Case No. 10-1011

IN THE

Supreme Court of the United States

HECTOR ESCATON

Petitioner,

v.

UNITED STATES OF AMERICA

Respondent.

On Writ of Certiorari

To the United States Court of Appeals

For the Fourteenth Circuit

BRIEF FOR PETITIONER

Hector Escaton

2019 UCLA Cyber Crimes
Moot Court Competition

Attorneys for Petitioner
HECTOR ESCATON
Team R14

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CONSTITUTIONAL PROVISIONS

STATUTES

UNITED STATES SUPREME COURT CASES

CIRCUIT COURT CASES

OTHER AUTHORITIES

QUESTIONS PRESENTED

1. Whether the Fourth Amendment requires that government officers must have reasonable suspicion before conducting forensic searches of electronic devices at an international border.
2. In *Carpenter*, this Court held that Government's warrantless acquisition of 7 days of cell-site location information pursuant to 18 U.S.C. § 2703(d) was a "search." Did Law Enforcement violate the Fourth Amendment when it obtained three tower dumps, three-days, and 100 hours of CSLI from Petitioner's cell phone without a warrant? If so, did the lower court error in denying petitioner's motion to suppress the evidence?

STANDARD OF REVIEW

This Court considers conclusions of law and application of the law to the facts under the de novo standard and its factual determinations for clear error. *United States v. Muglata,* 44 F.3d 153-, 1536 (11th Cir. 1995); *United States v. Cotterman*, 709 F.3d 952, 968 (9th Cir. 2013) (en banc) (citing *Ornelas v. United States*, 517 U.S. 690, 699 (1996)). The court is to review the court's legal conclusions de novo and its factual findings for clear error, considering the evidence in the light most favorable to the government. *See United States v. Palmer*, 820 F.3d 640, 648 (4th Cir. 2016).

OPINION BELOW

The opinion of the United States Court of Appeals for the Fourteenth Circuit, affirming the district court's decision, is reported as *Escaton v. United States,* 1001 F.3d 1341 (14th Cir. 2021).

CONSTITUTIONAL PROVISIONS AND RULES

"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

The Fourth Amendment establishes an individual's right against "unreasonable" governmental searches and seizures. US. Const. amend. IV. The courts have long recognized border searches as an exception to the warrant requirement of the Fourth Amendment, this does not mean, however, that at the border "anything goes." *United States v. Seljan*, 547 F.3d at 999 (9th Cir. 2008). The Supreme Court has made clear, that the Constitution restricts the border search exception "*subject to* substantive limitations imposed by the Constitution." *United States v. Ramsey*, 431 U.S. 606 at 621 (1972).

At a border or it's 'functional equivalent', government agents may conduct 'routine' searches of persons and property without a warrant or reasonable suspicion. *Almeida Sanchez v. United States*, 413 U.S. 266 (1973). "Non-routine" searches at the border may only be conducted if they have at least a "reasonable suspicion" that the searched individual is smuggling contraband or conducting other illegal activities. (Kim, 2009) [1]

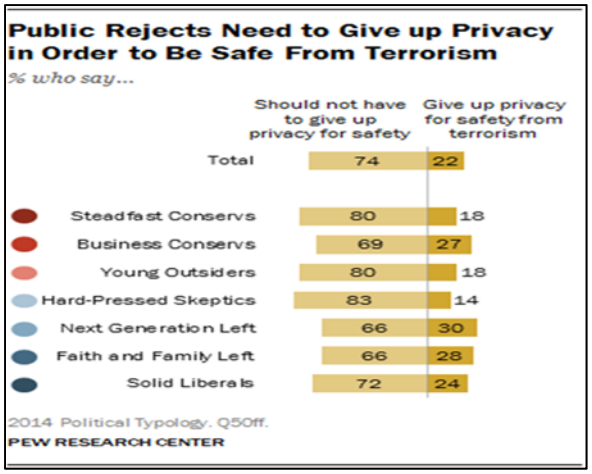
While suspicionless border searches are reasonable simply by virtue of the fact that they occur at the border," *Ramsey*, 431 U.S. at 616; *Montoya de Hernandez*, 473 U.S. at 541. Before the prominence of digital devices, border searches of personal property were "limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy." *Riley v. California*, 134 S.Ct. 2489 (2014).

