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 FROM THE UNITED STATES COURT OF APPEALS
FOR THE FOURTEENTH CIRCUIT

BRIEF FOR RESPONDENT

COUNSEL FOR RESPONDENT
FEBRUARY 10, 2023

TABLE OF CONTENTS

TABLE OF CONTENTS i

TABLE OF AUTHORITIES iii

QUESTIONS PRESENTED vi

OPINIONS BELOW vii

CONSTITUTIONAL PROVISIONS AND RULES vii

INTRODUCTION 1
Summary of the Argument 1
Standard of Review 3

STATEMENT OF THE CASE 4
Statement of Facts 4
Procedural History 6

ARGUMENT 7
I. THIS COURT SHOULD AFFIRM BECAUSE OFFICER STUBBS WAS NOT REQUIRED TO HAVE REASONABLE SUSPICION TO CONDUCT A FORENSIC SEARCH OF THE PETITIONER'S NUMEROUS ELECTRONIC DEVICES AT THE INTERNATIONAL BORDER. 8
A. Under the border search doctrine, the Government's forensic search of Petitioner's electronic devices did not require a warrant, probable cause, or reasonable suspicion because of the lonstanding right of the sovereign to protect itself by inspecting the persons and effects that enter the county. 8
B. Government agents do not need reasonable suspicion to conduct a search of electronic devices at the border unless the search is highly intrusive. 12
C. Reasonable suspicion is not required to conduct a forensic search of electronic devices at the border because the Court's decision in *Riley v. California* did not alter the settled border search doctrine. 19
II. THIS COURT SHOULD AFFIRM BECAUSE THE SCA REQUESTS FOR CSLI OF THREE DAYS AND ONE-HUNDRED HOURS, IN ADDITION TO THREE, ONE-HOUR TOWER DUMPS, DOES NOT REQUIRE PROBABLE CAUSE AND A SEARCH WARRANT. 22
A. Under *Carpenter*, the Government's acquisiton of Petitioner's CSLI did not violate the Fourth Amendment. 22
1. Under the extended border search exception, the Government's acquisition of CSLI pursuant to 18 U.S.C. § 2703(d) does not require a search warrant. 22
2. *Carpenter's* ceiling was not violated by either of the Government's two limited requests for Petitioner's CSLI. 24

B. *Carpenter* does not apply to CSLI data requests under 18 U.S.C. § 2703(d) made at international borders because of the diminished expectation of privacy. 26
C. *Carpenter* does not apply to a request for a one-hour tower dump under 18 U.S.C. § 2703(d), because the privacy concerns in *Carpenter* do not apply to the snapshot of information that a tower dump provides..... 27

CONCLUSION..... 29

CERTIFICATE OF SERVICE 30

TABLE OF AUTHORITIES

Cases

Almeida-Sanchez v. United States,
413 U.S. 266 (1973) 8

Carpenter v. United States,
585 U.S. ___ (2018) 2, 3, 24, 25, 26, 27, 28, 29

Immigration & Naturalization Serv. v. Delgado,
466 U.S. 210 (1984) 12

Katz v. United States,
389 U.S. 347 (1967) 7

New Jersey v. T.L.O.,
469 U.S. 325 (1985) 13

Ornelas v. United States,
517 U.S. 690 (1996) 3

Riley v. California,
134 S. Ct. 2473 (2014) 19, 20, 21

Skinner v. Ry. Labor Executives' Ass'n,
489 U.S. 602 (1989) 7

Terry v. Ohio,
392 U.S. 1 (1968) 13

United States v. Alfaro-Moncada,
607 F.3d 720 (11th Cir. 2010) 10, 12, 13, 15, 26

United States v. Arnold,
533 F.3d 1003 (9th Cir. 2008) 13

United States v. Cardenas,
9 F.3d 1139 (5th Cir. 1993) 22, 23

United States v. Cotterman,
709 F.3d 952 (9th Cir. 2013) 17

United States v. Flores-Montano,
541 U.S. 149 (2004) 1, 9, 13, 16, 18, 20, 26

United States v. Graham,
824 F.3d 421 (4th Cir. 2016) 15

United States v. Ickes,
393 F.3d 501 (4th Cir. 2005) 15

United States v. Jacobsen,
466 U.S. 109 (1984)..... 7

United States v. Jones,
565 U.S. 400 (2012)..... 7

United States v. Kay,
17-CR-16, 2018 U.S. Dist. LEXIS 141615 (E.D. Wisc. August 21, 2018) 28

United States v. Kolsuz,
890 F.3d 133 (4th Cir. 2018) 16, 17, 19

United States v. Kubasiak,
18-CR-120-PP, 2018 U.S. Dist. LEXIS 172514 (E.D. Wisc. October 5, 2018)..... 28

United States v. Mendenhall,
446 U.S. 544 (1980)..... 12

United States v. Montoya De Hernandez,
473 U.S. 531 (1985)..... 7, 13, 14, 15, 16

United States v. Ramsey,
431 U.S. 606 (1977)..... 7, 8, 9, 10, 12, 25, 26

United States v. Sokolow,
490 U.S. 1 (1989)..... 13

United States v. Thirty-Seven (37) Photographs,
402 U.S. 363 (1971)..... 10

United States v. Tirado,
16-CR-168, 2018 U.S. Dist. LEXIS 141605 (E.D. Wisc. August 21, 2018)..... 28

United States v. Touset,
890 F.3d 1227 (11th Cir. 2018) 9, 10, 11, 12, 13, 16, 18, 26

United States v. Tuggle,
No. 16-CR-20070-JES-JEH, 2018 U.S. Dist. LEXIS 127333 (C.D. Ill. July 31, 2018) 28, 29

United States v. 12 200-Ft. Reels of Super 8mm Film,
413 U.S. 123 (1973) 9

Statutes

18 U.S.C. § 1028A 6

18 U.S.C. § 1344 6

18 U.S.C. § 1349 6

18 U.S.C. §§ 2701–2711 ..... 22, 24, 26, 27, 28, 29

Act of July 31, 1789 9

U.S. Const. amend. IV 7

Secondary Sources

11 A.L.R. Fed. 3d Art. 1 (Originally published in 2016) 28

§ 4.8(a) Overview of the Stored Communications Act, 2 Crim. Pro. § 4.8(a) (4th ed.) 22

U.S. Customs and Border Protection, *U.S. Border Patrol Fiscal Year 2017 Sector Profile* (Dec. 12, 2017) 11

U.S. Customs and Border Protection, CBP Directive No. 3340-049A (Jan. 4, 2018) 8

U.S. Customs and Border Protection, *U.S. Customs and Border Protection Snapshot - December 2018*, (Dec. 2018) 11

QUESTIONS PRESENTED

I. Under the Fourth Amendment, was the forensic search of electronic devices at an international border checkpoint constitutional when the Government conducted the search without reasonable suspicion?

II. Under 18 U.S.C. § 2703(d), does the Government need a warrant during a border search to obtain cell-site location information and tower dump data when the data requested is within *Carpenter's* privacy threshold?

