Team P7

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,
FOURTEENTH CIRCUIT

BRIEF FOR RESPONDENT

COUNSEL FOR RESPONDENT
FEBRUARY 10, 2019

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Regulations

Other Authorities

QUESTIONS PRESENTED

1. Under the Fourth Amendment, can government officers conduct a forensic search of a person's electronic devices without reasonable suspicion when the person enters the United States through an international border where the expectation of privacy at its lowermost?
2. Under *Carpenter v. United States*, does the Court's seven day limitation on the use of cell-site location information prohibit the government from acquiring three days of cell-site location information corresponding with the window in which a crime occurred, one-hundred cumulative hours of daytime cell site location information targeting the area of the crime spree, and tower dump data limited to the time immediately surrounding the crime?

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 PROVISION

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.

INTRODUCTION

Respondent, 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

This Court should affirm the decision of the Fourteenth Circuit Court of Appeals because Petitioner's rights under the Fourth Amendment were not violated. The Fourth Amendment does not require that government officers must have reasonable suspicion before conduction forensic searches of electronic devices at the border. Further, law enforcement's acquisition of three days of cell-site location information, one-hundred cumulative hours of cell-site location information, and cell tower dumps data did not violate Petitioner's reasonable expectation of privacy.

Since before the adoption of the Fourth Amendment, customs officers have enjoyed plenary authority to search property crossing the border without a warrant, probable cause, or reasonable suspicion. All international travelers have an obligation to present themselves and their effects for a border inspection. Here, when Hector Escaton (Petitioner) returned to the United States and crossed the West Texas border, he subjected himself and his property to a search because he was entering the country at the border. Under well-established precedent, border searches are reasonable simply because they occur at the border. They are therefore exempt from both the probable cause and warrant requirements that pertain to most searches conducted inside the country. Therefore, this Court has long made clear that the Fourth Amendment permits suspicionless border searches of personal property, including private materials in closed containers. Because the search here was not highly intrusive, did not violate

the Petitioner's personal integrity, and was not destructive, the government did not need to have a particularized showing of reasonableness to conduct the search.

The circuit court in this case properly concluded that the government did not need reasonable suspicion to search Petitioner's electronic devices. Because electronic devices are legally and conceptually no different than other closed storage containers—like purses, briefcases, and luggage—presented for entry at the border, they are subject to search without a showing of reasonable suspicion. Courts have uniformly concluded that they will treat electronic devices as closed containers for Fourth Amendment purposes, and several courts have specifically applied this principle to uphold suspicionless searches of computer media at the border.

The reality of the digital age demands more, not less, vigilance at the border to ensure that that border agents can prevent unlawful or harmful materials—no matter the medium—from crossing the border freely without inspection. Malware, graphic materials, and other electronic materials stored on electronic devices are no less important to national security and public welfare than other physical contraband, such as drugs and explosives. Border agents cannot properly mind the borders unless they are authorized to search personal property at the border without regard to the type of container in which people may conceal it. The circuit court held this vision in mind when deciding this case.

The fact that border searches of electronic devices implicate the government's compelling interest in controlling its territorial integrity, regulating the flow of foreign commerce, and blocking the introduction of dangerous contraband is reason enough for the Court to decide that border agents do not need reasonable suspicion to search electronic devices at the border. Any other holding would seriously undermine the nation's vital interest in protecting its borders by removing the significant deterrent effect of suspicionless searches and effectively rendering

electronic devices the smuggler's container of choice for electronic contraband like malware, child pornography, and terrorist plans or communications. Accordingly, this Court should affirm the circuit court's suppression ruling and adopt the view that border agents do not need reasonable suspicion to search electronic devices at the border.

In articulating the limitations on the use of cell-site location information (CSLI), this Court explained that a search occurs when an individual's reasonable expectation of privacy is violated. It has long been understood that short-term surveillance of an individual comports with expectations of privacy that our society is willing to recognize as reasonable. In *Carpenter*, this Court reasoned that the use of seven days of CSLI constitutes a search because it goes beyond the surveillance that our society has come to recognize as reasonable. The court explained that with seven days of CSLI data law enforcement is able to gain an "all encompassing record" of an individual's movements, providing an "intimate view" into the individual's life. Further, this Court explained that this amount of information does not comport with society's reasonable expectation of privacy because traditionally law enforcement would not be able to engage in this level of surveillance due to "limited police resources."

In this case, the circuit court properly concluded that law enforcement's acquisition of CSLI data did not violate Petitioner's reasonable expectation of privacy and therefore, was not a search. First, law enforcement's acquisition of three days of cell-site location information was wholly consistent with the limitations on the use of CSLI that this Court established in *Carpenter*. Law enforcement's request for three days of CSLI data did not amount to comprehensive surveillance and was consistent with society's expectation of privacy. This limited request for three days of CSLI data does not implicate the "too permeating police surveillance" that serves as a guide post for this Court's Fourth Amendment jurisprudence.

Second, law enforcement's request for one-hundred cumulative hours of CSLI did not exceed the permissible amount of CSLI data that can be obtained without a warrant under *Carpenter*. Further, this request was limited to weekday hours when most Americans are in the workplace; therefore, the scope of private information that the CSLI data could reveal was limited and likely would not provide an "intimate window into a person's life." Moreover, law enforcement likely could engage in 100 hours of surveillance during traditional business hours even under the constraint of "limited police resources." For these reasons, the Weekday Record request did not violate Petitioner's reasonable expectation of privacy and therefore, was not a search.

Finally, law enforcement's request for tower dump data, limited to thirty minutes before and after the crime, did not violate Petitioner's reasonable expectation of privacy. Tower dump data does not reveal the intimate details of an individual's life that this Court was concerned with in both *Jones* and *Carpenter*. At its best, the data collected from a tower dump shows that an individual was present in an area as wide as a dozen city blocks during a specified period of time. The fixed area captured in tower dump data does not allow law enforcement to uncover an individual's particular movements nor intimate details of the individual's life. For these reasons, the request for tower dump data did not violate Petitioner's reasonable expectation of privacy and therefore, was not a search.

STATEMENT OF THE CASE

Statement of the Facts

On September 25, 2019, Petitioner, a West Texas citizen and resident, returned to the United States from Mexico. (R. at 3). Petitioner entered the United States through a West Texas border checkpoint. (R. at 3). Customs and Border Protection (CBP) Officer Ashley Stubbs

(Officer Stubbs) conducted a routine border search of Petitioner's vehicle. (R. at 3). Upon inspection, Officer Stubbs found three large suitcases in the back of Petitioner's car. (R. at 3).