Justice Louis Brandeis predicted that "[t]he progress of science in furnishing the government with means of espionage [was] not likely to stop with wiretapping." *Olmstead v.*

[1] Yule Kim, Congressional Research Service, Protecting the U.S. Perimeter (2009).

U.S., 277 U.S. 438 (1928*)*. Cell-site technology affords law enforcement the ability to go back in time and track any 'perp' with cellular network access, at any time without a warrant. Cell-site location information (CSLI), are cell tower records of subscriber location data collected every 7 seconds as its user moves in and out of range of a tower's transmission. Law enforcement's unfettered access to 'encyclopedic' quantities of CSLI allows them to review, in the aggregate, a suspect's precise movements for weeks, months, or even years at a time. But what if this new technology was used to monitor--you?

Privacy matters to American people. The right to choose how and what we reveal is at the crux of our identity. Benjamin Franklin said, "those who would give up essential liberty, to purchase a little temporary safety, deserve neither liberty nor safety." This sentiment holds true today, as a majority of Americans (81%) disapprove of the government's collection of our electronic data and (74%) value privacy and freedom over safety. [2]



How can we possibly protect our data from the very people who are charged with protecting, us?

Under the "mosaic theory," public observation of a collection of activities may constitute a search, because it is the aggregation of individual public movements, that reveal a ''snapshot," of the subject's personal life. As such, a series of non-searches could amount to a search when viewed collectively. A mosaic model is appropriate when

[2] George, Gao. What Americans think about NSA surveillance, national security and privacy, http://www.pewresearch.org/fact-tank/2015/05/29/what-americans-think-about-nsa-surveillance-national-security-and-privacy/, see Appendix B.

considering the vast amount of data generated by CSLI; much of it being 'non-content' location information. The CSLI acquired from Petitioner's cell phone was as search under a mosaic theory because the 'Three-day Records' coupled with the 10 days of 'week-day record hours' accumulated to more than 100 hours or two weeks of information which revealed a substantial amount of private information which should not have been made available absent a warrant. The Supreme Court has held that public monitoring of an individual's movements does not violate a right to privacy. In cases like *Jones* and *Carpenter* this Court has illustrated that prolonged surveillance of a person's public activities may reveal details that are both intimate and private. *United States v. Jones*, 565 U.S. 400 (2012); *Carpenter v. United States*, No. 16-402, 585 U.S. (2018).

Judges must now consider that small grants of subscriber data, in isolation may be entirely legal, but multiple forms and requests for these records, taken collectively, may amount to a "search" in violation of the Fourth Amendment. As our Supreme Court held in *Olmstead*, the "'application of a constitution, our contemplation cannot be only of what has been but of what may be.'" *Olmstead,* 277 U.S. 438.

SUMMARY OF ARGUMENT

The Fourteenth Circuit Court of Appeals determined that reasonable suspicion was not required for border agents to conduct a "non-routine search" on an individual's electronic devices upon entry into the United States. (R. at 6). This Court should reverse the Fourteenth Circuit Court of Appeals decision to deny the motion to suppress of Mr. Escanton's electronic devices. The forensic search conducted at the border on Mr. Escanton's electronic devices was a *highly intrusive* "non-routine search" and therefore reasonable suspicion was required.

The Supreme Court made clear in *Ramsey* that the Constitution restricts the border search exception "*subject to substantive limitations imposed by the Constitution." Ramsey*, 431 U.S. at 620. The Supreme Court has already recognized a category of "nonroutine" border searches that are constitutionally reasonable only if based on individualized suspicion. *Montoya de Hernandez*, 473 U.S. at 541 (1985).

