Docket 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 OF PETITIONER

Team 9
Counsel for Petitioner

TABLE OF CONTENTS

TABLE OF AUTHORITIES

QUESTIONS PRESENTED

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

II. Consistent with the Supreme Court's ruling in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), limiting the use of cell-site location information (CLSI), does the government's acquisitions pursuant to 18 U.S.C. § 2703(d) of three days of CSLI, 100 cumulative hours of CSLI over two weeks, and cell-site location information collected from cell tower dumps violate the Fourth Amendment?

OPINION BELOW

The United States Court of Appeals for the Fourteenth Circuit affirmed the decision of the United States District Court for the District of West Texas to deny Mr. Escaton's motion to suppress, holding that the government agents did not violate the Fourth Amendment.[1]

CONSTITUTIONAL PROVISIONS AND RULES

This case involves the Fourth Amendment to the United States Constitution.

> "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."[2]

STANDARD OF REVIEW

In reviewing the Court of Appeal's denial of the motion to suppress, the Court should review the legal conclusions de novo and its factual findings for clear error, considering the evidence in the light most favorable to the government.[3]

---

[1] *Escaton v. United States*, 1001 F.3d 1341 (14th Cir. 2021).
[2] U.S. CONST. amend. IV.
[3] *See United States v. Kolsuz*, 890 F.3d 133, 141-142 (2018).

INTRODUCTION

Summary of the argument

To protect individual privacy interests, the United States Supreme Court should reverse the lower court's decision to deny the petitioner's motion to suppress evidence seized from his vehicle during a warrantless search at the border.

Generally, border searches are reasonable simply because they occur at the border; however, the Supreme Court has distinguished a category of non-routine searches that require reasonable, individualized suspicion.[1] Non-routine border searches include highly intrusive searches which implicate significant privacy interests, as well as any particularly destructive search or searches which are carried out in a substantially offensive way.[2] Cell phones and similar technology, contain uniquely sensitive information which make forensic searches even more intrusive than any other search of property.[3] The forensic search of the petitioner's phone was unreasonable in the absence of any reasonable suspicion. The vast quantities and sensitive nature of the data on an individual's electronic devices should be protected, even at the border. In addition, although there is a strong government interest in protecting the border, when weighed against the substantial privacy interest of the individual, reasonable suspicion is the proper standard to protect both parties.

Reasonable suspicion is defined as "a particularized and objective basis for suspecting the particular person stopped of criminal activity."[4] The assessment of reasonable suspicion is made in light of the totality of the circumstances known to the officer at the time of the stop.[5] It is clear that the government, at the time of petitioner's stop, had no particularized suspicion to suspect

---

[1] *See United States v. Montoya de Hernandez*, 473 U.S. 531, 541 (1985).
[2] *See United States v. Flores-Montano*, 541 U.S. 149, 152, 156 (2004).
[3] *United States v. Cotterman*, 709 F.3d 952, 966 (9th Cir. 2013).
[4] *United States v. Cortez*, 449 U.S. 411, 417-18 (1981).
[5] *Cotterman*, 709 F.3d at 968.

the petitioner of any criminal wrongdoing. There was no indication of any reason for the stop besides a routine border search, and the initial cursory search revealed no incriminating evidence giving rise to reasonable suspicion. Therefore, there was no reasonable basis for conducting the forensic search.

Furthermore, law enforcement should have applied for a warrant based upon probable cause before it was able to obtain three days of the petitioner's cell-site location information, 100 cumulative hours of the petitioner's cell-site location information over two weeks, and cell-site location information collected from cell tower dumps. The Supreme Court held in *United States v. Carpenter*[6] that the privacy interests associated with such information are so great that they warrant Fourth Amendment protection. The reasoning in *Carpenter* should apply even if the timeframe is fewer than seven days and even if it is limited to certain hours within the day. Further, it would be extended to cell tower dumps because of the Court's decision regarding the third-party doctrine in *Carpenter* and the expectation of privacy innocent individuals have in their whereabouts.

