents stopped respondent's car for a routine immigration search at a traffic checkpoint, finding three aliens concealed in the car. Id. at 2586. Respondent argues that probable cause was required border searches. Id. The court reasoned that although there is precedence that gives a significant amount of deference to the Government when it comes to border searches, that degree of discretion is inconsistent with the Fourth Amendment in so much as a search, even one of an automobile, is a substantial invasion of privacy. Id. at 2588. In order to protect that privacy from official arbitrariness, the Court has always regarded that probable cause as the minimum requirement for a lawful search. Id. The Government listed factors it considers when deciding which cars to search, however, these nor no other special reasons were presented for believing respondent's vehicle contained aliens. Id. at 2589. Similarly, in U.S. v. Brigoni-Ponce, the court held that reasonable suspicion is required to stop and search a vehicle at the border. 95 S.Ct. 2574, 2583 (1975). On the evening of March 1973, two officers were conducting a roving patrol near a checkpoint, when they stopped respondent's car, claiming the reason for the stop was that the occupants were of Mexican descent. Id. at 2577. The officers questioned the occupants and found that the passengers were illegal aliens, and arrested and charged respondent. Id. The court reasoned that the Fourth Amendment requires that seizure be reasonable, defining reasonable as a balance between public interest and the individual's right to personal security. Id. at 2579. The

court was unwilling to let the Border Patrol dispense entirely with the requirement of reasonable suspicion to justify roving patrol stops, especially in the context of border area stops, which demand something more than the broad and unlimited discretion sought by the government. Id. at 2580-81.

Contrastingly, in U.S. v. Touset, the court held that reasonable suspicion was not required for forensic searches of electronic devices at the border. 890 F.3d 1227, 1238 (11th Cir. 2018). After a series of investigations by private organizations and the government, it suggested that Touset was involved with child pornography, after a tip from a payment service that indicated Touset was making low money transfers to individuals in course countries for sex tourism and child pornography. Id. at 1230. After arriving at an airport in Georgia off an international flight, border agents forensically searched his electronic devices, which found child pornography of the hard drives and the two laptops. Id. Touset moved to suppress the evidence from the forensic search of his electronic devices, which was denied. Id. at 1231. The court reasoned that the Fourth Amendment has never required reasonable suspicion for a search of property at the border, however non-routine and intrusive, Id. at 1233, and the factors that define intrusiveness are irrelevant to searches of electronic devices. Id. at 1234. Forensic searches of electronics are not like strip searches or x-rays that require an agent to touch a person, and even though it may intrude on the privacy of the owner, a forensic search of an electronic device is a search of property. Id. However, the concurring judge indicates that the government's new-found position in this case sets a daunting precedent that says that no justification is needed to detain and forensically search electronic devices of any American citizen returning from abroad, and heeds caution to that precedent. Id. at 1238-39.

Likewise, in Montoya de Hernandez, the court held that reasonable suspicion was present in this case. 105 S.Ct. at 3312. Respondent had entered the Los Angeles International Airport, and her documents from Bogota raised suspicion between the officers on the possibility other being a drug smuggler. Id. at 3306. Respondent was detained until she had a bowel movement or agreed to a rectal examination. Id. at 3307. After sixteen hours of not passing bowels, the agents went to get a court order for a rectal exam and an x-ray, and were able to discover a foreign substance in respondent's rectum, which later amounted to eighty-eight balloons filled with cocaine. Id. The court reasoned that precedence has placed the Government's interest in protecting the borders above the privacy interests of those who are entering the country through those borders. Id. at 3309. If officials at the border have a particularized and objective basis for suspecting a particular person, then a warrantless search is justified considering the totality of the circumstances. Id. at 3311. The dissenting judges call for a use of the standards of reasonable suspicion that have been applied and successful in striking the balance elsewhere, be applied to border searches. Id. at 3317. Judges bring up a slew of instances where reasonable suspicion and an impartial magistrate is required for many low-level instances, which differs than the current lack thereof at our country's borders. Id. at 3318.