This Court should reverse the Fourteenth Circuit Court of Appeals decision to deny the motion to suppress: three days of cell-site location information, one-hundred cumulative hours of cell-site location information over two weeks, and cell-site location information collected from cell tower dumps pursuant to 18 U.S.C. § 2703(d). Under *Carpenter*, Mr. Escaton's fourth amendment rights were violated because the government did not obtain a warrant to search the Cell Site Location Information ("CSLI") in which he had a reasonable expectation of privacy that was unaffected by the third-party doctrine. *Carpenter*, 585 U.S (2018).

CSLI present unique issues regarding privacy interests. They allow the government to ascertain the subscriber information and historical location for hundreds of cell phones without a warrant. This Court held that "an individual maintains a legitimate expectation of privacy, for fourth amendment purposes, in the record of his physical movements as captured through CSLI." *Carpenter*, 585 U.S. (2018). Therefore, Mr. Escaton can demonstrate a subjective expectation of privacy in his historical CSLI, which entitles it to fourth amendment protection.

The Fourth Amendment prohibits unreasonable searches and seizures. U.S. Const. amend. IV (Stored Communication Act*) This Court determined that 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." *Carpenter,* 585 U.S. (2018)**.** An application of the law as interpreted in *Carpenter,* to the facts of this case, suggests that law

enforcement violated Hector Escaton ("Petitioner")'s Fourth Amendment rights when it (1) obtained three types of cell-site location information (CSLI) records for Petitioner's cell phone number without a warrant supported by probable cause.

The mosaic theory considers whether a set of non-searches aggregated together amount to a search because their collection creates a "revealing" mosaic.[3] Law enforcement made two warrantless requests for CSLI of Petitioner's cell phone: the first included three days of CSLI, and the second added up to 100 hours over ten weekdays. In *Carpenter*, this Court held that an aggregation of surveillance records amounts to a "search." *Carpenter v. U.S.*, 585 U.S. (2018). The third-party doctrine is inapplicable to the facts here because Mr. Escaton never revealed his real-time location information to a third party. The third-party doctrine establishes that individuals have no expectation of privacy in information voluntarily conveyed to a third party. The courts in *Graham, Jones, Augustine,* have defined this as a volitional act wherein the subscriber acts use the phone to send or receive communication. Here, there are no facts to suggest that Petitioner's was in use during the relevant period. Therefore, the third-party doctrine does not apply. *Olmstead v. U.S.*, 277 U.S. 438 (1928*) United States v. Graham*, 824 F.3d 421 (4th Cir. 2016) *United States v. Jones*, 565 U.S. 400 (2012), *Commonwealth v. Augustine*, 467 Mass. at 258–259, 4 N.E.3d 846

STATEMENT OF THE CASE

On September 25, 2019, Hector Escaton ("Escaton"), a West Texas citizen and resident, returned to the United States from Mexico through a West Texas border checkpoint Customs and

[3] Christian Bennardo, *The Fourth Amendment, CSLI Tracking, and the Mosaic Theory*, 85 Fordham L. Rev. 2385 (2017). *http://ir.lawnet.fordham.edu/flr/vol85/iss5/42*

Border Protection ("CBP") Officer Ashley Stubbs ("Stubbs") conducted a routine border search of Escaton's vehicle and found three large suitcases in the back of Escaton's car. Through the search, Stubbs found an iphone, laptop, three external hard drives, and four USB devices. (R. at 2). The phone was returned to Escaton but the remaining electronic devices, including the laptop, hard drives, and USB deices. No passwords were needed to open the devices. Stubbs discovered that on the laptop, however, certain folders were password protected. Stubbs then inserted the USB devices in the computer and found that he could not access their contents. (R. at 3).