OPINION BELOW

The opinion and order of the Fourteenth Circuit are recorded at *Escaton v. United States*, 1001 F.3d 1341 (14th Cir. 2021).

CONSTITUTIONAL PROVISIONS AND RULES

The Fourth Amendment to the United States Constitution provides:

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

U.S. Const. amend. IV.

Congressional Statute 18 U.S.C. § 2703(d) provides:

> 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.

18 U.S.C. § 2703 (West).

INTRODUCTION

Respondent, the United States of America, Appellee in *Escaton v. United States*, 1001 F.3d 1341 (14th Cir. 2021), before the United States Court of Appeals, Fourteenth Circuit, respectfully submit this brief on the merits and ask the Court to affirm the Fourteenth Circuit's decision below.

Summary of the Argument

The case at bar presents two important issues regarding searches of emerging technology within the Fourth Amendment to the United States Constitution. This Court should affirm the Fourteenth Circuit Court of Appeal's decision because Petitioner, Hector Escaton, has failed to show a Fourth Amendment violation. Neither the forensic search of his electronic devices at an international border, nor the use of cell-site location information (CSLI) by federal agents, violated Escaton's rights under the Constitution.

First, the Fourteenth Circuit correctly concluded that government agents are not required to have reasonable suspicion when conducting forensic searches of electronics devices at an international border. The historical importance of the border search doctrine emphasizes the Government's weighty interest in protecting our national sovereignty and maintaining territorial integrity. When Escaton approached the international border to reenter into the United States, he subjected himself and the digital property in his vehicle to a search that was "reasonable simply by virtue of that fact that it occurred at the border." *United States v. Flores-Montano*, 541 U.S. 149, 152-53 (2004). The border search doctrine is an exception to the probable cause and warrant requirements for searches under the Fourth Amendment. Border searches grant the Government broad authority in the interest of national security, which outweighs individual privacy interests under this Court's Fourth Amendment balancing analysis. Given the Government's national

security interests, agents were fully justified in forensically searching the information on Escaton's laptop, external hard drives and USB devices, which included the incriminating evidence tying him to the Mariposa Bank ATM skimming scheme. Circuits have split interpretations on forensic searches. However, this court should not create complex balancing tests by differentiating between 'routine' and 'non-routine' searches, or 'manual' and 'forensic' methods.

Additionally, the use of CSLI and tower dumps by the federal agents' to prove Escaton's connection to the Mariposa Bank ATM skimming spree did not violate the Fourth Amendment for several reasons. First, the extended border doctrine is applied because Escaton entered into the United States through the West Texas border checkpoint. Under the extended border exception, there is no requirement of a warrant supported by probable cause to search. Next, in light of *Carpenter v. United States*, the threshold requirement for requesting warrantless CSLI data is met. *Carpenter v. United States*, 585 U.S. __ (2018). The FBI made two requests for CSLI data. The first was from October 11-13, 2018 to determine if Escaton was in the area of the Boswell Street branch of Mariposa Bank during the tampering window. The second request was for weekday CSLI data from October 1-12, 2018 between 8 A.M. and 6 P.M., to determine if Escaton and his accomplice were at the same place during that time period. These data requests were within the threshold set forth by *Carpenter*, which limited warrantless requests for CSLI data to less than six days, or 167 hours. *Id.*

Even assuming that the CSLI data requests would normally require a warrant post-*Carpenter*, this Court has repeatedly held that there is a diminished expectations of privacy at the U.S. border. This Court in *Carpenter* cited that people have a reasonable expectation of privacy in their CSLI data. However, Fourth Amendment jurisprudence has always given way to

protecting its national borders. Here, Escaton's two CSLI data requests were made during a border search while coming back to the U.S. from Mexico. Escaton has a lower expectation of privacy when entering the U.S., and a warrantless request of CSLI data is not an unreasonable search. Therefore, the use of this information does not violate the Fourth Amendment.

Finally, tower dumps do not implicate the same privacy concerns as cited in *Carpenter*, and are thus not subject to its scrutiny. A tower dump is a list of phone numbers that used a particular cell tower for any purpose during a short period of time. The limited nature of a tower dump does not track a person's movements, and is not for long durations. Here, the FBI acquired three one-hour tower dump near ATMs that had been attacked by malware and skimmers. These tower dumps are more similar to pole cameras which courts have held do not require a warrant, even in the post-*Carpenter* world. Since the tower dumps are a snap shot in time, in a very defined area, this Court should apply the same standard as pole cameras. Therefore, the acquisition of three one-hour tower dumps, without a warrant, is not a search under the Fourth Amendment.

For these reasons explained in detail below, the United States of America asks this Court to affirm the Fourteenth Circuit's decision.

Standard of Review

This Court deems questions of law reviewable under a *de novo* standard. *Ornelas v. United States*, 517 U.S. 690, 691 (1996). The two issues on appeal turn on questions of law. Therefore, this Court should review the issues *de novo*.

STATEMENT OF THE CASE

Statement of Facts

On September 25, 2019, Hector Escaton, came into the United States from Mexico through the West Texas border checkpoint. (R. at 2). Mr. Escaton, a citizen of West Texas, voluntarily brought his iPhone (cell phone), a laptop, three external hard drives, and four USB devices through the international border checkpoint. (R. at 2). At that checkpoint, Customs and Border Protection (CBP) Officer Ashley Stubbs conducted a routine inspection of Mr. Escaton's vehicle and found three large suitcases in the back of the car. (R. at 2). Officer Stubbs then conducted a search and located the nine devices Mr. Escaton was trying to bring into the United States. (R. at 2). Unsure of whether these devices were connected to criminal activity, Officer Stubbs seized the devices for further investigation. (R. at 2). Officer Stubbs then placed the iPhone on airplane mode, ensured the laptop was disconnected to wireless service, and proceeded to search both devices without the use of assistive technology. (R. at 2). After opening the laptop Officer Stubbs found a hand-written paper note just below the keyboard with the message "Call Delores (201) 181-0981 $$$." (R. at 2). He then recorded the message, and the iPhone's number and returned the phone to Mr. Escaton. (R. at 2–3). Officer Stubbs did however, detain the other electronic devices for further investigation, since no password was needed to open them. (R. at 3). After discovering that some of the folders on the laptop were password protected and the USB devices were encrypted, Officer Stubbs delivered the electronics to Immigration and Customs Enforcement (ICE). (R. at 3). Special Agent & Computer Forensic Examiner Theresa Cullen, who was stationed at the border checkpoint, used forensic software to copy and scan the devices. (R. at 3). These scans resulted in the discovery of individuals' bank account numbers, PIN numbers, and traces of malware. (R. at 3). The copied

data that did not contain incriminating information was destroyed. (R. at 3). Officer Stubbs was then informed of Special Agent Cullen's results and immediately notified the Federal Bureau of Investigations (FBI), who turned over the information to Special Agent Catherine Hale. (R. at 3).