Like in Ortiz and Brigoni-Ponce, where the respondent was stopped for a routine vehicle search at the border, Petitioner was also stopped for a search prior to re-entering the United States. Similar to Ortiz and Brigoni-Ponce, where the officers justified the searches at the border with either a reasonable suspicion of the driver or simply relied on the passenger's Mexican decent, the justification for stopping Petitioner was the fact that the stop and search was routine. Similar to Ortiz, where the court acknowledged the Government's degree of discretion in the

context of border searches, but stated that the level of discretion is inconsistent with Fourth Amendment principles because of the level of intrusiveness and privacy invasion, this court must see that the search of Petitioner's car and manual search of his cell phone as equally as inconsistent with Fourth Amendment principles. It is one thing that the Petitioner's car was searched as a matter of a routine border search, however, the manual search of the cell phone should be seen as substantial invasion of privacy, warranting at minimum reasonable suspicion to justify such a search. Although Agent Stubbs ensured that the phone and laptop were disconnected from Wi-Fi, that still does not take away the fact that there are personal and other information stored on a person's phone or laptop that can be accessed without internet. The search of something that personal in nature, even manually, can subject a person, a US citizen like Petitioner, to levels of indignity that would render any search inconsistent with the Fourth Amendment. Even though this principle has been applied to the likes of strip searches, x-rays, and other searches intimate in nature, the phone and laptop are akin to these sensitive criteria with the type and amount of personal information that can be stored on them, making a search of those comparable to that of a strip search, and thus should require reasonable suspicion.

Similar to Brigoni-Ponce, and Ortiz, where officers had criteria or standards that would lead them to determine there was reasonable suspicion enough to search a car, this court should consider that there is precedent that states criteria and standards that make up reasonable suspicion. Although most precedent has found that either reasonable suspicion is not required or was found, courts have ironically made reasonable suspicion a standard that is used and ultimately found in the case to justify most of the border searches that occur. The petitioner's case should be reviewed in the same light, and reasonable suspicion not be determined to be

unnecessary simply because precedent has leaned more toward the government. Ultimately, this court should find that reasonable suspicion is required for forensic searches of electronics at the border because of the invasiveness of the search of a cellphone or laptop can reveal just as much as a physical strip search of a body, subjecting a person, like petitioner, to suffer a great amount of indignity that is inconsistent with longstanding Fourth Amendment principles.

Additionally, unlike Touset and Montoya de Hernandez where suspicion was raised due to prior travels and returning from places where sex tourism or drugs were rampant, Petitioner was just returning back from Mexico, with no prior investigations on his whereabouts or travel patterns. There was no particularized or objective reason to raise reasonable suspicion to justify a manual search of Petitioner's phone or laptop. However, unlike Touset and Montoya de Hernandez, where the circumstances surrounding the stop and search were linked to objective reasons like prior criminal activity, prior investigations on such criminal activity, or tips from other organizations that assisted in the investigations, none of those circumstances were present in Petitioner's case. In fact, the manual search turned up no incriminating evidence. It was not until Petitioner's electronic devices were forensically searched and that information was submitted to the FBI, that objective means were established to justify reasonable suspicion that Petitioner was involved in ATM Skimming. Although searches of electronics are not like the physically searches where a person is touched by an agent, the minority in both opinions warn that the broad and overreaching power these cases give the government at the border to dispense with the Fourth Amendment in the name of national security is daunting and must be monitored. That is the responsibility of this court in our technologically advancing society. To acknowledge that reasonable suspicion is required in searches at the border and that the government cannot

just dispense with an integral protection of citizen's privacy without at least a reasonable suspicion for doing so in light of the totality of the circumstances. Therefore, the court incorrectly held that reasonable suspicion is not required for searches of electronic devices at the border.

II. THE COURT INCORRECTLY HELD THAT THE FORENSIC SEARCH OF PETITIONER'S ELECTRONIC DEVICES DOES NOT REQUIRE REASONABLE SUSPICION WHEN THE LEVEL OF INTRUSIVENESS TRIGGERS A NEED OF REASONABLE SUSPICION TO PROTECT PETITIONER'S PRIVACY CONCERNS.