For these reasons, the United States Supreme Court should reverse the lower court's decision to deny the petitioner's motion to suppress evidence seized from his vehicle during a warrantless search at the border.

STATEMENT OF THE CASE

Statement of facts

Petitioner Hector Escaton is a United States citizen who enjoys all the rights and privileges afforded to him under the United States Constitution. He was very likely one of thousands of United States citizens who crossed over the Mexican border into his home state of

[6] 138 S. Ct. 2206, 2210 (2018).

West Texas on September 25, 2019.[7] Although he was following all laws and presented nothing visually suspicious while he was reentering his home country, the petitioner was stopped for a random and "routine border search."[8] During the random search, a Customs and Border Protection (CBP) officer found three large yet unassuming suitcases in the back of the petitioner's car.[9] Even though suitcases are typical travel items, the CBP officer felt compelled to search them for reasons that were not articulated, aside from being subject to a "routine" search.[10] In the search, the CBP officer found and conducted a warrantless search of the contents of an iPhone and a laptop even though he lacked any articulable suspicion.[11] The CBP officer also found and attempted to search three external hard drives and four USB drives.[12]

Despite not finding anything suspicious in his warrantless searches, the CBP officer seized the laptop, hard drives, and USB drives.[13] He returned only the iPhone to the petitioner. The other electronics were given to an Immigration and Customs Enforcement (ICE) agent who used forensic software to copy and scan the devices, a process that typically takes several hours. The ICE agent reported finding documents on the laptop that contained individuals' bank account numbers and pins as well as traces of malware on the USB drives. No incriminating information was found on the hard drives.[14]

The ICE agent reported her limited findings to the Federal Bureau of Investigation, which had been investigating ATM skimming at Mariposa Bank ATMs in Sweetwater almost one year earlier in October 2018.[15] Using information provided by the bank and forensic search

---

[7] (R. at 2).
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] *Id*. at 3.
[13] *Id.*
[14] *Id.*
[15] *Id.*

information from CBP, the FBI in coordination with the U.S. Attorney's Office requested three tower dumps from the cell sites near three Sweetwater ATMs for 30 minutes before and 30 minutes after a man in a black sweatshirt approached the ATMs.

The CBP officer reported information found during the warrantless search of the petitioner's belongings to the FBI for potential bank fraud and identity theft claims.[16] While the malware found on the petitioner's USB drives did not match the malware used at Mariposa ATMs in Sweetwater, the petitioner's phone number did match one of the thousands of phone numbers generated from the three tower dumps. Based only on that information, the U.S. Attorney applied for court orders to obtain the petitioner's cell phone records, and a federal magistrate issued an order directing Delos Wireless to disclose the petitioner's cell site records from October 11, 2018, through October 13, 2018.[17] The three-day records placed the petitioner's cell phone in the area of the Sweetwater Boswell Branch ATM on October 12, 2018. The petitioner's cell phone was not in Escalante on those dates.[18]

The government, however, did not stop there. Using a sticky note found on the petitioner's laptop with the name Delores and phone number (201) 181-0981, the government requested, and a magistrate subsequently issued an additional order to Delos Wireless to disclose cell site information for the petitioner's and Delores' numbers for every weekday between October 1 and October 12 between 8 a.m. and 6 p.m. as well as subscriber information for Delores' phone.[19] Those records identified Delores as Delores Abernathy and placed her phone in the area of the three Escalante ATMs in early October. The CSLI records obtained from Delos also placed the petitioner in the same area as Abernathy during the same time period. [20]

---

[16] *Id.* at 5.
[17] *Id.*
[18] *Id.*
[19] *Id.*
[20] *Id.*

Abernathy had been previously convicted for ATM skimming.[21] After linking Abernathy to the Escalante ATMs, law enforcement indicted her and obtained a search warrant for her house, where they found cash and the same malware that the petitioner stored on his USB devices. After Abernathy was arrested, she entered a plea agreement and cooperated with the government in its case against the petitioner.[22]