Stubbs delivered the electronics to Immigration and Customs Enforcement ("ICE") Senior Special Agent & Computer Forensic Examiner Theresa Cullen ("Cullen") who was stationed at the border checkpoint. She used forensic software to copy and scan the devices, which typically takes several hours. Cullen personally examined the results of the forensic program and found that the laptop held documents containing individuals' bank account numbers and pins. The forensic analysis also found that the USB devices contained traces of malware. Cullen found no incriminating information on the hard drives and those scans were deleted. Her findings were reported to Stubbs and the CBP immediately notified the Federal Bureau of Investigation (FBI), which had been investigating an "ATM skimming" of Mariposa Bank ATMS in Sweetwater during October of 2018. FBI Special Agent Catherine Hale began examining the connections between the forensic evidence provided by Stubbs and Cullen and that reported by Mariposa Bank. (R. at 3).

A local branch manager of Mariposa Bank had discovered ATM tampering on October 13, 2018 at the Boswell Street branch after a customer noticed that adjacent ATM's displayed different screens. An ATM engineer examined the Boswell ATM's and determined that the ATM had been cut open and infected with malware through its USB port. A Mariposa Bank internal

investigation revealed that skimming occurred at four additional Mariposa ATMs in Sweetwater and three in the neighboring city of Escalante. (R. at 3).

Agent Hale received information regarding the malware used and surveillance photographs near the three ATMs, all of which captured images of a man in a black sweatshirt. Using the forensic search information from CBP and the information provided from the banks, Agent Hale, in coordination with U.S. Attorney Elsie Hughes, requested three tower dumps from the cell sites near three Sweetwater ATMs pursuant to 18 U.S.C. § 2703(d) of the Stored Communications Act (SCA) for 30 minutes before and 30 minutes after the man in a black sweatshirt approached the ATMs. (R. at 4).

Stubbs reported Escaton's information, including his telephone number which had been found in Escaton's phone, and details to the FBI for potential bank fraud and identity theft claims. (R. at 5). The malware found on the USB devices, though not identical, was similar to the malware used at Mariposa ATMs in Sweetwater. The phone number also matched one of the numbers generated from the three tower dumps. Based on the foregoing, U.S. Attorney Hughes working with Agent Hale on the investigation applied for court orders under the SCA to obtain Escaton's cell phone records. A federal magistrate judge issued an order directing Delos Wireless-Escaton's wireless carrier-to disclose "cell site records corresponding to [the] telephone number…of Hector Escaton during the period October 11, 2018 through October 13, 2018" (Three-day Records). The records, however, did not place Escaton in neighboring Escalante from October 11-13.

Procedural History

Hector Escaton was convicted of bank fraud, 18 U.S.C. §1349, and aggravated identity theft, 18 U.S.C. §1028A. Appellant appealed his conviction with the Fourteenth Circuit Court of

Appeals on the grounds that the district court erred in denying his motion to suppress because the forensic search of his "devices" and CSLI requests violated his Fourth Amendment rights. The Fourteenth Circuit affirmed the District Court's ruling and denied Appellant's motion to suppress. Appellant filed a petition for writ of certiorari which was granted on November 22, 2022.

ARGUMENT

I. The Supreme Court Has Held That Reasonable Suspicion Is Not Required For Routine Border Searches But Has Not Established A Bright Line Rule For Non-Routine Border Searches of Electronic Devices

As there is no established precedent, the Fourteenth Circuit Court of Appeals determined that reasonable suspicion was not required for border agents to conduct a "non-routine search" on an individual's electronic devices upon entry into the United States. (R. at 6). The forensic search conducted at the border on Mr. Escanton's electronic devices was a *highly intrusive* "non-routine search" and therefore reasonable suspicion was required.