The court incorrectly held that reasonable suspicion is not required for a forensic search of electronics at the border. The Fourth Amendment commands that searches and seizures be reasonable, and what is reasonable depends upon all of the circumstances surrounding the search or seizure and the nature of the search itself. U.S. v. Montoya De Hernandez, 105 S.Ct. 3304, 3308 (1985). It 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. U.S. v. Cotterman, 709 F.3d 952, 962 (9th Cir. 2013); in fact, when privacy concerns are weighty enough, a search may require a warrant, notwithstanding the diminished privacy expectations of the arrestee. Riley v. California, 134 S.Ct. 2473, 2488 (2014).

In Riley, the court held that searches of electronics required reasonable suspicion and a warrant. Id. at 2495. Riley was pulled over for expired tags, and was subsequently arrested when a search at impound turned up concealed and loaded firearms. Id. at 2480. The arresting officer seized a cell phone from Riley's pant pocket. Id. The police officer accessed some information on the phone, which alluded to some gang affiliated text chains. Id. At the police station, two hours after the arrest, a detective specializing in gangs went through the phone looking for

evidence since gang members like to video themselves with guns. Id. Photos on the phone showed Riley standing in front of a car that was suspected to be involved in a shooting a few weeks ago, which led to Riley being charged in connection to the shooting. Id. at 2481. The court reasoned that diminished privacy interests of the arrestee does not mean that the Fourth Amendment is dispensed with entirely. Id. at 2488. The possible intrusion on privacy is not physically limited when it comes to cellphones, Id. at 2489, since the element of pervasiveness characterizes the very nature of the amount of personal information stored on cell phones, and not physical records. Id.

Also, in U.S. v. Saboonchi, the court held that reasonable suspicion was required to search the electronic devices. 990 F.Supp.2d 536, 549. Saboonchi and his wife were stopped by US Customs and Border Protection agents outside of Buffalo, New York after returning from a day trip to Canada. Id. at 539. Without his knowledge and consent, all of his electronic devices seized with the intent to search, which he claims had no real justification for why the devices were kept. Id. The officer that conducted the secondary search on Saboonchi when he re-entered the U.S. stated that his name got two hits on the TECS system, and he was questioned about an internship he held in an Iranian business. Id. at 540. The court reasoned that when a search reaches beyond the routine, it must rest on a reasonable, particularized suspicion, Id. at 545, since this is required due to the high expectation of privacy. Id. at 551. Accordingly, even if the search is not destructive or damaging, if it is sufficiently invasive or intrusive, or butts up against other Fourth Amendment values, it may be non-routine in any event. Id. at 552.

Similarly, in U.S. v. Ramos, the court held that requiring reasonable suspicion for forensic searches and manual searches would likely impose only minimum burdens on customs

officials' current methods. 190 F.Supp.3d 992, 1003 (S.D.Cal. 2016). Defendant Ramos entered the U.S. form Mexico, when a narcotics detector dog pinpointed defendant's backseat. Id. at 994. The secondary inspection of the car revealed eleven packages of methamphetamine in the backseat and additional packages in the gas tank. Id. Agents conducted a manual search of his cell phone, taking screen shots of incoming calls, texts messages, and select contacts, and with a warrant, completed a forensic search of the cell phone. Id. at 995. The court reasoned that cell phones contain information about every aspect of life, creating unique privacy concerns led the Supreme Court to conclude that a search of a modern cell phone could be more intrusive than a person's home. Id. at 1002.

Contrastingly, the court in U.S. v. Ramsey held that the search of the envelopes did not violate any aspects of defendant's Fourth Amendment rights. 97 S.Ct. 1972, 1983 (1977). Ramsey and Kelly jointly commenced a heroin-by-mail enterprise out of the Washington D.C. area, mailing and receiving the packages primarily from Thailand. Id. at 1974. Associates of Ramsey had recently been arrested with eleven heroin filled envelopes, which linked them back to

Ramsey and Kelly. Id. at 1975. Two days after the arrest, a United States Customs officer inspected a sack of international mail from Thailand, and with the knowledge that it was a source country for heroin, weighed and opened the letters, which contained heroin. Id. The envelopes were addressed to the D.C. area, and were sent there to be used by DEA agents to capture the recipients. Id. Ramsey and Kelly were arrested after the envelopes were received and the drop was made. Id. at 1976. The court reasoned that with the wealth of authority afforded to the government establishing border searches as reasonable, no distinction need to be made as to whether there was intrusiveness or reasonable cause to believe that customs laws are being

violated. Id. at 1982.