Officer Stubbs discovered an iPhone, a laptop, three external hard drives, and four USB devices. (R. at 3). Following discovery, Officer Stubbs placed the iPhone on airplane mode—ensuring there was no cellular connection—and confirmed that the laptop had no wireless service connection. (R. at 3). The two devices were not password protected. (R. at 4). Officer Stubbs then conducted a manual search of the iPhone and laptop without assistive technology. (R. at 3). After searching the iPhone, Officer Stubbs returned the phone to Petitioner and detained the remaining electronic devices, including the laptop, hard drives, and USB devices. (R. at 4).

Placed just below the keyboard of the laptop was a paper note. (R. at 3). The note read "Call Delores (201) 181-0981 $$$." (R. at 3). Officer Stubbs recorded the message and Petitioner's iPhone telephone number. (R. at 3). On the laptop, Officer Stubbs discovered certain folders with password protections. (R. at 4). Officer Stubbs inserted the USB devices into the computer and discovered he could not access their content. (R. at 4).

Officer Stubbs delivered the electronic devices to Immigration and Customs Enforcement (ICE) Senior Special Agent & Computer Forensic Examiner Theresa Cullen (Officer Cullen) who was stationed at the border checkpoint. (R. at 4). Officer Cullen used forensic software to copy and scan the devices. (R. at 4). The forensic analysis revealed the laptop held documents containing individuals' bank account numbers and pins, as well as traces of malware. (R. at 4).

CBP notified the Federal Bureau of Investigation (FBI) about the potential bank fraud and identity theft claims and provided them with Petitioner's information, including his telephone number—which Officer Stubbs found on Petitioner's iPhone. (R. at 4, 6). The FBI was investigating "ATM skimming" of Mariposa Bank ATMs in Sweetwater during October of 2018.

(R. at 4). The FBI examined the connections between the forensic evidence CBP provided and the illegal activity Mariposa Bank reported—skimming occurred at eight of Mariposa's ATMs, three in Escalante and five in Sweetwater. (R. at 4).

Mariposa Bank determined that the skimming occurred in early October and the perpetrators employed several methods to steal information and cash from the ATMs. (R. at 5). Two ATMs had "skimmers" overlaying the debit card readers on the ATMs, two ATMs had malware—similar to that found on Petitioner's USB devices—installed through a USB port on the ATMs, and one ATM had sophisticated malware that allowed the criminals to withdraw cash directly from the ATM. (R. at 5, 6). Mariposa Bank's investigation revealed an estimated $50,000 of losses in October 2018 through withdrawals and false account creation resulting from ATM skimming and that hundreds of identities of Mariposa Bank customers were stolen. (R. at 5). Surveillance photographs near the ATMs showed a man in a black sweatshirt at the three Sweetwater ATMs. (R. at 5).

Based on the forensic evidence provided by CBP and the information from Mariposa Banks, the FBI requested three tower dumps from the cell sites near the Sweetwater ATMs, pursuant to 18 U.S.C.A. § 2703(d) (West) of the Stored Communications Act (SCA), for 30 minutes before and 30 minutes after the man in the surveillance photos approached the ATMs. (R. at 5). Petitioner's phone number matched one of the numbers produced from the three tower dumps. (R. at 6).

With this information, the U.S. Attorney's office and FBI applied for court orders under the SCA to obtain Petitioner's cell phone records from Delos Wireless. (R. at 6). A federal Magistrate issued an order direction Delos Wireless to disclose the "cell site records corresponding to [Petitioner's] telephone number . . . during the period [of] October 11, 2018, through October 13, 2018." (R. at 6). Petitioner's cell site records indicated that his cell phone

was in the area of one of the Sweetwater ATMs on October 12, 2018. (R. at 6). This was the only ATM that Petitioner's records indicated his phone was near between October 11, 2018, and October 13, 2018. (R. at 6).

The government requested an additional order to Delos Wireless from the magistrate judge. (R. at 6). The additional order was to disclose "cell site sector information for [Petitioner's] and 'Delores's' telephone [numbers] for all weekday records between October 1 and 12 between the hours of 8 AM MDT and 6 PM MDT, as well all subscriber information for 'Delores's' telephone." (R. at 6). The records revealed that the phone number belonged to Delores Abernathy (Ms. Abernathy) and she was in the area of three of the ATMs in early October. (R. at 6). The records also placed Ms. Abernathy and Petitioner together during the same time period. (R. at 6).

Procedural History

The Government indicted Petitioner on three counts: Count One for Bank Fraud, in violation of 18 U.S.C.A. § 1344 (West); Count Two for Conspiracy to Commit Bank Fraud, in violation of 18 U.S.C.A. § 1349 (West); and Count Three for Aggravated Identity Theft, in violation of 18 U.S.C.A. § 1028(A) (West). (R. at 7). Prior to trial in the District of West Texas, Petitioner filed a motion to suppress the results of the forensic search and the cell-site data requested from Delos Wireless. (R. at 7). The district court denied the motion on both issues. (R. at 7). A jury convicted Petitioner on all three counts. (R. at 3).

Petitioner appealed to the United States Court of Appeals for the Fourteenth Circuit. (R. at 3). On appeal, Petitioner asserted that the district court erred in denying his motion to suppress because the forensic search of his electronic devices and the cell site location information requests violated his Fourth Amendment rights. (R. at 3). The circuit court disagreed, holding that law enforcement acted properly and within the bounds of the Fourth Amendment

protections. (R. at 3). The circuit court affirmed the district court's ruling denying Petitioner's motion to suppress. (R. at 3). Petitioner petitioned for writ of certiorari to the Supreme Court of the United States. (R. at 1). The Court granted certiorari on November 22, 2022. (R. at 1).

ARGUMENT

I. THE UNITED STATES COURT OF APPEALS FOR THE FOURTEENTH CIRCUIT PROPERLY HELD THAT NO REASONABLE SUSPICION IS REQUIRED TO CONDUCT A FORENSIC SEARCH OF ELECTRONIC DEVICES AT INTERNATIONAL BORDER CROSSINGS.

a. Border Agents Have Longstanding Plenary Authority Under the Fourth Amendment to Conduct Suspicionless Searches of Personal Property At the International Border.