Procedural posture

The petitioner was indicted in the United States District Court for the District of West Texas for single counts of bank fraud, 18 U.S.C. § 1344, conspiracy to commit bank fraud, 18 U.S.C. § 1349, and aggravated identity theft, 18 U.S.C. § 1028A. Before a jury trial, the petitioner filed a motion to suppress all evidence obtained through the warrantless search of his electronics as well as the cell-site data from Delos Wireless as violative of the Fourth Amendment to the United States Constitution. The district court denied the motion on both issues and the case proceeded to trial. The petitioner was convicted on all three charges. He then appealed to the United States Court of Appeals for the Fourteenth Circuit arguing that the district court erred in denying his motion to suppress. Oral arguments were held September 11, 2021, and the court affirmed the district court's ruling denying the petitioner's motion to suppress on November 2, 2021, holding that the government agents did not violate the Fourth Amendment.[23] The petitioner subsequently filed a writ of certiorari to the United States Supreme Court, and review was granted on November 22, 2022. Jurisdiction is appropriate under 28 U.S.C. § 1254(1).

---

[21] *Id.*
[22] *Id.* at 5-6.
[23] *Escaton v. United States*, 1001 F.3d 1341 (14th Cir. 2021).

ARGUMENT

I. GOVERNMENT OFFICERS MUST HAVE REASONABLE SUSPICION BEFORE CONDUCTING A FORENSIC SEARCH OF AN ELECTRONIC DEVICE AT AN INTERNATIONAL BORDER.

The Fourth Amendment ensures 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, and no Warrants shall issue, but upon probable cause . . . ."[24] Typically, the Fourth Amendment requires that law enforcement searches be accompanied by a warrant based on probable cause.[25] However, border searches, or their functional equivalent, are different.[26] As an exception to the warrant requirement, searches conducted at an international border never require probable cause or a warrant.[27] The border exception is rooted in the principle that it is a recognized right of the sovereign to control who and what may enter the country.[28] Under this exception, routine searches and seizures occurring at the border, or its functional equivalent, are exempted from standard Fourth Amendment requirements so that the government can prevent contraband or person's who seek to bring diseases, narcotics, or explosives from entering the country.[29] Border searches are generally, though not always, deemed reasonable simply by virtue of the fact that they occur at the border.[30]

Courts have long recognized border searches as an exception to the Fourth Amendment's customary rule requiring a warrant; however, this does not mean that "anything goes" during

---

[24] U.S. Const. amend. IV.
[25] *See United States v. Kolsuz*, 890 F.3d at 137 (2018) (citing *Arizona v. Gant*, 556 U.S. 332, 338 (2009)).
[26] *United States v. Touset*, 890 F.3d 1227, 1232 (11th Cir. 2018).
[27] *Id.*
[28] *Kolsuz*, 890 F.3d at 137. *See United States v. Ramsey*, 431 U.S. 606, 620 (1977); *see Flores-Montano*, 541 U.S. at 152 (border exception rests on government interest in "preventing the entry of unwanted persons and effects").
[29] *Kolsuz*, 890 F.3d at 137; *Montoya de Hernandez*, 473 U.S. at 537, 544.
[30] *Cotterman*, 709 F.3d at 960; *See Ramsey*, 431 U.S. at 616.

border searches.[31] The government's authority to act is not without limits.[32] During border searches, individual privacy should not be and is not abandoned, but rather, the privacy interest is "balanced against the sovereign's interests," in protecting the country.[33] This balancing test is weighed favorably for the government.[34] Although the scales are weighed in favor of the government, the ultimate touchstone of the Fourth Amendment still requires that a search and seizure is reasonable.[35]

When analyzing the reasonableness of a search or seizure, the court should consider the totality of the circumstances, including the nature, scope and duration of the search or deprivation.[36] The Supreme Court recognized that the privacy interests of persons being searched at the border will sometimes necessitate the need for some level of individualized suspicion in order to conduct highly intrusive searches of a person.[37] In addition, the Court acknowledged that even some searches of property require particularized suspicion, especially when the search is considered destructive, particularly offensive or overly intrusive in scope and nature.[38] However, although the Court has never delineated a bright-line rule regarding what is a reasonable border search, it has stated the need for case-by-case analysis.[39]

a. A forensic search of an electronic device is non-routine and requires individualized suspicion.