Special Agent Catherine Hale had been investigating a string of criminal activity associated with Mariposa Bank ATMs during October of 2018. (R. at 3). On October 13, 2018 the Boswell Street branch of Mariposa Bank in Sweetwater, West Texas discovered their ATM had been infected with malware. (R. at 3). The branch manager then alerted the other local branches, and through an internal investigation, found many other local ATMs had been infected with malware and skimming technology. (R. at 3-4). In all, eight ATMs were tampered with, costing roughly $50,000 of losses to the Bank, and hundreds of identities of Mariposa Bank customers to be stolen. (R. at 3-4).

Upon receipt of the information from Mariposa Bank's internal investigation, Special Agent Hale and U.S. Attorney Elsie Hughes requested tower dumps from the cell sites near three Sweetwater ATMs pursuant to 18 U.S.C. § 2703(d) of the Stored Communications Act (SCA). (R. at 4). The request was limited to 30 minutes before and after the identified suspect appeared on the ATM's timestamped video camera. (R. at 4). When Officer Stubbs gave Agent Hale details with regards to the search of Mr. Escaton's vehicle at the West Texas-Mexico border, Agent Hale discovered a phone number match to the tower dump request. (R. at 5). After discovering the match, U.S. Attorney Hughes and Agent Hale applied for, and received, cell site records for Mr. Escaton's phone number from October 11-13 of 2018 under the SCA. (R. at 5). These three-day records placed Mr. Escaton's phone in the area of the Boswell branch on October 12, the day before the ATM's malware was detected. (R. at 5). A second SCA request was for weekday records between October 1 and 12, limited to normal business hours from 8

A.M. to 9 P.M., which placed Mr. Escaton with Delores Abernathy during this time period. (R. at 5). With all this information, and corroborating evidence from Delores' phone records, law enforcement executed a search warrant and subsequently arrested and convicted Mr. Escaton and Delores Abernathy. (R. at 5).

Procedural History

The Government charged Escaton with 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). (R. at 2). Escaton filed a motion to suppress the evidence from both the forensic border search and the CSLI requests, seeking to exclude the financial information that implicated Escaton in the ATM skimming scheme. (R. at 2). Both parties stipulated that no reasonable suspicion existed at the time of the border search. The District Court denied the motion, and Escaton appealed. A unanimous panel of the Fourteenth Circuit Court of Appeals affirmed, holding that law enforcement acted properly and within the bounds of Fourth Amendment protections. This appeal followed.

ARGUMENT

The Fourth Amendment guarantees "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 (emphasis added). For much of our history, Fourth Amendment searches were "tied to common law trespass" and focused on whether the Government obtained information by "physically intruding on a constitutionally protected area." *United States v. Jones*, 565 U.S. 400, 405, 407 (2012). Consistent with the interpretation that "the Fourth Amendment protects people, not places," this Court expanded the property-based approach. *Katz v. United States*, 389 U.S. 347, 351 (1967). In the absence of trespass, this Court uses the *Katz* two-prong test to determine the reasonableness of a search, looking at whether a person has "an actual (subjective) expectation of privacy," and whether that expectation is "one that society is prepared to recognize as 'reasonable.'" *Id.* at 361 (Harlan, J., concurring).

Generally, the Fourth Amendment requires a search to be executed under a judicial warrant based on probable cause. *Id.* at 357. This protection only proscribes governmental action. It is "wholly inapplicable 'to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government.'" *United States v. Jacobsen*, 466 U.S. 109, 113–14 (1984). However, there are exceptions to the warrant requirement in "special needs" situations that endow government officials with greater flexibility, one being the border search doctrine. *Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602, 619 (1989).

Border searches "are reasonable simply by virtue of the fact that they occur at the border." *United States v. Ramsey*, 431 U.S. 606, 616 (1972). Routine searches at international borders "are not subject to any requirement of reasonable suspicion, probable cause, or warrant." *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985). This Court has held, "without

doubt," that the Government's "power can be effectuated by routine inspections and searches of individuals or conveyances seeking to cross our borders." *Almeida-Sanchez v. United States*, 413 U.S. 266, 272 (1973). The searches are reasonable by the "single fact that the person or item in question had entered into our country from outside," a longstanding recognition that "has a history as old as the Fourth Amendment itself." *Ramsey*, 431 U.S. at 619.

I. THIS COURT SHOULD AFFIRM BECAUSE OFFICER STUBBS WAS NOT REQUIRED TO HAVE REASONABLE SUSPICION TO CONDUCT A FORENSIC SEARCH OF THE PETITIONER'S NUMEROUS ELECTRONIC DEVICES AT THE INTERNATIONAL BORDER.

The case at bar raises Fourth Amendment scrutiny of the interaction between forensic searches of electronic devices and individual privacy rights within the border search context. A forensic search, also known as an advanced search by CBP, "connects external equipment" to an electronic device that can "review, copy, and/or analyze its contents." U.S. Customs and Border Protection, CBP Directive No. 3340-049A (Jan. 4, 2018), https://www.cbp.gov/document/directives/cbp-directive-no-3340-049a-border-search-electronic-devices. Therefore, in determining the level of suspicion required, this Court must look to the historical importance and the distinct context of the border search doctrine, rather than the mere privacy interests within electronic devices.

A. Under the border search doctrine, the Government's forensic search of Petitioner's electronic devices did not require a warrant, probable cause, or reasonable suspicion because of the longstanding right of the sovereign to protect itself by inspecting the persons and effects that enter the country.

This Court should maintain its reluctance to narrow the scope of the border search exception because of the Government's longstanding plenary authority to conduct suspicionless border searches. In affirming the Fourteenth Circuit's decision, this Court will recognize the

historical importance and broad scope of the border exception, thereby properly exercising judicial restraint in interpreting constitutional privacy rights. The Government's interest in protecting the borders from the illegal movement of contraband, weapons, and unwanted persons "is at its zenith at the international border." *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004). "It is axiomatic that the United States, as sovereign, has the inherent authority to protect, and a paramount interest in protecting, its territorial integrity." *Id.* at 153.

The longstanding right of the sovereign to protect itself dates back to the founding of our Republic. Customs officials were granted plenary authority in statutes enacted by the First Congress, the same Congress who proposed the Fourth Amendment. *Ramsey*, 431 U.S. at 616. The first customs statute, Act of July 31, 1789, endowed customs officials "full power and authority" to enter and search "any ship or vessel" where they had "reason to suspect any goods, wares or merchandise subject to duty" were concealed. *Id.* (*See* Act of July 31, 1789, ch. 5, § 24, 1 Stat. 29, 43 (1789); *Ramsey*, 431 U.S. at 616–17 ("The historical importance of the enactment of this customs statute by the same Congress which proposed the Fourth Amendment is, we think, manifest."). Congress then expanded that power a year later "by permitting customs officials to board vessels even before they reached the United States." *United States v. Touset*, 890 F.3d 1227, 1232 (11th Cir. 2018). These broad powers have been necessary to prevent the smuggling of contraband into this country. *United States v. 12 200-Ft. Reels of Super 8mm Film*, 413 U.S. 123, 125 (1973). The historical importance of these broad powers emphasizes the Founders' intent behind Fourth Amendment protections, which purposely permits governmental discretion to protect international borders. The Framers of the Constitution did not fight a war to guarantee a nation with sovereign certainty to merely be undermined by the Fourth Amendment as a result of emerging technology crossing the borders.