The Supreme Court has repeatedly recognized the government's longstanding plenary authority to conduct border searches as an exception to the probable cause and warrant requirements in the Fourth Amendment. *See, e.g., United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985); *United States v. Alfonso*, 759 F.2d 728, 733–34 (9th Cir. 1985). Searches made at the border "pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border." *United States v. Ramsey*, 431 U.S. 606, 616 (1977). Courts have long recognized that the government possesses broad authority to conduct searches of persons and their belongings at the border to protect its "paramount interest" in protecting its "territorial integrity," which "is at its zenith" at the border. *United States v. Flores-Montano*, 541 U.S. 149, 153 (2004). *See also United States v. Ickes*, 393 F.3d 501, 506 (4th Cir. 2005) (characterizing the government's interests as "overriding").

i. Under the longstanding border-search exception to the Fourth Amendment's warrant requirement, the border search of Petitioner's electronic devices did not require reasonable suspicion.

The Fourth Amendment provides, in part, "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. Ordinarily, "reasonableness requires the obtaining of a judicial warrant." *United States v. Touset*, 890 F.3d 1227, 1232 (11th Cir. 2018) (quoting *Riley v. California*, 134 S. Ct. 2473, 2482 (2014)). Border searches are, however, different. *Touset*, 890 F.3d at 1232. The authority of border officers to conduct suspicionless searches at the border predates the adoption of the Fourth Amendment and the courts have long recognized this authority as an aspect of the sovereign's interest in controlling its borders. *See United States v. Villamonte-Marquez*, 462 U.S. 579, 585 (1983) (stating government's authority to perform border searches has an "impressive historical pedigree"); *Witt v. United States*, 287 F.2d 389, 391 (9th Cir. 1961) ("[D]ifferent rules are applicable [to the border], and for over a hundred years have been applicable with respect to the plenary power to search at the border.").

Courts have recognized the border searches "have a unique status in constitutional law." *United States v. Vega-Barvo*, 729 F.2d 1341, 1344 (11th Cir. 1984). This exception is based on the recognition that the United States has a compelling interest in securing its borders and regulating both who and what may enter the country. *Montoya de Hernandez*, 473 U.S. at 537–38; *Ramsey*, 431 U.S. at 620; *United States v. Alfaro-Moncada*, 607 F.3d 720, 728 (11th Cir. 2010). The exception is also based on the recognition that the expectation of privacy is lower at the border than in the interior. *Montoya de Hernandez*, 473 U.S. at 539; *see also Alfaro-Moncada*, 607 F.3d at 728. The balance of those interests is both "qualitatively different" and construed "much more favorable" to the United States at the border. *Montoya de Hernandez*, 473 U.S. at 538, 544; *Alfaro-Moncada*, 607 F.3d at 728, 730.

Consistent with the compelling interest to control what enters through the United States' borders, courts have given border agents broad authority to search vehicles and persons as they enter the United States, including their personal effects. *Flores-Montano*, 541 U.S. at 152 ("The government's interest in preventing the entry of unwanted persons and effects is at its zenith at

the international border."). The authority of the United States to search the baggage of arriving international travelers is based on its inherent sovereign authority to protect its territorial integrity. *Torres v. Com. of Puerto Rico*, 442 U.S. 465, 473–74 (1979). The United States is entitled, by reason of that authority, to require "whoever seeks entry must establish the right to enter and to bring into the country whatever he may carry." *Id.* "The government has an overriding interest in securing the safety of its citizens and to do this it must seek to prevent the introduction of contraband into the country." *Ickes*, 393 F.3d at 506 (internal citations and quotations omitted).

Border Searches by their very nature are reasonable under the Fourth Amendment, and they do not require reasonable suspicion. *Montoya de Hernandez*, 473 U.S. at 538; *Ramsey*, 431 U.S. at 616–18. "A greater interest on the side of the government at the border is coupled with a lesser interest on the side of the potential entrant. Since 'a port of entry is not a traveler's home,' his expectation of privacy there is substantially lessened." *Ickes*, 393 F.3d at 506 (quoting *United States v. Thirty-Seven (37) Photographs,* 402 U.S. 363, 376 (1971)). As the Eleventh Circuit has noted, "[b]ecasue an individual's expectation of privacy is at its lowermost at border entry points, the officer need not possess any level of suspicion." *Denson v. United States*, 574 F.3d 1318, 1340 (11th Cir. 2009). In addition, border searches need not take place at the actual border but may occur at places considered the "functional equivalent" of a border, such as at an airport where international flights arrive. *Almeida-Sanchez v. United States*, 413 U.S. 266, 273 (1973).

Border agents conducting border searches serve this compelling governmental interest and thus "have more than merely an investigative law enforcement role at the border. *Montoya de Hernandez*, 473 U.S. at 544. Terroristic acts within the United States and the growing concern for international drug smuggling have only heightened the concern for border agents to be vigilant in searching persons and merchandise at the border for contraband. *See Montoya de*

Hernandez, 473 U.S. at 538 (referencing the national crisis caused by smuggling of illegal narcotics into the United States); *United States v. Yang*, 286 F.3d 940, 944 n.1 (7th Cir. 2002) (referring to the September 11, 2001 attacks); *Alfaro-Moncada*, 607 F.3d at 730–31 (citing studies on various methods terrorists could use to commit chemical, biological, or nuclear attacks). Thus, the border is where the government must be the most vigilant to "interdict those who would further crime, introduce matter harmful to the United States, or even threaten the security of its citizens." *United States v. Okafor*, 285 F.3d 842, 845 (9th Cir. 2002).[1]

ii. Border agents did not need reasonable suspicion to search Petitioner's electronic devices because they need reasonable suspicion only where they conduct an invasive search of a person or destructive search of property.

The Supreme Court has only required reasonable suspicion once in the border context—when it considered the prolonged detention of a person suspected of smuggling drugs in her alimentary canal. *Touset*, 890 F.3d at 1233 (citing *Montoya de Hernandez*, 473 U.S. at 541–544). The Court declined, however, to hold that border agents need particularized suspicion for the search of a person's effects at the border. *See Id.* For instance, in *Flores-Montano,* the Court rejected the defendant's claim that the removal, disassembly, and reassembly of his vehicle's fuel tank required reasonable suspicion, noting that the considerations that might

[1] In addition to case law, there is a long list of statutes and regulations granting border agents the authority to conduct searches at the border—none of which requires reasonable suspicion before exercising the authority. *See* 19 U.S.C.A. § 1496 (West) (authorizing border agents to search the baggage of persons entering the country); 19 C.F.R. § 162.6 (authorizing border agents to inspect and search all persons, baggage and merchandise arriving from foreign countries); 19 U.S.C.A. § 1582 (West) (authorizing border agents to detain and search "all persons coming into the United States from foreign countries").

require some level of suspicion for "highly intrusive searches of the person" do not apply to vehicle searches. 541 U.S. at 150, 152.