---

[31] *Cotterman*, 709 F.3d at 957; *See Ramsey,* 431 U.S. at 621; *See also United States v. Seljan,* 547 F.3d 993, 1000 (9th Cir. 2008)
[32] *See Kolsuz*, 890 F.3d 133 at 137.
[33] *Montoya de Hernandez*, 473 U.S. at 539.
[34] *Cotterman*, 709 F.3d at 960.
[35] *See Kolsuz*, 890 F.3d at 138; *see also Riley v. California*, 134 S. Ct. 2473, 2482 (2014); *see also Montoya de Hernandez,* 473 U.S. at 538.
[36] *Cotterman*, 709 F.3d at 960; *See also United States v. Jacobsen*, 466 U.S. 109, 124 (1984).
[37] *Cotterman*, 709 F.3d at 963; *Flores-Montano*, 541 U.S. at 152
[38] *Cotterman*, 709 F.3d at 963.
[39] *Id.*

As previously mentioned, at a border or functional equivalent, government agents may conduct routine searches and seizures of persons and property without a warrant or any suspicion.[40] While border searches are generally reasonable simply because they occur at the border, the Supreme Court has distinguished a category of non-routine searches that require reasonable, individualized suspicion.[41] Non-routine border searches include highly intrusive searches which implicate significant privacy interests, as well as any particularly destructive search or searches which are carried out in a substantially offensive way.[42] Border searches of luggage, clothing and personal effects are treated as routine, while searches that involve a significant invasion of privacy including strip searches, alimentary-canal searches, and x-rays are deemed nonroutine and allowed only with reasonable suspicion.[43]

Despite the sensitive information contained on electronic devices, they are not immune to border searches.[44] Reasonableness is the proper inquiry; however, this determination must account for differences in property.[45] After the Court's decision in *Riley*, it is clear that a forensic search of a phone or laptop must be treated as non-routine, and impermissible in the absence of individualized suspicion.[46] In *Riley*, the Court held that because of the breadth and sensitivity of

---

[40] *Kolsuz*, 890 F.3d at 137; *Montoya de Hernandez*, 473 U.S. at 538 (1985).
[41] *See Montoya de Hernandez,* 473 U.S. at 541 ("holding that overnight detention for monitored bowel movement followed by rectal examination is 'beyond the scope of a routine customs search' and permissible under the border exception only with reasonable suspicion").
[42] *See Flores-Montano*, 541 U.S. at 152, 156 ("While it may be true that some searches of property are so destructive as to require a different result, this was not one of them"); *See also Montoya de Hernandez*, 473 U.S. at 541 ("the detention of a traveler at the border, beyond the scope of a routine customs search and inspection, is justified at its inception if customs agents, considering all the facts surrounding the traveler and her trip, reasonably suspect that the traveler is smuggling contraband in her alimentary canal.").
[43] *Kolsuz,* 890 F.3d at 144.
[44] *Cotterman*, 709 F.3d at 966.
[45] See *Samson v. California*, 547 U.S. 843, 848 (2006) (Under our general Fourth Amendment approach, we examine the totality of the circumstances to determine whether a search is reasonable)
[46] *Kolsuz*, 890 F.3d at 144; *See, generally Riley*, 134 S. Ct. 2473 (2014).

private information stored on smart phones and other such technology, a forensic search of a phone cannot be analogized to an ordinary search of luggage or other containers.[47] Cell phones and similar technology, contain uniquely sensitive information which make forensic searches even more intrusive than any other search of property.[48] Analysis regarding the intrusiveness of a search should consider both the extent of a search as well as the degree of indignity that may accompany it.[49]