Thus far, this Court has adhered to the Founders' intent for protecting the nation's borders. This Court should maintain the scope of the border search doctrine and continue to properly emphasize the distinctiveness of the border search context in regards to forensic searches of electronic devices. While Supreme Court precedent affords more Fourth Amendment protection to digital information in comparison to other kinds of property, searches that occur at the border are subject to fewer constraints, "simply by virtue of the fact that they occur at the border." *Ramsey*, 431 U.S. at 616.

Under the border search doctrine, the scope of a routine search includes a pat-down search, frisk, luggage inspection, examination of incoming international mail, vehicle search, and more, "all without any level of suspicion." *United States v. Alfaro-Moncada*, 607 F.3d 720, 728 (11th Cir. 2010) (collecting cases). A traveler's privacy rights "neither prevents the search of his luggage nor the seizure of unprotected, but illegal, materials" when government officials discover the items during a border search. *Touset*, 890 F.3d at 1233 (*citing United States v. Thirty-Seven (37) Photographs*, 402 U.S. 363, 376 (1971) (plurality opinion)). "Customs officers characteristically inspect luggage," and their power to do so is a historic practice that "is intimately associated with excluding illegal articles from the country." *Thirty-Seven (37) Photographs*, 402 U.S. at 376. Therefore, reasonable suspicion should never be required to search property at the border, regardless of how arbitrary or intrusive, because of the compelling government interests in national security that considerably outweigh individual interests.

In the case at bar, there were two contemporaneous searches of Escaton's electronic devices derived from Officer Stubbs' routine border stop. (R. at 2–3). Officer Stubbs initially conducted a manual search of Escaton's cell phone and laptop, followed by Theresa Cullen's subsequent search of the laptop, three external hard drives, and four USB devices using

technologically advanced law enforcement tools. (R. at 2–3). Cullen used forensic software to bypass the password protected barriers that prevented Officer Stubbs from viewing the documents on the laptop and the inaccessible information on the USB devices. (R. at 3). Both government agents conducted the searches at the border checkpoint, which only required detaining the devices for a few hours. (R. at 3). Escaton was not under arrest at this point, but he did not voluntarily offer to show Officer Stubbs the content of his digital property to avoid the detainment of the items for forensic examination. In 2017, suspicions of criminal activity resulted in more than 875,000 pounds of drugs seized in the Southwestern border of the United States alone. U.S. Customs and Border Protection, *U.S. Border Patrol Fiscal Year 2017 Sector Profile* (Dec. 12, 2017), https://www.cbp.gov/document/stats/us-border-patrol-fiscal-year-2017-sector-profile. In December of 2018, 1,600 individuals were suspected of national security concerns at United States border checkpoints. U.S. Customs and Border Protection, *U.S. Customs and Border Protection Snapshot - December 2018* (Dec. 2018), https://www.cbp.gov/newsroom/stats. These statistics are just a snapshot of why the Government has a paramount interest in protecting the nation and preserving territorial integrity. Therefore, in light of the historical interpretation and longstanding broad scope of the border context, this Court should affirm.

Proponents of narrowing the border exception argue that individual privacy interests outweigh the government's interest with regards to digital devices because of the possibility that a device has intimate information stored within it. This argument fails because border agents bear the same responsibility of preventing contraband from entering the country, regardless of advances in technology. *Touset*, 890 F.3d at 1233. Therefore, the argument lacks rationality when distinguishing electronic devices from other personal effects in a vehicle, such as boxes

loaded with personal medical records or other sensitive documents. *Id.* More importantly, there is great potential harm if the border exception is narrowed to require reasonable suspicion to conduct forensic searches because this Court would essentially be granting special treatment to a specific form of property. The resulting ramifications of this special treatment create a loophole for smugglers to introduce damaging contraband into the country via electronic devices, such as child pornography, malware, terrorist weapon detonators, and other forms of cyberespionage. Because of the potential harm, this Court should recognize the weightier governmental interest within the border context.

To conclude, the historical precedent of this Court has repeatedly held that it is reasonable for government officials to exercise plenary authority to conduct suspicionless searches at the border. *Ramsey*, 431 U.S. at 622. The border search doctrine serves not only the purpose of national security, but also the prevention of crimes involving drugs, human trafficking, identity theft, and child pornography. The historical importance of the Government's broad power, combined with the scope and purpose established by the Founding Fathers of the Constitution, serve as sufficient weight to override individual privacy concerns.

B. Government agents do not need reasonable suspicion to conduct a search of electronic devices at the border unless the search is highly intrusive.

Within the border search context, this Court has not decided whether a forensic search of an electronic device requires a more particularized level of suspicion. However, it has established precedent that reasonable suspicion is only required when a government agent conducts a non-routine, "highly intrusive" search. *United States v. Alfaro-Moncada*, 607 F.3d 720, 729 (11th Cir. 2010). Reasonable suspicion requires a "minimal level of objective justification." *Immigration & Naturalization Serv. v. Delgado,* 466 U.S. 210, 217 (1984) (*citing United States v. Mendenhall*, 446 U.S. 544, 554 (1980)). It is "considerably less than proof of

wrongdoing by a preponderance of the evidence," and "obviously less demanding than that for probable cause." *United States v. Sokolow*, 490 U.S. 1, 7 (1989). However, the government agent must be able to articulate something more than a mere hunch. *Id.* (*citing Terry v. Ohio*, 392 U.S. 1, 27 (1968)). Reasonableness "depends upon all of the circumstances surrounding the search or seizure and the nature of the search or seizure itself." *United States v. Montoya De Hernandez*, 473 U.S. 531, 537 (1985) (*citing New Jersey* v. *T.L.O.*, 469 U.S. 325, 337 (1985)).

This Court has already held that it is reasonable to conduct routine searches of people and their belongings at international borders. *Touset*, 890 F.3d at 1232–33. Reasonable suspicion is only required in the border context for "highly intrusive" searches, such as strip searches, body-cavity searches, and x-ray examinations. *Alfaro-Moncada*, 607 F.3d at 729. A search is "highly intrusive" if it is "so destructive," or is conducted in a "particularly offensive manner." *Flores-Montano*, 541 U.S. at 155–56; *United States v. Arnold*, 533 F.3d 1003, 1009, n.2 (9th Cir. 2008). Courts look to "dignity and privacy interests" of the person being searched to determine whether individualized suspicion is required when conducting a highly intrusive search. *Flores-Montano*, 541 U.S. at 152. However, a forensic search of an electronic device is not an invasive search. Individuals do not have a heightened privacy interest in digital devices because of their capability to store large quantities of data. This Court has held that it will not distinguish between different kinds of property to determine what constitutes a "routine" search because it would lead to complex balancing tests that have no place in the context of border searches. *Flores-Montano*, 541 U.S. at 152. Therefore, this Court should find that borders searches are routine and permissible without any particularized suspicion because forensic searches are reasonable, regardless of the technologically advanced tools that the government uses to conduct the search.