Like Riley and Ramos, where the court dictated that the level of intrusiveness a forensic search can reach far beyond that of the search of physical documents due to the amount and type of information stored on a phone, Petitioner's forensic search of his devices exhibits the same level of intrusiveness. Similar to Riley, where respondent was charged for the suspected connection to a crime after a photo was discovered on the search of his phone, Petitioner was charged with the Bank fraud, Conspiracy to Commit Bank Fraud, and Aggravated Identity Theft after the information provided by the forensic search prompted an investigation of his suspected involvement. Similar to Saboonchi, where the forensic search of his electronic devices stretched beyond routine, the search of Petitioner's devices is also non-routine, since the initial manual search turned up no incriminating evidence, and being unable the folders and USB drives initiated a forensic search. The initiation of the forensic search of Petitioner's electronic devices after not being able to open up portions of the files on the laptop and the USB drives should have triggered the need for reasonable suspicion to do so. It is the responsibility of this court to acknowledge that the privacy concerns of Petitioner are different when it comes to electronic devices because even if the search is not destructive or damaging, if it is sufficiently invasive or intrusive, or contradicts other Fourth Amendment values, it may be non-routine in any event, as stated in Saboonchi.

Unlike Ramsey, where the court attributed no distinction between electronics and physical property when it comes to reasonable suspicion and border searches, that distinction must be made for the Petitioner. The reasonable suspicion requirement is more like the case of Ramos, where the court reasoned that cell phones contain information about every aspect of life,

creating unique privacy concerns led the Supreme Court to conclude that a search of a modern cell phone could be more intrusive than a person's home. The distinction must be made because of the intrusiveness of the search and the fact that electronic devices go with a person everywhere. It is this level of intrusiveness that triggers a need for reasonable suspicion, and absent that, conflicts with the Fourth Amendment's principles that make persons secure in themselves and their effects. Petitioner's privacy interests were intruded upon at this level, and there require reasonable suspicion to be applied in this respect to honor the long standing principles that are awarded by the Fourth Amendment. Therefore, this court should rule that reasonable suspicion is required to forensically search electronic devices at the border.

The failure of the lower courts to analyze this Court's decision in Carpenter v. United States is not their own, but rather the lack of a proper test in the determination of what triggers a person's right to Fourth Amendment protection with regard to our technologically advancing world. 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." The "basic purpose of this Amendment," our cases have recognized, "is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." ." Carpenter citing Camara v. Municipal Court of City and County of San Francisco, 387 U. S. 523, 528, 87 S. Ct. 1727, 18 L. Ed. 2d 930 (1967). Justice Gorsuch stated himself, "We have arrived here [not because the court has misunderstood Katz, but] because this is where Katz inevitably leads." Id. at 577. It is not for the lower courts to determine the direction in which Katz and the Fourth Amendment give way to modern technology, but rather for this court to decide the boundaries that must be drawn in a modern society.

III. THE 14TH CIRCUIT INCORRECTLY AFFIRMED THE DISTRICT COURT'S RULING DENYING PETITIONER'S MOTION TO SUPPRESS THE CELL SITE LOCATION INFORMATION GATHERED PURSUANT TO 18 U.S.C. § 2703(D), BECAUSE THE INFORMATION WAS A FRUIT OF THE ILLEGAL SEARCH IN VIOLATION OF THE FOURTH AMENDMENT, AS WELL AS A VIOLATION OF PETITIONER'S EXPECTATION OF PRIVACY WITH REGARD TO A RETROACTIVE RECORD OF HIS PHYSICAL MOVEMENTS.