The Supreme Court has also declined to determine "what level of suspicion, if any is required for non- routine border searches such as strip, body-cavity, or involuntary x-ray searches" *Touset*, 890 F.3d at 1233 (citing *Montoya de Hernandez*, 473 U.S. at 541 n.4), or "whether, and under what circumstances a border search might be deemed unreasonable because of the particularly offensive manner in which it was carried out." *Ramsey*, 431 U.S. at 618 (internal quotation marks omitted). The Supreme Court has never required any particularized suspicion for the border search of property, although it has left open the possibility that some property searches may be "so destructive" that they would require a level of suspicion similar to that required for "highly" intrusive searches of people. *Touset,* 890 U.S. at 1233 (quoting *Flores-Montano*, 541 U.S. at 152, 155–56).

In applying the Fourth Amendment's reasonableness standard to highly intrusive searches of a person's body at the border, the Eleventh Circuit has employed a flexible test that "adjusts the strength of suspicion required for a particular search to the intrusiveness of that search. *United States v. Villabona-Garnica*, 63 F.3d 1051, 1057 (11th Cir. 1995); *Vega-Barvo*, 729 F.2d at 1344. Because the search here was of electronic devices and was not an invasive physical search of the defendant's body, nor was it a search that required prolonged detention, border agents did not need to have reasonable suspicion to detain Appellant and search his phone, laptop, and hard drives.

iii. Border agents may conduct searches of closed containers and items of personal property contained therein without particularized suspicion.

Due to longstanding border search authority, border agents may search, without particularized suspicion, the contents of a traveler's briefcase and luggage, *United States v. Tsai*, 282 F.3d 690, 696 (9th Cir. 2002), his "purse, wallet, or pockets," *Henderson v. United States*,

390 F.2d 805, 808 (9th Cir. 1967), and the papers stored in such closed containers. *See United States v. Schoor*, 597 F.2d 1303, 1305–06 (9th Cir. 1979) (airway bills carried by passengers); *United States v. Grayson*, 597 F.2d 1225, 1227 (9th Cir. 1979) (papers in shirt pocket); *United States v. Fortna*, 796 F.2d 724, 738 (5th Cir. 1986) (documents in carry-on bag, including map and handwritten note); *see also* Wayne R. LaFave, *Search & Seizure: A Treatise on the Fourth Amendment*, § 10.5(a) at 193 (4th ed. 2004) ("Papers may be examined" at the border); *Villamonte-Marquez*, 462 U.S. at 588–93 (upholding suspicionless boarding of vessels for inspection of documents); *contra United States v. Arnold*, 533 F.3d 1003 (9th Cir. 2008). They may also view pictures, films, and similar graphic materials. *See United States v. Thirty-Seven (37) Photographs*, 402 U.S. 363, 365 (1971); *United States v. 12 200-Foot Reels of Super 8mm. Film*, 413 U.S. 123, 124 (1973) ("movie films, color slides, photographs, and other printed and graphic material"); *United States v. Borello*, 766 F.2d 46, 58–59 (2d Cir. 1985) ("the opening of the cartons and the screening of the 8-millimeter films were plainly permissible steps in a reasonable border search").

In *Flores-Montano*, the Supreme Court reaffirmed the broad power of border agents to search property without particularized suspicion, holding "that the Government's authority to conduct suspicionless inspections at the border includes the authority to remove, disassemble, and reassemble a vehicle's fuel tank." 541 U.S. at 155. While *Flores-Montano* involved the fuel container in a car, nothing in the opinion suggests the Court would apply a different analysis to border searches of other physical objects and containers. *See Flores-Montano*, 541 U.S. at 155–56; *Touset*, 890 F.3d at 1233; *and see United States v. Camacho*, 368 F.3d 1182, 1183 (9th Cir. 2004) ("The Supreme Court [in *Flores-Montano*] recently made clear that reasonable suspicion is usually not required for officers to conduct non-destructive border searches of *property*.") (emphasis added). Therefore, *Flores-Montano* was not simply a "gas tank" case; rather, it

reaffirmed the overarching Fourth Amendment principle governing this appeal: searches of property, including electronic devices, at the border, do not require reasonable suspicion.

b. Computer Storage Devices Are Neither Conceptually nor Constitutionally Different Than Other Closed Storage Containers Subject to Suspicionless Border Searches.

Computer devices are conceptually no different for Fourth Amendment purposes than other closed storage containers that are subject to suspicionless searches at the border. To be sure, outside the border context, "individuals undoubtedly have a high expectation of privacy in the files stored on their personal computers." *United States v. Adjani*, 452 F.3d 1140, 1146 (9th Cir. 2006). This is equally true, however, of their personal belongings and effects stored in purses, suitcases, briefcases, and the like, which nonetheless are justifiably exposed to suspicionless searches at the border to protect the nation against imported threats. *See Tsai*, 282 F.3d at 696; *Henderson*, 390 F.2d at 808; *Schoor*, 597 F.2d at 1305–06; *Grayson*, 597 F.2d at 1227; *Fortna*, 796 F.2d at 738. There is no reason to apply a different rule at the border for computers just because they can store—in electronic form—equally private material. For constitutional purposes, nothing distinguishes a computer from other closed containers used to store highly personal items; they are all, conceptually, repositories that can hold not only innocent materials, but also contraband and evidence of criminal conduct. Therefore, the Fourteenth Circuit properly held that border agents did not need reasonable suspicion to search Appellant's phone, laptop, and hard drives.

i. The Third, Fourth, Sixth, and Eleventh Circuit Courts of Appeal have held that no suspicion is required to search electronic devices at the border.

This Court has not yet addressed the question of whether a border search of a phone, laptop, hard drive, or other electronic device requires reasonable suspicion. However, the Circuit courts that have addressed the issue, excluding the Ninth Circuit, have determined that a border search of digital evidence does not demand reasonable suspicion, and this Court should join.