A border search where government officials search an individual's property, including situations where government officials disassemble an individual's gas tank in search of contraband, is less intrusive than a forensic search of an electronic device. In *Flores-Montano*, customs officials found contraband in the defendant's gas tank during a routine search of the vehicle at the border.[50] In denying the defendant's motion to suppress the evidence found without reasonable suspicion, the court found that the reasons for a "requirement of some level of suspicion in the case of highly intrusive searches of the person—dignity and privacy interests—simply do not carry over to vehicles."[51] In reaching this conclusion, the court found that the search of a gas tank, unlike more intrusive searches, takes only about 25 minutes and does not subject the individual to a substantial invasion of privacy interest common of more destructive or intrusive searches.[52]

A forensic search of an electronic device is a substantial intrusion upon the personal privacy and dignity of an individual.[53] In *Cotterman*, the Ninth Circuit held that the uniquely

---

[47] *Kolsuz*, 890 F.3d at 140.
[48] *Cotterman*, 709 F.3d at 966.
[49] *Id.*
[50] *Flores-Montano*, 541 U.S. at 150-151.
[51] *Id.* at 152.
[52] *See Id*., generally.
[53] *Cotterman,* 709 F.3d at 968.

sensitive nature of data on electronic devices carries with it a significant expectation of privacy and thus renders an exhaustive exploratory search more intrusive than with other forms of property. [54] In the case, after copying the individual's hard drives, it took days for the forensic evaluation to discover contraband. [55] The Court assessed this process and determined that forensic searches intrude upon privacy interest to a far greater degree than any cursory search at the border. In conclusion, the Court analogized forensic searches of electronic devices to "a computer strip search."[56]

The nature of a forensic search of electronic devices differs from that of a cursory search of property. Unlike forensic searches, the Court has made it abundantly clear that routine, cursory border searches of property are acceptable even in the absence of reasonable suspicion.[57] In view of this principle allowing "routine" cursory searches, it is clear that the initial search of the petitioner's luggage was in line with the border search exception of the 4th Amendment. This includes the cursory search of the car, luggage and a quick-view of the laptop and phone. If the search had stopped here, it is likely the search would have been reasonable despite the lack of reasonable suspicion. However, this search transformed into something more when the agents, without any indication of reasonable suspicion following the initial cursory search, seized the laptop and hard drives for more thorough forensic examination. The thoroughness inherent in any forensic search which typically includes the revealing of the most intimate details of one's life is a substantial intrusion upon personal privacy and dignity.

---

[54] *Id.* at 966.
[55] *Id*.
[56] *Id.*
[57] *Kolsuz*, 890 F.3d at 137; *Montoya de Hernandez*, 473 U.S. at 538; See also *Seljan*, 547 F.3d at 1004 (suspicion-less cursory scan of a package in international transit was not unreasonable; See also *United States v. Arnold,* 533 F.3d 1003, 1009 (9th Cir. 2008) (quick look and unintrusive search of laptops acceptable).

A forensic search of a targeted individual's electronic devices is significantly more intrusive than any other search of property. Unlike the search involved in *Flores-Montano* where officers conducted a search of the individual's gas tank, the search that the petitioner was subjected to involved vast amounts of data taken from his electronic devices. In addition to his luggage, the government officials search included an iPhone (which was not forensically searched), laptop, three external hard drives and four USB drives. The rest of the items were forensically searched. This widely differs from the privacy expectation and intrusive nature of disassembling a gas tank. Although gas tank searches are intrusive, gas tanks do not store private information which there is a legitimate privacy interest in protecting; however, electronic devices contain the most intimate details of our lives: financial records, confidential business documents, medical records and private emails.[58] Unlike a gas tank which may be reassembled, once private and confidential information is revealed, it cannot be undone.