A rare example of when this Court held a border search as highly intrusive occurred when the search went "beyond the scope of a routine customs search and inspection" because it involved a cavity search. *Montoya De Hernandez*, 473 U.S. at 541. In *Montoya De Hernandez*, a woman was detained by customs officials upon reentering the country from an international flight because they suspected her of smuggling narcotics in her alimentary canal. *Id.* at 532–533. The customs officials found her "smuggling 88 cocaine-filled balloons in her alimentary canal." *Id.* The Court held that her detention violated the Fourth Amendment because the customs inspectors did not have a "clear indication" of alimentary canal smuggling at the time she was detained. *Id.* Yet, the invasive nature of a cavity search distinguishes this search from a routine border search.

However, the case at bar is also analogous to *Montoya* because an individual is put on notice and assumes the risk to have their vehicle and belongings searched when crossing the border. The defendant in *Montoya* assumed the risk of a border search when she "presented herself at the border for admission" to the country and "subjected herself to the criminal enforcement powers of the Federal Government." *Id.* at 539. Likewise, a traveler determines the time and place of the search by his own actions, and thus has ample opportunity to limit the nature and extent of the effects that he brings with him. The individual's privacy is less invaded by border searches because of this assumption of the risk. For instance, people choose to bring their suitcase to the airport knowing that it will be subject to examination and run through an x-ray machine. This same concept of assuming the risk applies to bringing electronic devices across the border. The only difference is that the risks are heightened when entering or exiting the country, in comparison to domestic travel, thereby further buttressing the endowment of the Government's broad authority within the border search context. Advances in technology should

not provide individuals with a Fourth Amendment protection to "conceal information that otherwise would not have been private." *United States v. Graham*, 824 F.3d 421, 436 (4th Cir. 2016). Therefore, this Court should refuse to create "a sanctuary at the border" that would undermine the Government's compelling interest in the border search doctrine. *United States v. Ickes*, 393 F.3d 501, 506 (4th Cir. 2005). The balance of interests is both "qualitatively different" at international borders and "struck much more favorably" to the government than in the interior of the country. *Montoya De Hernandez*, 473 U.S. at 538, 540. Despite the standards that other circuits have applied to forensic searches of electronics at the border, "our law is clear that searches at the border are a different matter altogether." *Ickes*, 393 F.3d at 503.

Similarly, this Court held that no reasonable suspicion was required to search a crew member's cabin at the border. *Alfaro-Moncada*, 607 F.3d at 732. In *Alfaro-Moncada*, the governmental interests in national security outweighed an individual's privacy interests in their dwelling. The Court upheld a search conducted without reasonable suspicion of a crew member's living quarters on a foreign cargo vessel that was entering through the United States border. *Id.* The Customs agents found child pornography when performing a routine inspection of the vessel. *Id.* at 725. The Eleventh Circuit held that reasonable suspicion was not required to search crew members' cabins because the vessel was docked at a port of entry into the country, thereby invoking the border search exception of the Fourth Amendment. *Id.* at 732. Individual's homes are generally afforded the greatest Fourth Amendment protection, and homes contain just as much intimate detail about a person as a cell phone, laptop, or tablet. The holding in *Alfaro-Moncada* exemplifies that the Government's interests triumph against even weighty privacy concerns when the border search exception applies. Therefore, the Court should apply the Eleventh Circuit's reasoning when evaluating forensic searches of electronic devices because the

privacy interests of the individual are the same, if not less, than the interests of an individual in their home.

The Eleventh Circuit reached a similar conclusion in *Touset*, where the petitioner argued his Fourth Amendment rights were violated when CBP agents searched his luggage when he returned to the United States from an international flight. *Touset*, 890 F.3d at 1230. The agents found "two iPhones, a camera, two laptops, two external hard drives, and two tablets," in Touset's luggage. *Id.* The initial manual search of the iPhones and camera did not reveal any incriminating information, but a subsequent forensic search revealed child pornography on the laptops and external hard drives. *Id.* The Court held that reasonable suspicion was not required to conduct the forensic search of Touset's devices because the Fourth Amendment does not require that same standard for a search of other forms of personal property at the border. *Id.* at 1233.

To further illustrate, the decision in *Montoya De Hernandez* required "reasonable suspicion for the prolonged detention of a *person* until she excreted the contraband" that she was smuggling in her alimentary canal, but it has never extended this requirement to *property*. *Id.* Similarly, the Court held in *Flores-Montano* that the search of a vehicle's gas tank did not require reasonable suspicion because the government has "authority to remove, disassemble, and reassemble a vehicle's fuel tank" at the border. *Flores-Montano*, 541 U.S. at 155. It argued that "the reasons that might support a requirement of some level of suspicion in the case of highly intrusive searches of the person—dignity and privacy interests of the person being searched—simply do not carry over to vehicles." *Id.* at 152.

Alternatively, the Fourth Circuit and the Ninth Circuit have failed to recognize the border context distinction in their holdings, which require reasonable suspicion to conduct a forensic search of digital devices at the border. In *United States v. Kolsuz*, the defendant was detained at a

United States airport before departing on an international flight because federal customs agents found firearms parts in his luggage. *United States v. Kolsuz*, 890 F.3d 133, 136 (4th Cir. 2018). The agents detained his cell phone for an off-site forensic analysis, where they found incriminating digital information. *Id.* The Court held that the forensic search of the cell phone was a "nonroutine" border search that is unconstitutional without "a showing of individualized suspicion" because of the scale of intimate nature of cell phone devices. *Id.* at 144–145.

In like manner, the Ninth Circuit held reasonable suspicion is required to conduct a forensic examination of a laptop at the border. In *United States v. Cotterman*, federal agents seized two laptops and three digital cameras from the defendant when he was crossing the international border. *United States v. Cotterman,* 709 F.3d 952, 957 (9th Cir. 2013). The Government agents sent the computers to a federal lab where forensic software was used to examine password-protected files that contained child pornography. *Id.* at 958. However, the Court reasoned that reasonable suspicion is required because "such a thorough and detailed search of the most intimate details of one's life is a substantial intrusion upon personal privacy and dignity." *Id.* at 968. The Ninth Circuit misinterpreted intrusiveness because the fact that electronic devices store more private information than their non-electronic counterparts does not justify creating a bright line rule requiring reasonable suspicion. *Id.* at 977–78; ("This rule flouts more than a century of Supreme Court precedent, is unworkable and unnecessary, and will severely hamstring the government's ability to protect our borders." *Id.* at 971 (Callahan, J., dissenting)).