First, the Third Circuit reached the conclusion that border patrol agents do not need reasonable suspicion to search electronic devices. In *United States v. Linarez-Delgado*, 259 F. App'x 506, 507 (3d Cir. 2007), a customs officer searched the defendant's camera when he attempted to re-enter the country from Mexico. After the search, the agent believed the defendant was involved in drug smuggling. *Id.* Following, agents arrested the defendant and charged him with various drug offenses. *Id.* Defendant moved to suppress the evidence, asserting the search of his camera was a violation of his Fourth Amendment rights. *Id.* The circuit court affirmed the district court's denial of his suppression motion. *Id.* The court held "Customs Officers exercise broad authority to conduct routine searches and seizures for which the Fourth Amendment does not require . . . reasonable suspicion." *Id.* at 508 (citations omitted). It elaborated, "[d]ata storage media and electronic equipment, such as films, computer devices, and videotapes may be inspected and viewed during a reasonable border search." *Id.*

The Fourth Circuit has reached the same conclusion, declaring an agent need not have reasonable suspicion to conduct a border search of digital evidence. In *Ickes*, the defendant arrived at the Canadian-United States border near Detroit, Michigan. 393 F.3d at 502. A customs inspector looked at the defendant's video camera which had a recording of a tennis match, most of which focused on a young ball boy. *Id.* A more thorough search uncovered a computer and 75 discs containing child pornography. *Id.* at 503. Subsequently, the officers charged the defendant with transporting child pornography. *Id.* He filed a motion to suppress, claiming that the search violated his Fourth Amendment rights. *Id.* The Fourth Circuit disagreed. It noted the "'impressive historical pedigree of the Government's power and interest' at the border." *Id.* at 505 (quoting *Flores-Montano*, 541 U.S. at 153). The court continued, since our country began, "customs officers have wielded broad authority to search the belongings of would-be entrants without obtaining a warrant and without establishing probable cause." *Ickes*, 393 F.3d at 505

(citations omitted). The court affirmed the lower court's denial of the defendant's suppression motion. *Id.* at 507–08.

The Sixth Circuit agrees. In *United States v. Stewart*, 729 F.3d 517 (6th Cir. 2013), border agents decided to search the defendant's luggage and two computers at the Detroit Airport after he provided "standoffish" and "confrontational" answers to their questions. *Id.* at 520. After finding a dozen thumbnail images of nude children on one of the laptops, the border agents detained both laptops for a further search off-site at the main office. *Id.* at 521. The search of those laptops resulted in the defendant being charged with transporting child pornography. *Id.* The defendant moved to suppress the evidence because he claimed that the off-site search of his computers was an extended border search, which required reasonable suspicion to search. *Id.* The district court denied the motion, and a jury convicted him. *Id.* at 521–22. While endorsing the need for reasonable suspicion for an extended border search, the Sixth Circuit found that searching the laptops at Immigration and Customs Enforcement's (ICE's) office was not an extended border search. *Id.* at 525–26. Accordingly, the agents did not need reasonable suspicion to search the laptops. *Id.* at 526.

Most recently, the Eleventh Circuit has spoken on the issue. In *Touset*, border agents "forensically searched [the defendant's] electronic devices after he arrived at the Atlanta airport on an international flight." 890 F.3d at 1230. The searches revealed child pornography on two laptops and two external hard drives. *Id.* The search of those laptops resulted in the defendant being charged with transporting child pornography. *Id.* at 1231. The defendant filed motions to suppress the evidence obtained from his electronic devices at the border. *Id.* The district court denied the motion, and a jury convicted him. *Id.* The Eleventh Circuit adopted the notion that the Fourth Amendment permits forensic searches of electronic devices at the border without

suspicion. *Id.* at 1232. Accordingly, the agents did not need reasonable suspicion to search the laptops. *Id.*

Contrary to the Third, Fourth, Sixth and Eleventh Circuits, only the Ninth Circuit has required a showing of reasonable suspicion to search digital devices at the border. *See United States v. Cotterman*, 709 F.3d 952, 962–70 (9th Cir. 2013) (*en banc*). In *Cotterman*, the defendant crossed the Mexico-United States border, where border agents detained his two laptops for a further search based on the defendant's 15-year-old conviction for child sexual exploitation offenses. *Id.* at 957–58. ICE searched the laptops at its office 170 miles away, where the examiner found hundreds of images of child pornography. *Id.* at 958–59. The district court granted the defendant's motion to suppress evidence, finding that the search was an extended border search and that the border agents did not have reasonable suspicion to search the computers. *Id.* at 959. The Ninth Circuit held that the search was not an extended border search but that the border agents required reasonable suspicion to search a computer. *Id.* at 961–65. The court found that the officers had reasonable suspicion to search the computers based on the defendant's prior conviction as well as the fact that he was returning from Mexico, a country associated with sex tourism. *Id.* at 968–70. It reversed the district court's order. *Id.* at 970. As pointed out in one of the opinions dissenting from the requirement for reasonable suspicion, "[t]he majority's holding contravenes Supreme Court precedent, defies logic and common sense, and is unworkable." *Id.* at 978 (Callahan, J., *dissenting*). The dissent stated that "electronic devices are like any other container that the Supreme Court has held may be searched at the border without reasonable suspicion." *Id.* at 976 (*citing Ickes*, 393 F.3d at 507). 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. *Cotterman*, 709 F.3d at 977–78.

In this case, when deciding the defendant's motion to suppress evidence, the circuit court joined its sister courts—the Third, Fourth, Sixth, and Eleventh Circuits—in holding that border agents do not need reasonable suspicion to search electronic devices. The government urges this Court to affirm the denial of the defendant's suppression motion on the basis that a border search of his digital devices does not require any particularized showing of suspicion. This Court may affirm the denial of the motion to suppress on any ground supported by the record. *United States v. Perkins*, 787 F.3d 1329, 1344 (11th Cir. 2015). When the defendant arrived at the border and presented himself to border agents for inspection and entry into the United States, those officers were legally authorized to detain his laptops, hard drives, and phone for further inspection. This search was reasonable. It did not involve a highly intrusive search of the defendant's person. Neither did it involve a "personal indignity" consisting of physical contact, exposure of intimate body parts, or use of force. See *Vega-Barvo*, 729 F.2d at 1346 (the "personal indignity suffered by the individual searched controls the level of suspicion required to make the search reasonable"); *Villabona-Garnica*, 63 F.3d at 1057 (standing for the same proposition). The search of the electronic devices was not carried out in an offensive manner, nor was it destructive. The search was reasonable, so border agents had no need for a showing of particularized suspicion to search. This Court should join its sister circuits that have found that border agents do not need reasonable suspicion to search items at the border.

ii. Computer storage devices are conceptually identical to closed storage containers.

Conceptually, computers are the "modern analogues" of "earlier methods of storing information." *In re Grand Jury Subpoena Duces Tecum Dated Nov. 15, 1993*, 846 F. Supp. 11, 13 (S.D.N.Y. 1994). "A computer file is a repository for information and images in electronic form, just as a footlocker is a repository for more tangible items such as papers and other personal effects." *Trulock v. Freeh*, 275 F.3d 391, 409 (4th Cir. 2001) (Michael, J., concurring).