A forensic search was conducted on the personal property of Petitioner, without a particularized or objective reason for suspicion. The Exclusionary Rule applies to evidence that was the fruit of an illegal search, or rather the direct or indirect product of a search that if included would allow for a violation of the constitutional protections of the sanctity of a person and his effects. Wong Sun v. United States, 371 U.S. 471, 83 S. Ct. 407, 9 L. Ed. 2d 441, 1963. Even if the search was incorrectly found to be legal, Petitioner argues that his expectation of privacy was violated with regard to the warrantless acquisition of his Cell-Site-Location-Information (CSLI), pursuant to this Court's analysis of Carpenter v. United States. With the advancement of technology leading to the enhancement of the government's ability to encroach on the privacies of the people's day to day lives, this court has sought to preserve the degree of privacy that existed upon the adoption of the Fourth Amendment. Carpenter at 517. In order to continue to preserve the same standard of privacy that was at the founding of the Fourth Amendment, this Court must decide how much power they are willing to allow the government to open a window into the day to day lives of the average individual, whether it be freely, or with the traditional standard of a warrant acquired through probable cause.

A. The warrantless acquisition of cell tower dumps, three days of CSLI and 100 cumulative hours over two weeks of CSLI pursuant to 18 U.S.C. § 2703(d) was an unreasonable intrusion with respect to Petitioner's expectation of privacy, not governed by the Third-Party Doctrine.

A Cell Tower Dump (CTD) is a technique law enforcement officials use to determine whether or not a suspect was in a certain area during a specific period of time. R4.

Unlike the collection of CSLI, a CTD does not specifically pull out all information from a suspect, but rather pulls all information from a specific tower, including all people that have connected to that tower during the specified period. R4. The use of CTD should not only be limited with regards to the selling of said information to third parties for purposes of privacy as stated in Carpenter, but banned for its intrusiveness without the use of a specified warrant. Carpenter at 521.

The Fourteenth Circuit's analysis of Carpenter placed the restrictions of CSLI use by law enforcement on a time or day basis, rather than a reasoning basis, stating, "To hold otherwise, lower courts and law enforcement would be forced to repeatedly answer the same question that Carpenter purportedly decided, yet on iteratively smaller scales, a legal matryoshka doll. Rather than reassess an individual's privacy right in historical cell cite location data, lower courts would instead reassess six-day warrantless CSLI requests, then five-day requests, then four." R11. However, this Court never suggested that fewer than six days does or does not constitute a Fourth Amendment search, but rather reiterated that individuals have a reasonable expectation of privacy in the whole of their physical movements and that allowing government access to cell-site records which have a record of their every movement contravenes that expectation. Carpenter at 521 citing Jones v. United States, 565 U.S. at 430, 132 S. Ct. 945, 181 L. Ed. 2d 911. As an entirely different species of business record, a warrant with a showing of probable cause is required for the acquisition of CSLI, outside of the scope of the third-party doctrine and 18 U.S.C. § 2703(d). Id. at 526.

The fourteenth district focuses mostly on this courts minority opinions in Carpenter on its adaptation of Smith v. Md., 442 U.S. 735, 99 S. Ct. 2577, 61 L. Ed. 2d 220, 1979 and United States v. Miller, 425 U.S. 435, 96 S. Ct. 1619, 48 L. Ed. 2d 71, 1976. In Smith, a reasonable

expectation test was formed, where a court would determine 1) if defendant had a subjective expectation of privacy given the activity, and 2) if the subjective expectation is one society is willing to perceive as reasonable. Id. at 740. The police in Smith had installed a pen register at the telephone company's office in order to determine the numbers being dialed by petitioner. Id. at 736-7. In 1979, this court had found that gathering this information was not a violation of Petitioner's Fourth Amendment protections, since there was no expectation of privacy in the numbers being dialed. Id. at 738.

Though the fourteenth circuit and this court's minority in Carpenter believe the issue before us has been decided in Smith, the difference lies in the intrusiveness of the search. Both Carpenter and Smith involved phone company business records, separated by almost forty years. At the time, CSLI was not available in Smith as it was in Carpenter. However, the reasoning behind the Smith court was the lack of a reasonable expectation of privacy in phone numbers dialed, while Carpenter decided the issue based on there being a reasonable expectation of privacy in the business records relating to CSLI due to the intrusiveness of obtaining geographical information of a person without a warrant.