Although it is commonly known to travelers that there is a diminished expectation of privacy at an international border and that their bags may be searched, travelers do not anticipate, absent some individualized suspicion, that government officials will perform exhaustive and intrusive search of all of the data on their electronic devices.[59] Electronic devices, unlike typical luggage, are capable of storing vast amounts of date. In addition, laptops, smart phones and other electronic devices serve multiple functions and contain both business and private information.[60]

Whereas the amount of private information carried by a traveler was limited to the amount of which they could carry; now, this is no longer the case. It is unreasonable to subject individuals to the embarrassment and invasion of an unlimited search of the vast amount of data on their

[58] *Cotterman*, 709 F.3d at 964.
[59] *Id*. at 967-968.
[60] *Id*. at 966.

electronic devices simply because it was not feasible to delete such data every time they traveled. It is time-consuming to effectively erase data.[61]

Although the government has a legitimate and substantial interest in protecting the border, the Fourth Amendment rights of travelers is also legitimate and must be accounted for. Implementing a reasonable suspicion standard to conduct forensic searches of phones protects both of these interests. First, for the government, reasonable suspicion is a workable standard that is already applied in extended border searches.[62] This lenient standard will not inhibit border officials from properly monitoring the border and conducting appropriate forensic examinations.[63] In addition, reasonable suspicion does not create an unobtainable bar for government officials to conduct these types of intrusive searches. Instead, this standard leaves ample room for agents to use their expertise to determine whether there is a crime occurring.[64] For individuals, it gives them a proper expectation of privacy in the extensive and potentially sensitive and confidential information stored on their electronic devices. Also, it protects individuals from being subjected to arbitrary searches and seizures.

The express guarantee of the people's right to be secure in their "papers", is evidence that the Fourth Amendment extends to forensic searches of electronic devices because of the nature of documents and information found on such platforms.[65] The Framers, by including papers, manifested an intent to safeguard the privacy of ideas and thoughts from government intrusion.[66] In conclusion, the non-routine, highly invasive nature of a forensic search of an electronic device necessitates the need for reasonable suspicion before conducting such a search.[67] Therefore, to

---

[61] *Id*. at 965.
[62] *Id*. at 966.
[63] *Id.*
[64] *See United States v. Tiong*, 224 F.3d 1136, 1140 (9th Cir. 2000).
[65] U.S. Const. amend. IV.
[66] *Seljan*, 547 F.3d at 1014 (Kozinski, C.J., dissenting).
[67] *Cotterman*, 637 F.3d at 1086-87 n.6.

determine whether the forensic search was reasonable in the case of the petitioner, it is necessary to determine whether the government agents had reasonable suspicion at the time of the stop.

b. The government lacked reasonable suspicion to conduct the forensic search of the petitioner's electronic devices.

Reasonable suspicion is defined as "a particularized and objective basis for suspecting the particular person stopped of criminal activity."[68] The assessment of reasonable suspicion is made in light of the totality of the circumstances.[69] In addition, the inquiry focuses on the information available to the officer at the time of the stop.[70] Lastly, factors considered in isolation which are vulnerable to an innocent explanation may constitute reasonable suspicion if, when viewed collectively, raise a reasonable suspicion that the targeted individual is engaged in criminal activity.[71]

Government officials cannot rely solely on factors, such as password protections for electronic devices, that would apply to many law-abiding citizens.[72] In *Cotterman*, agents discovered password protected files on an individual suspected of child pornography's computer.[73] The Court was reluctant to put much weight on this factor because it is commonplace for individuals to use password-protections for their devices.[74] The Court concluded that "to contribute to reasonable suspicion, password protection of files must have some relationship to the suspected criminal activity."[75]

---

[68] *United States v. Cortez*, 449 U.S. at 417-18.
[69] *Cotterman*, 709 F.3d at 968.
[70] *Touset*, 890 F.3d at 1237.
[71] *United States v. Berber-Tinoco*, 510 F.3d 1083, 1087 (9th Cir. 2007); *Cotterman*, 709 F.3d at 968.
[72] *Cotterman*, 709 F.3d at 969.
[73] *Id.*
[74] *Id.*
[75] *Id.*