The Eleventh Circuit rejected these decisions by its sister circuits. A forensic search of electronic devices at the border is constitutional in the absence individualized suspicion, as illustrated when courts emphasize the distinctiveness of the border search context in conducting

its balancing analysis. Electronics are no different than other forms of personal property. Therefore, following the Fourth and Ninth Circuits judicial attempts to distinguish between "routine" and "nonroutine" searches, or "manual" and "forensic" searches, will result in complex balancing tests for determining the level of intrusiveness. *Flores-Montano*, 541 U.S. at 152. Instead, the Court should maintain the highly intrusive factors already established, which does not apply to electronic devices. *Touset*, 890 F.3d at 1233. The Government has an immense interest in screening for illegal contraband and protecting our sovereign nation. The increase in emerging technology "only heightens the need of the government to search property at the border unencumbered by judicial second-guessing." *Id.* at 1235. The ramifications of holding otherwise would allow digital contraband to bypass border security safeguards, thereby limiting the scope of national protection and creating an uneven standard for different forms of property.

Like the respondent in *Touset*, Escaton did not have a heightened privacy interest in his electronic devices when crossing the border. The Fourteenth Circuit correctly applied the Eleventh Circuit's standard of no requirement of reasonable suspicion for border searches. The Government urges this Court to affirm the denial of the Petitioner's suppression motion on the basis that a border search of his digital devices does not require any particularized showing of suspicion. When the Petitioner arrived at the international border checkpoint and presented himself to CBP for inspection and entry into the United States, Officer Stubbs was legally authorized to detain Escaton's laptop, external hard drives, and USB devices for further inspection. Escaton subjected himself and his property, including his digital property, to the border authority. The search was reasonable, and the resulting evidence of financial fraud renders the Government's interest even weightier.

Consequently, the Fourth Amendment does not require reasonable suspicion for a forensic search of non-digital forms of personal property, and therefore, it should not be required for digital devices. Adhering to the rationale of sister circuits, this Court should adopt the Eleventh Circuit's holding that no suspicion is necessary to conduct forensic searches of electronic devices at the border and affirm the Fourteenth Circuit's decision.

C. Reasonable suspicion is not required to conduct a forensic search of electronic devices at the border because the Court's decision in *Riley v. California* did not alter the settled border search doctrine.

After this Court's decision in *Riley v. California*, the Fourth Circuit improperly applied *Riley's* reasoning to the border search doctrine. (*see United States v. Kolsuz*, 890 F.3d 133, 145 (4th Cir. 2018)). Citing *Riley's* privacy concerns, that Court restricted the border search doctrine to its narrowest interpretation, holding that the Government search improperly exceeds the scope of a border search if the Government uses forensic tools to search an electronic device beyond its physical attributes. *Id.*

In *Riley*, the Court determined that the police may not search digital information on a cell phone seized from an individual incident to an arrest, without a warrant. *Riley v. California*, 134 S. Ct. 2473, 2493 (2014). In two consolidated cases, police searched defendants' cellular devices during lawful arrests, which led to obtaining further incriminating evidence. In the first case, defendant Riley was stopped for driving with expired registration tags. *Id.* at 2480. The arresting officer obtained information through a search of his smartphone that incriminated Riley on weapons charges. *Id.* In the second case, an officer conducting routine surveillance of an apparent drug sale, searched defendant Wurie's cell phone, in which the contents of the device provided the location of the residence where he was distributing illegal drugs. *Id.* at 2481. After being convicted, the defendant's moved to suppress evidence obtained from accessing their cell

phones without a search warrant. *Id.* at 2481–82. The Court held both searches unreasonable and set forth the precedent that a warrant is required to search a cell phone incident to a lawful arrest because modern cell phones have the capability to store large amounts of private information. *Id.* at 2485.

Nevertheless, applying *Riley's* privacy concerns in the context of a border search in this case poses two problems. First, this argument is inapplicable to the case at bar because it fails to address the different contexts in which both searches were conducted. *Riley* involved the search incident to arrest exception to the warrant requirement, which allows government agents to conduct warrantless searches under the rationale that the search is permissible as a protective measure for the safety of police and to prevent the escape of arrestees. *Id.* at 2483. In contrast, the border search exception to the warrant requirement allows government agents to conduct searches without individualized suspicion under the rationale that the Government's interest in territorial integrity and national security of the country outweigh individual's privacy interests, which are diminished at the border. *Flores-Montano*, 541 U.S. at 153. Therefore, the Fourth Circuit ignored the differing rationales behind each exception to the warrant requirement before balancing the Government and individual interests within the border context.

Second, the argument that a cell phone may contain an immense amount of private information, some of which may not be stored on the device itself, is inconsequential in this case because Officer Stubbs did not access, nor attempt to access this type of information. (R. at 3). Opponents argue that the Government's analogy of treating a cell phone like any other "container" in a vehicle, subject to suspicionless search in both the search incident to arrest and border search exceptions, does not account for a cell phone's cloud computing ability. *Riley*, 134 S. Ct. at 2491. "Cloud computing is the capacity of internet-connected devices to display data

stored on remote servers rather than on the device itself." *Id.* However, the Government acknowledges this issue by establishing protocol to ensure that officers disconnect a phone from the network before searching the device, just as Officer Stubbs did when he handled Escaton's cell phone. (R. at 2). Furthermore, this issue relates back to the notion that the legislature is better suited to draw lines for balancing competing law enforcement and privacy interests. *See Riley*, 134 S. Ct. at 2497 (Alito, J., concurring).

Here, Officer Stubbs discovered several electronic devices in suitcases when he conducted a lawful border search of Escaton's vehicle. (R. at 2). Officer Stubbs manually searched Escaton's cell phone without assistive technology, and then detained the remaining laptop, external hard drives, and USB devices for further forensic investigation by ICE examiner Theresa Cullen, who was stationed at the border checkpoint. (R. at 2–3). The forensic analysis revealed evidence of financial fraud on the laptop and malware on the USB devices, which aided the FBI in connecting Escaton to the "ATM skimming" scheme of Mariposa Bank in October of 2018. (R. at 3). Unlike in *Riley*, Escaton was not arrested at the border, but rather searched at a routine border checkpoint, where he was put on notice that his person, vehicle, and belongings are subject to suspicionless searches by government agents to prevent contraband from entering into the country. (R. at 2). Officer Stubbs could not access the information on the laptop and USB devices during his initial manual search because both were password protected. (R. at 3).

In sum, if the border search doctrine is construed to require reasonable suspicion to conduct forensic searches of devices at the border, then criminal activity will be allowed to bypass inspection, resulting in dangerous digital content making its way into our nation.

II. THIS COURT SHOULD AFFIRM BECAUSE THE SCA REQUESTS FOR CSLI OF THREE DAYS AND ONE-HUNDRED HOURS, IN ADDITION TO THREE, ONE-HOUR TOWER DUMPS, DOES NOT REQUIRE PROBABLE CAUSE AND A SEARCH WARRANT.

Individual's cell-site records can be obtained by law enforcement through a court order under the SCA. 18 U.S.C. §§ 2701-11. The Government's showing to obtain cell-site records are "specific and articulable facts showing that there are reasonable grounds to believe that … the records or other information sought are relevant and material to an ongoing criminal investigation." *Id*. at § 2703(d). The original intent of the SCA was to "enact statutory privacy protections regulating the relationship between government investigators and service providers in possession of users' private information." § 4.8(a) Overview of the Stored Communications Act, 2 Crim. Proc. § 4.8(a) (4th ed.). While "specific and articulable facts" is not defined in the statute, legislative history and case law suggest that the standard is "an intermediate standard," "higher than a subpoena, but not a probable cause warrant." H.R.Rep. No. 103-827, at 31–32 (1994), reprinted in 1994 U.S.C.A.A.N. 3489, 3511–12.