Routine Border Search

The border search exception permits warrantless and suspicionless, what are deemed as "routine", searches of individuals and items in their possession when crossing the U.S. border. *U.S. v. Montoya de Hernandez*, 473 U.S. 531 (1985). A routine border search is a search that does not pose a serious invasion of privacy or offend the average traveler. *United States v. Johnson*, 991 F.2d 1287, 1291 (7th Cir. 1993**)**. A routine search may consist of searching for contraband or weapons through a pat-down, *United States v. Beras*, 183 F.3d 22, 24 (1st Cir. 1999) (holding that a pat-down of an international traveler's legs was not intrusive enough to qualify as non-routine); the removal of outer garments, *United States v. Sandler*, 644 F.2d 1163, 1169 (5th Cir. 1981)**;** the use of drug-sniffing dogs, *United States v. Kelly*, 302 F.3d 291, 294-95

(5th Cir. 2002); examination of outbound materials, *United States v. Kolawole Odutayo*, 406 F.3d 386, 392 (5th Cir. 2005); and the inspection of luggage. *United States v. Okafor*, 285 F.3d 842 (9th Cir. 2002). A government agent does not need reasonable suspicion before conducting a "routine" search at the border as it has long been established that border crossers' reasonable expectation of privacy is lower at the border. Kim, supra at 1.

Customs Border Protection and Immigration officers' powers are limited to 8 U.S.C. §1357(c), 19 U.S.C. § 1496, 19 U.S.C. § 1582. Two statutory provisions confer border search powers on agents of the United States: 19 U.S.C. § 482 (customs official searches) and Immigration and Nationality Act (INA) § 287 (immigration officer searches). These statutes allow agents to conduct searches and arrests at the border without warrant or probable cause subject to constitutional constraints.

Non-Routine Border Search

Government officials may conduct certain "non-routine" searches at the border only if they have at least a "reasonable suspicion" that the searched individual is smuggling contraband or conducting other illegal activities. Kim, supra, at 1. "Reasonable suspicion" means an officer has a particularized and objective basis for suspecting the searched individual of wrongdoing. *Terry v. Ohio*, 392 U.S. 1, 21 (1968). Certain "non-routine" search procedures are perceived to intrude and have the potential to be embarrassing or destructive. In order to prevent their excessive use, courts have held that border agents must have at least a "reasonable suspicion" of wrongdoing before they may conduct destructive searches of inanimate objects, prolonged detentions, strip searches, body cavity searches, x-ray searches and the like. This court has not explicitly established the degree of suspicion required to justify a warrantless search of an electronic device (such as a laptop) at the border but found that reasonable suspicion was present

in the cases it reviewed to support the search before them**.** See *United States v. Touset*, 890 F.3d 1227 (2018); *United States v. Kolsuz*, 890 F.3d 133 (2018).

Only the Ninth Circuit in United States v. Arnold has explicitly held that reasonable suspicion is not needed to support a warrantless border search of laptops and other electronic devices. The Ninth Circuit first stated that warrantless "searches of closed containers and their contents can be conducted at the border without particularized suspicion under the Fourth Amendment. *United States v. Arnold*, 213 F.3d 894, 1007 (5th Cir. 2000). The Ninth Circuit refused to take into consideration any special qualities of laptops that may distinguish them from other containers, such as a laptop's capability of storing large amounts of privacy data. The Court treated border searches of laptops no differently from border searches of any other type of personal property. *Arnold*, 213 F.3d at 1009 (2000). The court adopted a categorical approach to warrantless border searches: so long as the search is of a physical object rather than a person's body, reasonable suspicion is not required if the search is not physically destructive or particularly offensive.

The incident at issue in the Arnold case occurred on July 17, 2005 and the Ninth Circuit's decision was released on April 21, 2008. This decision was rendered before the release of Apple's iPhone and iPad, when only 4% of adults in the United States were tablet owners compared to 45% in 2015. Gao, supra. The holding in *Arnold* and the electronic devices that were asked to be considered in that case are very different from the electronic devices prevalent today. Before the prominence of digital devices, border searches of personal property were "limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy." *Riley v. California*, 134 S.Ct. 2489 (2014). Yet the contents of electronic devices, such as laptops and cell phones, are different from that of other containers because of the

immense amount of information that is contained in cell phones and the reasonable expectation of privacy an individual maintains in them subsequent to a private search. *Riley*, 134 S.Ct. 2473; *United States v. Lichtenberger*, 786 F.3d 478 (6th Cir. 2015).