Unlike *Touset* and *Kolsuz*, where government officials at least had a prior tip or connection between the targeted individual and criminal activity, there was no indication that the petitioner was engaged in criminal conduct when stopped at the border. Viewing the record, it appears that there was no special motivation for stopping the petitioner at the border, other than for a routine border inspection. After a search of the petitioner's vehicle, the agents found nothing suspicious. Next, although it is typical for travelers to carry suitcases, CBP decided to search the suitcases found in the petitioner's trunk without articulating any reason besides a routine stop. During the search of the suitcases, the CBP officer found and conducted a warrantless search of the petitioner's iPhone and a laptop, which contained a note under the keyboard with the message, "Call Delores (201) 181-0981 $$$." The laptop contained password protected folders. In addition, he found three external hard drives and four USB drives, which he could not access. Despite the fact that these initial warrantless and suspiciousless searches produced no incriminating evidence, the officer seized the laptop, hard drives, and USB drives. The other electronics were given to ICE who used forensic software to copy and scan the devices. Only after this extensive and exhaustive search was the petitioner implicated in a financial fraud.

In addition, the existence of password protected files, without any further indicia of criminal activity, is insufficient to create reasonable suspicion. Unlike *Cotterman,* there is no indication in the record that the petitioner was suspected of committing a crime. There is no indication of a prior criminal record, no indication that any incriminating evidence was found during the initial cursory search of the vehicle, and no indication that the petitioner was acting suspiciously at the time of the stop. Therefore, to consider password protections "suspicious" under these circumstances, would be to grant government officials reasonable suspicion for every individual with a password on their electronic devices.

Considering these standards, the government violated the Fourth Amendment when it conducted a forensic search of the petitioner's electronic devices in the absence of reasonable suspicion.

II. THE GOVERNMENT VIOLATED THE FOURTH AMENDMENT AND THE LIMITATIONS SET IN *CARPENTER* WHEN IT ACQUIRED THREE DAYS OF CELL-SITE LOCATION INFORMATION, 100 CUMULATIVE HOURS OF CELL-SITE LOCATION INFORMATION OVER TWO WEEKS, AND CELL-SITE LOCATION INFORMATION COLLECTED FROM CELL TOWER DUMPS.

The Supreme Court has recognized the Fourth Amendment protects certain privacy interests from unreasonable searches.[76] When an individual "seeks to preserve something as private," and his expectation of privacy is "one that society is prepared to recognize as reasonable," official intrusion into that sphere generally qualifies as a search and requires a warrant supported by probable cause.[77] Further, the Supreme Court has recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements. The Supreme Court previously recognized the privacy concerns associated with GPS monitoring in *United States v. Jones*.[78] In *Carpenter v. United States*, however, the Supreme Court recognized that historical cell-site records present even greater privacy concerns than GPS monitoring because CSLI gives the government near perfect surveillance and allows it to travel back in time to retrace a person's whereabouts, subject only to the five-year retention policies of most wireless carriers.[79]

In *Carpenter*, like in the present case, the government did not obtain a warrant supported by probable cause before acquiring cell-site records. Rather, it acquired records in both cases pursuant to a court order under the Stored Communications Act, which required the government

[76] *Katz v. United States*, 389 U. S. 347, 351 (1967).
[77] *Smith v. Maryland*, 442 U. S. 735, 740 (1979).
[78] 565 U. S. 400 (2012).
[79] 138 S. Ct. at 2210.

to show "reasonable grounds" for believing that the records were "relevant and material to an ongoing investigation."[80] Because of the privacy interests associated with CSLI, the Court held in *Carpenter* that an order issued under §2703(d) is not a permissible mechanism for accessing such information. Rather, the government must get a warrant unless case-specific exceptions support a warrantless search.[81] Such exceptions involve exigent circumstances, which include the need to pursue a fleeing suspect, protect individuals who are threatened with imminent harm, or prevent the imminent destruction of evidence.[82] In this regard, the Court in *Carpenter* noted that lower courts have approved warrantless searches related to bomb threats, active shootings, and child abductions.[83]