Although computers today have an "unparalleled ability to store and process information" and "are increasingly relied upon by individuals in their work and personal lives," *United States v. Hunter*, 13 F. Supp. 2d 574, 583 (D. Vt. 1998), "[t]here is no justification for favoring those who are capable of storing their records on a computer over those who keep hard copies of their records." *Id.* at 584. As the Ninth Circuit has explained, "[c]omputers are simultaneously file cabinets (with millions of files) and locked desk drawers; they can be repositories of innocent and deeply personal information, but also of evidence of crimes." *Adjani*, 452 F.3d at 1152. Thus, the "differences between computer files and physical repositories of personal information and effects are legally insignificant." *Trulock*, 275 F.3d at 410 (Michael, J., *concurring in part*).

Accordingly, for Fourth Amendment purposes, "[c]ourts have uniformly agreed that computers should be treated as if they were closed containers." *United States v. Al-Marri*, 230 F. Supp. 2d 535, 541 (S.D.N.Y. 2002); *accord United States v. Upham*, 168 F.3d 532, 536 (1st Cir. 1999); *Davis v. Gracey*, 111 F.3d 1472, 1480 (10th Cir. 1997); *Trulock v. Freeh*, 275 F.3d 391, 403 (4th Cir. 2001); *United States v. Chan*, 830 F. Supp. 531, 534 (N.D. Cal. 1993); *United States v. Barth*, 26 F. Supp. 2d 929, 936 (W.D. Tex. 1998); *United States v. David*, 756 F. Supp. 1385, 1390 (D. Nev. 1991); *see also United States v. Runyan*, 275 F.3d 449, 458 (5th Cir. 2001) (both parties conceded that computer disks are "containers" for Fourth Amendment purposes); *but cf. United States v. Carey*, 172 F.3d 1268, 1275 (10th Cir. 1999) (criticizing file cabinet analogy where police with search warrant for only drug evidence expanded scope of computer search to child pornography evidence).

It follows, that because border agents can search the contents of suitcases, purses, and briefcases without particularized suspicion, there is no reason to grant special treatment to computers simply because they store information electronically. It should not matter whether a person keeps documents and pictures in "hard copy" form in a briefcase or stored digitally in a

computer. The authority of border agents to search the former should extend equally to searches of the latter. Indeed, this highlights the source of border agents' ability to search electronic devices. Had defendant carried with him in a briefcase hard copies of the bank-skimming malware that were contained on his computer devices, there would be no doubt that a border agent could, without any suspicion, search the contents of the briefcase and then seize any evidence found during the search. And it would not matter whether the Appellant kept the malware in a file folder labeled "confidential and private," or whether it was co-mingled with otherwise innocent but private papers and effects.

Therefore, for the aforementioned reasons, this Court should adopt the view of the United States Court of Appeals for the Fourteenth Circuit and adopt the view that no reasonable suspicion is required to conduct a forensic search of electronic devices at border crossings.

II. LAW ENFORCEMENT'S REQUEST FOR HISTORICAL CELL-SITE LOCATION INFORMATION FOR THE PERIOD OF TIME CORRESPONDING WITH THE CRIME DID NOT VIOLATE PETITIONER'S FOURTH AMENDMENT RIGHTS.

In *Carpenter v. United States*, 138 S. Ct. 2206, 2210 (2018), this Court was presented with the question of "whether the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements." There, this Court reviewed a case where a wireless carrier had produced records of Cell Site Location Information (CSLI) that revealed the location of the petitioner's cell phone for a period spanning 127 days." *Id.* at 2212. This Court explained that the Fourth Amendment "seeks to secure 'the privacies of life' against 'arbitrary power'" and "'to place obstacles in the way of a too permeating police surveillance.'" *Id.* at 2214. Ultimately, this Court issued a narrow decision, in which it held "that accessing seven days of CSLI constitutes a Fourth Amendment search;" thereby limiting the use of CSLI data obtained without a warrant through the SCA to a period of 6 days or less. *See id.* at 2217.

This Court explained that "the ability to chronicle a person's past movements through the record of his cell phone signals" was a new phenomenon that implicated the individual's reasonable expectation of privacy. *Id.* at 2216. The roots of the individual's expectation of privacy in his physical location and movements were traced back to *United States v. Knotts*, 460 U.S. 276, 276 (1983), where the Court held that police had not conducted a search when they tracked the signal of a beeper within the petitioner's car because an individual traveling on a public road had no reasonable expectation of privacy in his movements. *Carpenter*, 138 S. Ct. at 2215. The Court then went on to discuss the implications of its more recent decision involving GPS in *United States v. Jones*, 565 U.S. 400, 402–03 (2012). *Id.* In *Jones*, the court considered whether the use of a GPS tracking device to monitor the movements of a vehicle for a 28-day period constituted a search under the Fourth Amendment. 565 U.S. at 402-03. The majority decided the case on the grounds that the government "physically occupied private property for the purpose of obtaining information" when it placed the GPS monitoring device on the vehicle; therefore, a Fourth Amendment search had occurred. *Id.* at 404. In their concurrences, Justice Sotomayor and Justice Alito both reasoned that the case should have considered whether the defendant's reasonable expectation of privacy was violated by the long-term monitoring of his movements. *See id.* at 414 (Sotomayor, J., concurring); *see also id.* at 419 (Alito, J., concurring). Although *Jones* was decided on the basis of trespass, the *Carpenter* Court focused on the concurring Justices' discussion of privacy concerns that advancements in technology raise. *See Carpenter*, 138 S. Ct. at 2215.

It is these privacy concerns that the Court called upon in its analysis of Carpenter's reasonable expectation of privacy. *Id.* The Court turned to the *Jones* concurrence to explain that "[p]rior to the digital age, law enforcement might have pursued a suspect for a brief stretch, but doing so "'for any extended period of time was difficult and costly and therefore rarely

undertaken.'" *Id.* at 2217 (quoting *Jones*, 565 U.S. at 430 (Alito, J., concurring)). The Court reasoned that due to the difficulty and cost of surveillance, society had formed an expectation that law enforcement could not monitor an individual's movement for an extended period of time. *Id.* Analogizing cell site location information to GPS data, this Court explained that "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.* (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)). For these reasons, the Court determined that allowing the government to access 127 days of cell site location information contravenes society's expectation of privacy. *See id.*

a. The United States Court of Appeals for the Fourteenth Circuit Properly Held Law Enforcement's Request for Less Than Seven Days of CSLI Data Did Not Constitute a Search Under *Carpenter*.