A. Under *Carpenter*, the Government's acquisition of Petitioner's CSLI did not violate the Fourth Amendment.

1. Under the extended border search exception, the Government's acquisition of CSLI pursuant to 18 U.S.C. § 2703(d) does not require a search warrant.

The border search doctrine allows for a routine search at the border, or its functional equivalent, without probable cause or a warrant. *United States v. Cardenas*, 9 F.3d 1139, 1148 (5th. Cir. 1993). An extended border search is also an exception to the probable cause and warrant requirement, which allows for a "warrantless search and seizure *beyond* the border." *Id*. There are three factors the Court must consider when determining if the extended border search is reasonable, and thus constitutional. *Id*. These are:

> (1) a showing of a 'reasonable certainty' or a 'high degree of probability' that a border crossing has occurred; (2) a showing of a 'reasonable certainty' that no change in the condition of the person or vehicle being inspected occurred from the time of the border crossing until the search and that the contraband found was present when the person or vehicle crossed the border; and (3) a showing of a "reasonable suspicion" that criminal activity was occurring.

Id. at 1148 (internal citations omitted).

The reasonable certainty standard requires "more than probable cause, but less than proof beyond a reasonable doubt." *Id*. Further, the standard for determining whether there was reasonable suspicion of criminal activity requires looking at the totality of the circumstances. *Id*.

In the present case, Petitioner crossed into the United States through the West Texas border checkpoint. (R. at 2). At the time of Petitioner's entrance into the U.S., his vehicle was searched by CBP Officer Stubbs. (R. at 2). During the search, CBP Officer Stubbs wrote down the phone number for the cell phone that Petitioner had in the vehicle, as well as had a forensic examination performed on the three hard drives and four USB devices. (R. at 2–3). The USB devices were found to contain traces of malware. (R. at 3). The results of the USB's malware and the cell phone number were provided to the FBI, which had been investigating ATM "skimming" in Sweetwater, West Texas. (R. at 3). The cell phone number gathered during the border search matched one of the phone numbers on the tower dump requested by the FBI, under the SCA. (R. at 5).

Based on these facts, the extended border doctrine factors are met, thus the CSLI data obtained by the Government did not require a warrant. Applying the factors, (1) the Petitioner came through the West Texas border crossing, (2) the contraband was the CSLI data which remained in the condition it was at the time of the border crossing, and (3) based on the totality of the circumstances, there was reasonable suspicion the Petitioner was involved in the ATM skimming ring.

2. *Carpenter's* ceiling was not violated by either of the Government's two limited requests for Petitioner's CSLI.

A search of CSLI data, pursuant to 18 U.S.C. § 2703(d), is presumed unreasonable where there is not a warrant, and the CSLI data is for more than six continuous days. *Carpenter*, 585 U.S. __ (slip op., at 15). In *Carpenter*, there were two CSLI data requests by the Government, the first for 152 days, and the second for seven days. The Court held that in the specific set of circumstances presented in the case, there was an unreasonable search. *Id.* at __ (slip op., at 18). The continuous CSLI data of seven days (168 hours), the Court reasoned, was so intrusive as to require a warrant because, "the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'" *Id.* at __ (slip op., at 12).

The Government's first request was for only three days of CSLI data, and thus falls short of the threshold requirement in *Carpenter*. (R. at 5). This request is distinguishable from *Carpenter* because the limited time frame of three days is a reasonable search. The concerns that the *Carpenter* Court had were based on an original construction of the Fourth Amendment. *See generally Carpenter*, 585 U.S. __ (slip op., at 4–18). These concerns, however, fall short in the present case because the limitation that *Carpenter* places on the Government's ability to obtain warrantless CSLI data. Additionally, Government's first request tied directly to the timeframe of when the branch's ATM was tampered with. (R. at 3). The limited scope of the search was as narrow and defined as the Government could reasonably have made it. Finally, the Court in *Carpenter* never invalidates the use of 18 U.S.C. § 2703(d) as a means of obtaining CSLI data in criminal investigations. *Carpenter* at __ (slip op., at 18). Therefore, in light of *Carpenter's* limitation, the Government's first request for three full days of CSLI data does not require probable cause and a warrant.

Next, the Government's second request for one hundred hours of CSLI data does not violate the threshold requirement of *Carpenter*. (R. at 5). Similarly, the second request is distinguishable from *Carpenter* because the limited scope of the request is a reasonable search. The one hundred-hour CSLI request does not meet the threshold cited in *Carpenter*, which found that 168 continuous hours of CSLI data was an unreasonable search without probable cause and a warrant. *Carpenter* at __ (slip op., at 17).

In the present case, the second request from the Government was for the specific two-week window during the ATM skimming spree. (R. at 3–4). Further, the second CSLI data request of one hundred weekday business hours is not directly addressed by the *Carpenter* Court. *See generally Carpenter* at __ (slip op., at 3). In *Carpenter*, the Court only reviewed CSLI data that was continuously requested over 152 days, and seven days, respectively. *Id.* The privacy concerns of continuous surveillance for these long periods of time outweighed the Government's interest in seeking warrantless data. *Id*. The Court in *Carpenter* focused on the duration and intrusiveness of the Government's continuous surveillance. *Id.* at __ (slip op., at 13). The intrusive nature of continuously tracking a person's movements at all hours of the day is substantially greater than when a person is at work in the public thoroughfare. Whereas here, the request was limited to normal business hours from 8 A.M. to 6 P.M., Monday through Friday, for the two weeks during ATM skimming scheme. (R. at 5).

As seen in *Ramsey*, where a search is authorized, and the search is reasonable, the search will be valid. *Ramsey*, 431 U.S. at 625. There the defendants were convicted of possession of narcotics using evidence obtained when a customs officer searched international mail that was intended for the defendants. *Id.* at 607-11. The Court held that because there was a statute which allowed for the search, and the search was reasonable, there was not a Fourth Amendment

violation. *Id.* at 625. With regards to CSLI data, *Carpenter* defined when a CSLI search is unreasonable, and 18 U.S.C. § 2703(d) gives authorization to request cell-site data. Based on the *Ramsey* test, since the Government's CSLI request is within the threshold of *Carpenter*, thus reasonable, and 18 U.S.C. § 2703(d) authorizes the search, there is not a Fourth Amendment violation.

Since the threshold limits placed by Carpenter have not been exceeded, both of the Government's requests for CSLI data are permissible without probable cause and a warrant.

Therefore, since the extended border search doctrine applies, and the Government's request was within *Carpenter's* threshold, this Court should affirm the use of Petitioner's CSLI data pursuant to 18 U.S.C. § 2703(d).