While the lower court fixated on the seven-day timeframe, the Supreme Court's reasoning in *Carpenter* certainly applies to shorter timeframes. When using CSLI during any length of time, law enforcement is still able to access information that would otherwise be unknowable, by using technology to travel back in time and trace a person's movements. Unlike GPS monitoring, law enforcement does not need to know in advance whether they need to follow a person. Once a person is deemed a suspect, law enforcement can access information showing that person's location every day for five years. It does not matter whether this timeframe is seven days, six days, five days, four days, or, in this case, three days. Furthermore, CSLI is not imprecise. In FBI Special Agent Catherine Hale's affidavit for a court order to search under the SCA, she noted that, because of the density of the towers in Sweetwater, CSLI is often more accurate than GPS location.[84]

---

[80] *Id.* at 2212 (quoting 18 U. S. C. §2703(d)).
[81] *Id.* at 2221.
[82] *Id.* at 2223.
[83] *Id.*
[84] (Hale Aff. ¶ 11).

Tracing one's whereabouts for three days has the possibility of revealing just as much information as tracing one's whereabouts for seven days. For example, if a person has the same routine every day, that routine will not change on day four, five, or six. The same privacy interests at stake in *Carpenter* are clearly still at stake in this case with this shorter timeframe.

The same reasoning applies to the 100 hours of tracking over the course of ten days. The lower court reasoned that privacy concerns are diminished when the tracking occurs during "working hours," but that reasoning simply does not hold weight. The lower court assumes that everyone works between the hours of 8 a.m. and 6 p.m. and would not be traveling to their homes, churches, or other revealing locations during the timeframe, when it is common knowledge that many people work outside of regular business hours or simply do not work at all. Their movements during this timeframe could reveal the type of sensitive information with which the Supreme Court has historically been concerned. The ten-day search request is also problematic because it exceeds *Carpenter's* seven-day limit. Allowing law enforcement to get creative with the ways it requests CSLI could result in the judiciary's approval of a warrantless request for one hour of CSLI a day for 100 days. This type of request is certainly not in the spirit of *Carpenter*.

The lower court was also erroneous when it suggested that law enforcement could have conducted a two-week stakeout to discover the same information as the CSLI. That is simply not true because the tampering was first discovered on October 13, 2018. CSLI allowed law enforcement to travel back in time and trace the petitioner's movements from October 1-12, 2018. A stakeout would not have accomplished the same.

The Supreme Court specifically excluded tower dumps from its holding in *Carpenter*, but with the Court's shift in thinking regarding the third-party doctrine when applied to CSLI, the time has come for this Court to require law enforcement to obtain a warrant based upon probable

cause for cell tower dumps. While tower dumps do not chronicle a single person's movements, law enforcement should still have to obtain a warrant before having access to such information. Tower dumps reveal the personal location of hundreds, sometimes thousands, of people at a certain date and time – many of them innocent people who law enforcement has no reason to intrude on their individual privacy. Moreover, these innocent people have no knowledge that law enforcement can tap into their phone's location at any time. Requiring a warrant and probable cause would have very little effect on law enforcement's ability to use the tower dumps to create a list of suspects, but it deserves a heightened standard because of the vast quantity of information law enforcement receives about innocent Americans.

The Court in *Carpenter* was very clear that the privacy interests associated with CSLI were so great that it was impermissible to accept anything but probable cause as the standard. In the present case, probable cause simply did not exist at the time of the search. Law enforcement officers were working off weak suspicions from the moment they started searching the petitioner's vehicle. They continued their fishing expedition for several hours without finding anything solid. Once they found malware that was "similar" but not the same as the kind used in the skimming incidents, several hours had passed and law enforcement should have applied for a warrant as there were no exigent circumstances to justify not doing so.

CONCLUSION

For the aforementioned reasons, the petitioner respectfully requests this Court REVERSE the judgment of the Fourteenth Circuit Court of Appeals.

Respectfully submitted,

Attorneys for
Petitioner