In holding that "an individual maintains a legitimate expectation of privacy in the record of his physical movements," the Court noted "it is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search." *Id.* at 2217 n.3. Each dissenting Justice acknowledged the limitation imposed by the Court's seven-day standard. *See id.* at 2224 (Kennedy, J., dissenting); *see id.* at 2266 (Gorsuch, J., dissenting). In his dissent, joined by Justice Thomas and Justice Alito, Justice Kennedy expressed his concern with the majority's determination that "the Government crosses a constitutional line when it obtains a court's approval to issue a subpoena *for more than six days of cell-site records* in order to determine whether a person was within several hundred city blocks of a crime scene." *Id.* at 2224 (Kennedy, J., dissenting) (emphasis added). Justice Kennedy further explained that "the Court's holding that the Government must get a warrant to obtain *more than six days of cell-site records* limits the effectiveness of an important investigative tool for solving serious crimes." *Id.* at 2233 (emphasis added). Justice Gorsuch also interpreted the majority's opinion as holding that more

than six days of cell-site records constitutes a search under the Fourth Amendment, noting that the majority "tells us that access to seven days' worth of information *does* trigger Fourth Amendment scrutiny." *See id.* at 2266 (Gorsuch, J., dissenting) (alteration in original).

The petitioner attempts to manipulate the language of the Court's opinion by isolating the terms that are advantageous to his position. For example, the Court stated that "[h]aving found that the acquisition of Carpenter's CSLI was a search, we also conclude that the Government must generally obtain a warranted supported by probable cause before acquiring such records." *Id.* at 2221. Petitioner uses this language to support the proposition that the government is always required to obtain a warrant in order to acquire CSLI data. Construing the Court's language in this way ignores the fact that the words "such records" reference the seven days of CSLI data that had previously been classified as acquired via a search. *See id.* As Justice Kennedy explained "[t]he Court suggests that less than seven days of location information may not require a warrant." *Id.* at 2234 (Kennedy, J., dissenting).

i. Law Enforcement's Request for Three Days of Cell-Site Location Information Did Not Infringe Petitioner's Reasonable Expectation of Privacy.

The Fourteenth Circuit's holding that three days of CSLI data did not violate the petitioner's reasonable expectation of privacy is consistent with this Court's holding in both *Jones* and *Carpenter*. In those cases, this Court articulated concerns about the government's ability to engage in long term monitoring of an individual's movements. *See Carpenter*, 138 S. Ct. at 2215 (quoting *Jones*, 565 U.S. at 430 (Alito, J., concurring)). This Court has explained that society has a reasonable expectation that law enforcement cannot secretly monitor an individual's movements for an extended period of time given the resources required to do so. *See Jones*, 565 U.S. at 430 (Alito, J., concurring). This Court has also recognized that "relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable." *Id.*

In *Jones*, the Court did not define the exact point at which tracking the defendant's vehicle became a search but concluded that the point had been crossed before the 28-day mark. *See id.* (Alito, J., concurring). The Court explained that prior to the invention of GPS monitoring, constant monitoring of a vehicle's location for a four-week period "would have required a large team of agents, multiple vehicles, and perhaps aerial assistance." *Id.* The cost associated with such measures would have prevented law enforcement from engaging in extended surveillance in all but the most important investigations. *Id.*

Similarly, in *Carpenter*, the Court explained that CSLI data is cheap and efficient, allowing the government to access "historical location information at practically no expense." 138 S. Ct. at 2218. This Court also explained that CSLI data implicates privacy concerns similar to those presented by GPS because people routinely carry their cell phones "into private residences, doctor's offices, political headquarters, and other potentially revealing locales." *Id.* Further, unfettered access to CSLI would allow the government to retrace a person's whereabouts using up to five years of data. *See id.* Applying the reasoning established in *Jones*, the Court explained that "'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy'" *Id.* at 2215. In order to protect society's reasonable expectation of privacy in their physical movements, the Court concluded that "accessing seven days of CSLI constitutes a Fourth Amendment search." *See id.* at 2217 n.3.

In *United States v. Skinner*, 690 F.3d 772 (6th Cir. 2012), the Sixth Circuit Court of Appeals held that law enforcement did not conduct a search when they tracked the GPS location information emitted from the defendant's cell phone for a period of three days. In that case, the DEA had used data emanating from the defendant's cell phone to establish his location over a three day period as he transported drugs. *Id.* at 774. The court reasoned that the three days of tracking did not amount to comprehensive surveillance that infringed upon the defendant's

reasonable expectation of privacy. *Id.* at 780. The court emphasized that three days of monitoring is consistent with "relatively short-term monitoring of a person's movements on public streets [that] accords with expectations of privacy that our society has recognized as reasonable." *See id.* (quoting *Jones*, 565 U.S. at 430 (Alito, J., concurring)).

Here, police enforcement request for three days of CSLI data was not a search because it did not violate the defendant's reasonable expectation of privacy. Like the three days of GPS surveillance in *Skinner*, requesting three days of CSLI data did not amount to comprehensive surveillance and was consistent with society's expectation of privacy. *See id.* Although society has a reasonable expectation that police cannot engage in surveillance for an extended period of time, engaging in a three-day surveillance operation would not be overly burdensome for law enforcement.

Further, law enforcements request for three days of CSLI data was less invasive than the three days of GPS monitoring in *Skinner* and did not provide an intimate window into petitioner's movements. 690 F.3d at 781. This Court has explained that "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *Id.* at 415 (Sotomayor, J., concurring). GPS tracking devices allow the government to pinpoint the defendant's location within a 100-foot area. *See Jones*, 565 U.S. at 403. Unlike GPS monitoring, CSLI data is imprecise; "in urban areas cell-site records often would reveal the location of a cell phone user within an area covering between around a dozen and several hundred city blocks." *Carpenter*, 138 S. Ct. at 2225 (Kennedy, J., dissenting). One dozen city blocks may contain a wide variety of businesses; making it nearly impossible for the government to determine if the suspect is visiting a doctor, bar, church, or nail salon using CSLI data alone.