In the case before us, Petitioner was not only the subject of an illegal forensic search at the border, but also the subject of a warrantless search. The fourteenth circuit agrees no reasonable suspicion or probable cause existed for the acquisition of CSLI, but rather the search was made through a court order under the Stored Communications Act (SCA). However, this court in Carpenter decided that warrants are required when the suspect has a legitimate privacy interest in records held by a third party. Carpenter at 526. In Smith, the records merely contained information relating to numbers dialed, while the records in our case are tantamount to GPS tracking, where this court has constantly ruled against warrantless tracking of a person's physical

movements given some exigent circumstances not present in our case. Furthermore, Petitioner believes that he met the test under the Smith standard, as his expectation of privacy was reasonable, and society at large would reasonably view that expectation as adequate for the test, given the intrusiveness and ability of your every move being recorded and viewed through CSLI under the SCA.

In Miller, this Court decided that bank records were not under Fourth Amendment protection, due to the fact that defendant bank records are considered third party information not protected under the Fourth Amendment. Miller at 444. According to this court, Miller had no expectation of privacy in bank records, as they were third party business records relating to the underlying alleged crime of tax evasion, and banks have a duty of reporting suspicious activity in the first place.

In our case, the records were not related to the underlying crime alleged, but rather contained detailed, encyclopedic, and effortlessly compiled geographical data of Petitioner's every movement for as long as the records were kept. Carpenter at 521. The records were less business records, and more GPS records like that of an ankle monitor. Id. at 524. When Petitioner was first under investigation, the fourteenth circuit agrees no probable cause existed, or reasonable suspicion for the initial forensic search, but rather that reasonable grounds existed for believing the records were relevant and material to an ongoing investigation pursuant to 18 U.S.C. § 2703(d), which is a blatant violation of the Fourth Amendment with regards to the physical person.

In Carpenter, this court adds that in their decision in Kyllo v. United States, they addressed the issue of technology now being able to easily circumvent the protections of the Fourth Amendment.

> "As technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to "assure[ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." Kyllo v. United States, 533 U.S. 27, 34, 121 S. Ct. 2038, 150 L. Ed. 2d 94 (2001).

When this court decided the issue in Kyllo, the warrantless search was considered unreasonable due to the fact that the technology was not in general public use. Id. at 34. The thermal scanner used to determine that heat lamps were being used to grow marijuana inside did not show intimate details of Defendant's life, but was intrusive enough for this court to see as a violation of the Fourth Amendment. Id. at 34.

Petitioner had a reasonable expectation of privacy regarding all his movements, during the three days, and the 100 hours over two weeks. The warrantless acquisition of Petitioner's CSLI was intrusive as it not only revealed Petitioner's location at one point in time, but across a span of 13 different days. The fourteenth circuit and Respondent argued that the total amount of time may have amounted to less than seven days. According to the fourteenth Circuit's interpretation of Carpenter, this court made the acquisition of CSLI for less than seven days allowable under the SCA. However, as this court stated in Kyllo and in Carpenter, the CSLI acquired without a warrant reveals intimate facets of Petitioner's life, tantamount to an ankle monitor, or GPS tracker, but without the need for a warrant. It is that similarity that the court in Carpenter warns about, and is seen in the present case.

Contrary to the fourteenth circuit and this court's minority opinion in Carpenter, the acquisition of CSLI records in our case raise serious Fourth Amendment issues. If the SCA is allowed to grant the government complete access to anyone's geographical information based on

their CSLI, this Court would be granting law enforcement the ability to circumvent the Fourth Amendment, rather than protecting the rights of the people as a whole, and therefore abandoning the belief that Fourth Amendment protections must advance with technology, as this court explained in Kyllo and Carpenter.

CONCLUSION

In closing, Petitioner's Fourth Amendment rights had been violated through the forensic search of all of Petitioner's electronic devices, as well as the subsequent fruits of the illegal search, including the cell tower dump, three days of CSLI information, and 100 hours of CSLI information from a span of two weeks. Petitioner respectfully requests that this court reverse the decision of the lower court, finding that Petitioner's Fourth Amendment rights were violated.

Dated: February 10, 2018

Respectfully Submitted,

Attorneys for
Petitioner