B. *Carpenter* does not apply to CSLI data requests under 18 U.S.C. § 2703(d) made at international borders because of the diminished expectation of privacy.

Border search jurisprudence demonstrates a diminished expectation of privacy due to the heightened government interest in protecting its international borders. *Flores-Montano*, 541 U.S. at 152–53. The Court has consistently held that the "Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border." *Id.* at 152. For the purposes of securing its borders, protecting the sovereignty of the nation, and protecting the people of the United States, "searches made at the border…are reasonable simply by virtue of the fact that they occur at the border." *Ramsey*, 431 U.S. at 616. Finally, in execution of these purposes, Congress "has granted the Executive plenary authority to conduct routine searches and seizures at the border, without probable cause or a warrant…." *Flores-Montano*, 541 U.S. at 153.

As discussed in Section I, forensic searches at the border have been authorized under these principles of protection and safety. *See Alfaro-Moncada*, 607 F.3d at 723; *Touset*, 890 F.3d at 1233. In the present case, the Petitioner came into the United States through the West Texas

border checkpoint. (R. at 2). While Petitioner asks the Court to apply the CSLI holding in *Carpenter* to the facts of this case, it simply cannot be done. The crux of *Carpenter's* argument is centered on a person's reasonable expectation of privacy. *See generally Carpenter*, 585 U.S. __ (slip op.). In *Carpenter*, the defendant was the leader in a string of robberies throughout Michigan and Ohio. *Id*. at __ (slip op., at 2–3). While it is clear from the record that the defendant drove between Ohio and Michigan, there is no factual basis, nor reasonable inference, that the defendant ever crossed out of, and back into, the United States border. *See generally Id*. In holding that obtaining seven days of CSLI data without a warrant is an unreasonable search, the Court stated that, "our decision today is a narrow one." *Id*. at __ (slip op., at 17). The narrow nature of *Carpenter's* holding is to be viewed based on the facts that this Court had in front of it, and was not intended to stretch beyond the bounds of those same facts in other cases. In the case at bar, the distinguishing fact that the Petitioner drove into Mexico, and then came back into the United States, goes beyond the scope of *Carpenter's* decision. (R. at 2). Thus, the Petitioner's CSLI data collected by the FBI pursuant to 18 U.S.C. § 2703(d) is not subject to *Carpenter's* scrutiny due to the search occurring at the border checkpoint.

Since *Carpenter* is held on privacy grounds, the application of the border search doctrine through the use of 18 U.S.C. § 2703(d) to obtain CSLI data, is valid without probable cause and a warrant. The acquisition of the Petitioner's CSLI data is consistent with these requirements, and thus no search warrant was required. Therefore, this Court should affirm the use of Petitioner's CSLI data pursuant to 18 U.S.C. § 2703(d).

C. *Carpenter* does not apply to a request for a one-hour tower dump under 18 U.S.C. § 2703(d), because the privacy concerns in *Carpenter* do not apply to the snapshot of information that a tower dump provides.

Carpenter's limited applicability to CSLI data protected by privacy interests does not extend to tower dump data. *Carpenter*, 585 U.S. __ (slip op., at 15). Tower dump applications

under 18 U.S.C. § 2703(d) "request that cellular phone providers provide all cell phone numbers that used any of multiple towers in a geographic area during a period of time when a crime was committed in that area." 11 A.L.R. Fed. 3d Art. 1 (Originally published in 2016). The greatest concern cited by the *Carpenter* court was that CSLI data can provide "near perfect surveillance, as if it had attached an ankle monitor to the phone's user." *Carpenter*, 585 U.S. __ (slip op., at 13). A tower dump does not provide the same intimate details that concerned the Carpenter court. A tower dump is more similar to post-*Carpenter* decisions relating to the use of pole cameras. *See United States v. Kubasiak*, 18-cr-120-pp, 2018 U.S. Dist. LEXIS 172514 (E.D. Wisc. October 5, 2018) ; *United States v. Kay*, 17-CR-16, 2018 U.S. Dist. LEXIS 141615 (E.D. Wisc. August 21, 2018); *United States v. Tirado*, 16-CR-168, 2018 U.S. Dist. LEXIS 141605 (E.D. Wisc. August 21, 2018). In these cases, the courts all held that *Carpenter's* privacy concerns did not overlap into the sphere of camera use. *Id*. While Petitioner will point that Carpenter states the decision applies to tower dumps, it is important to note that there was not a tower dump in that case. *Carpenter*, 585 U.S. __ (slip op.). The two searches that the Government performed in *Carpenter* were both CSLI data requests. *Id.* at __ (slip op., at 3).

The Government's use of 18 months of surveillance video was not enough to violate a person's reasonable expectation of privacy. *United States v. Tuggle*, No. 16-cr-20070-JES-JEH, 2018 U.S. Dist. LEXIS 127333, at *10 (C.D. Ill. July 31, 2018). The Government used 18 months of security footage in its investigation for conspiracy against the defendant. *Id.* at 5. The Government placed the camera to watch the defendant's home without ever seeking a warrant. *Id.* In holding that the use of a warrantless pole camera for 18 months did not violate the defendant's reasonable expectation of privacy, the Court reasoned that "[p]ole cameras are limited to a fixed location and capture only activities in camera view, as opposed to GPS, which

can track an individual's movement anywhere in the world." *Id.* at 10. Similarly, the tower dump in this case is a snapshot of all individuals who connected to one of the requested towers, during the small one-hour period, for which the Government requested. Likewise, a tower dump is not as invasive as GPS because it does not track an individual's movements. *Id.*

Since the tower dump does not track a person's movements, a tower dump request under 18 U.S.C § 2703(d) does not implicate the privacy concerns that were cited in *Carpenter*. *Carpenter*, 585 U.S. __ (slip op., at 15). The privacy interests are greatest in one's home, and as such, the use of 18 months of warrantless recording at one's residence is of greater privacy concern than a one-hour tower dump. Therefore, if a long-term warrantless home surveillance does not violate the Fourth Amendment, the use of a short-term data request shall not either. This Court should affirm the use of the tower dump under 18 U.S.C. § 2703(d).

CONCLUSION

The Fourteenth Circuit correctly found no Fourth Amendment violation. First, the Government's forensic search of Escaton's electronic devices did not require a reasonable suspicion. Reasonable suspicion is not required because the historical purpose and routine nature of the border search context override individual privacy interests. Second, the warrantless use of CSLI and tower dump data pursuant to 18 U.S.C. § 2703(d) is not a Fourth Amendment violation. The warrantless search is constitutional because the data requested falls within the border search exception, and is within *Carpenter's* privacy threshold. For the foregoing reasons, Respondent respectfully requests that this Court AFFIRM the ruling of the Fourteenth Circuit.

Respectfully submitted,
/s/ Alicia Henry
/s/ Eric Leeman
Attorneys for Respondent

CERTIFICATE OF SERVICE

We certify that a copy of the Respondent's brief was served upon the Petitioner, Hector Escaton, and, through the counsel of record by verified U.S. Mail return receipt requested, on this, the 10th day of February, 2023.

Attorneys for
Respondent