Unlike the seven days of historical cell phone records accessed in *Carpenter*, the data accessed here was not capable of providing a comprehensive chronicle of the petitioner's movements. *See id.* at 2212. Just as this Court's holding in *Carpenter* was "a narrow one," the request for CSLI in this case was narrowly tailored to reveal only information related to the three-day window when the ATM skimming had likely occurred. *Id.* at 2220. This limited request for three days of CSLI data does not implicate the "too permeating police surveillance" that serves as a guide post for this Court's Fourth Amendment jurisprudence. *See id.* at 2214; *Jones*, 565 U.S. at 417.

ii. Law Enforcement's Request for Weekday Records Did Not Infringe Petitioner's Reasonable Expectation of Privacy.

In limiting the Weekday Record request to the hours of 8:00 a.m. to 6:00 p.m., law enforcement also limited the privacy concerns related to the data request. According to the United States Bureau of Labor Statistics, over fifty percent of Americans are on the job between the hours of 8:00 a.m. and 5:00 p.m. and at 6:00 p.m. twenty percent of Americans are on the job. *See* Elka Torpey, U.S. Bureau of Labor Statistics, *Career Outlook: Careers for Night Owls and Early Birds*, (2015), https://www.bls.gov/careeroutlook/2015/article/pdf/night-owls-and-early-birds.pdf. Given that a majority of Americans are in the workplace during the hours encompassed by law enforcement's request for Weekday Records, the scope of private information that the CSLI data could reveal was limited and likely would not provide an "intimate window into a person's life." *See Carpenter,* 138 S. Ct at 2217. Moreover, the Weekday Record request could not provide law enforcement with an "all-encompassing record" of the Petitioner's whereabouts because the request excluded the fourteen hours of the day that fall outside of traditional business hours as well as all weekend data. *See id.* Rather, the Weekday Record request is more akin to the "relatively short-term monitoring of a person's movements on

public streets that our society has recognized as reasonable." *See Jones*, 565 U.S. at 430 (Alito, J., concurring).

Further, the Weekday Record request encompassed significantly less hours of CSLI data than what is permissible under *Carpenter*. *See* 138 S. Ct at 2217 n.3. In *Carpenter*, this Court elucidated that the government engages in a search when it requests seven days of CSLI data; ultimately allowing the government to access up to 144 hours of CSLI data without engaging in a search. *See id.* Here, law enforcement requested 100 hours of CSLI data through its weekday request; therefore, the request was not in violation of *Carpenter*. *See id.* Moreover, law enforcement likely could engage in 100 hours of surveillance during traditional business hours even under the constraint of "limited police resources." *See Jones*, 565 U.S. at 416.

For the aforementioned reasons, law enforcement's Weekday Record request, limited to CSLI data between the hours of 8:00 a.m. and 6:00 p.m., did not violate the Petitioner's reasonable expectation of privacy and therefore did not constitute a search.

b. Tower Dumps Do Not Violate an Individual's Reasonable Expectation of Privacy and Do Not Constitute a Search.

A tower dump occurs when law enforcement requests that a cell phone company provide a record of all cell phones that have connected to a particular cell tower during a specified time period. *See In re Cell Tower Records Under 18 U.S.C. 2703(D)*, 90 F. Supp. 3d 673, 674 (S.D. Tex. 2015). Unlike other types of CSLI requests, law enforcement often does not know the identity or phone number of the suspect at the time that an application for a tower dump is submitted. *See id.* Law enforcement often uses tower dump data to identify a suspect during the early stages of an investigation. *See id.* Tower dumps are an especially strong investigative tool in serial crimes because law enforcement is able to cross-reference data from multiple crime scenes and identify suspects who may have been in all locations. *See* Honorable Brian L.

Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in its Electronic Surveillance*, Journal of Constitutional Law, Vol. 16:1, 1, 6 (Oct. 2013).

Following *Carpenter*, courts have reasoned that surveillance of a fixed area does not violate an individual's reasonable expectation of privacy. *See United States v. Kay*, No. 17-CR-16, 2018 WL 3995902 (E.D. Wis. Aug. 21, 2018); *See United States v. Kubasiak*, No. 18-CR-120-PP, 2018 WL 4846761 (E.D. Wis. Oct. 5, 2018). In *Kay*, the court held that pole camera surveillance did not constitute a Fourth Amendment Search. 2018 WL 3995902. In that case, police had installed a hidden camera on a utility pole in order to monitor the defendant's driveway and front yard. *Id.* The court reasoned that pole camera surveillance only captures information within a fixed location and does not provide an "intimate window" into the defendant's life. *Id.* (quoting *Carpenter*, 138 S. Ct. at 2217*).* Similarly*,* in *Kubasiak*, the court held that police had not conducted a search when they surveilled the defendant using a camera that they had installed in his neighbor's house. 2018 WL 4846761. The court reasoned that the "surveillance did not present the kind of aggregate view of intimate details of the defendant's every movement that concerned the concurrence in *Jones*, or the majority in *Carpenter*." *Id.*

Tower dumps do not provide a "comprehensive chronicle of the user's past movements" and therefore, do not implicate the same privacy concerns as other CSLI data requests. *See Carpenter*, 138 S. Ct. at 2210. The data included in a tower dump shows that an individual was present in an area consisting of approximately "a dozen and several hundred city blocks" during a brief time period. *See Carpenter*, 138 S. Ct. at 2225 (Kennedy, J., dissenting). The fixed area captured in tower dump data does not allow law enforcement to uncover an individual's particular movements nor the individual's "familial, political, professional, religious, and sexual associations." *See id.* at 2218. Therefore, tower dumps do violate the individual's reasonable expectation of privacy and do not constitute a search.

Further, law enforcement's tower dump request here was very narrow in scope; limited to thirty minutes before and after the suspect had used the Mariposa Bank ATM. The limited time frame of the request further reduced the potential that the data would reveal intimate information about an individual and was consistent with the short-term surveillance that comports with society's reasonable expectation of privacy. *See Jones*, 565 U.S. at 430 (Alito, J., concurring). For these reasons, law enforcement's tower dump request did not violate Petitioner's reasonable expectation of privacy and therefore, was not a search.

CONCLUSION

By virtue of the government's broad authority to search person's when they seek to enter the United States, Border Agents were allowed to detain and search Petitioner's electronic devices. If a search is not invasive, does not violate the personal dignity of the individual, and is not destructive border agents do not need any particularized showing of suspicion to search a person's property. Further, in light of this Court's limitation on the use of cell-site location information law enforcement's requests for CSLI data here did not constitute a search. Additionally, tower dumps are consistent with short-term surveillance that comports with society's reasonable expectation of privacy and therefore, do not constitute a search. For these reasons, the Court should affirm the district court's denial of the defendant's motion to suppress evidence.

Respectfully submitted,
Attorneys for Respondent