II. Reasonable Suspicion Is Required To Conduct a "Non-Routine" Forensic Search of an Individual's Electronic Devices At The Border

The *Riley* Court presented an analytical framework that complements the border search doctrine's traditional consideration of whether a search is "routine" or "non-routine." *Kolsuz*, 890 F.3d 133 (6th Cir. 2018). The Court explained that, in determining whether to apply an existing exception to the warrant and probable cause requirements to a "particular category of effects" such as cell phones, individual privacy interests must be balanced against legitimate governmental interests. *Riley*, 134 S. Ct. at 2484**.** The border search exception is intended to serve the narrow purposes of enforcing immigration and customs laws. *See Cotterman*, 709 F.3d at 956 (emphasizing the "narrow" scope of the border search exception). Therefore, the government's interests are analyzed by considering whether a search conducted without a warrant and probable cause is sufficiently "tethered" to the purposes underlying the exception. *Riley* at 2485.

On September 25, 2019, Mr. Escaton (a West Texas citizen and resident) returned to the United States from Mexico through a West Texas border checkpoint. Mr. Escanton was subjected to a "routine" border search of his vehicle. Through the search, a Customs and Border Protection Officer found an iPhone, a laptop, three external hard drives, and four USB devices. The Officer placed the iPhone on airplane mode and ensured the laptop was disconnected from wireless service and manually searched both devices without assistive technology. All actions by the Officer are analogous with a "routine" border search that does not pose a serious invasion o of privacy or offend the average traveler. *Johnson*, 991 F.2d (7th Cir. 1993**)**. The government

may "engage in suspicionless border searches where there is an interest unique to the border, such as preventing people from entering illegally or in intercepting drugs or weapons being brought into the country"; however, "these interests do not exist with regard to the memory of computers." [4]

The Officer proceeded to return the iPhone to Escanton but detained the remaining devices including the laptop, hard drives and USB devices. (R. at 3). There was no reason to detain the remaining devices. No passwords were needed to open the devices (R. at 3). No passwords were needed to open the devices. The Officer discovered that on the laptop, however, certain folders were password protected and after inserting the USB devices in the computer found that he could not access their contents (R. at 3). The fact that the Officer could not access certain folders or what was on the USB devices is not anything particularly suspicious or interesting. Yet, the Officer proceeded to deliver the electronics to Immigration and Customs Enforcement (ICE) to conduct a forensic examination. (R. at 3).

The purpose of the border exception should not be expanded to justify purely information searches, beyond identification of the individual seeking entry because the government's interest in searching data and information is lower, and there is no greater need to search computers at the border than anywhere else already in the United States. The government may "engage in suspicionless border searches where there is an interest unique to the border," which is absent in this case. *Supra*. The border should not be a place where the government has a good excuse to rummage around in people's stuff in hopes of finding anything that violates any kind of law without being subject to traditional Fourth Amendment requirements. The government's interest

[4] Erwin Chemerinsky, Laptop Search at Border Was Illegal, L.A. Daily J. Nov 29, 2006 at 6

in searching the files on a laptop at the border is lower because the same data contained within every laptop can float across the border via the internet; therefore, border searches aren't that effective in preventing "dangerous data" from entering the country. Because the distinction between routine and nonroutine searches turns on privacy and intrusiveness in order to require some level of suspicion, laptops must either be more like an extension of private body parts or a home. Instead courts have found it is more like a suitcase. The authority to search a laptop at the border should not depend on whether it is similar enough to a small list of things that judges consider to be sufficiently private at the border; it should turn on whether it is reasonable to search for information that has little to do with customs laws at the border. It was not reasonable for a "non-routine" search to be conducted on Mr. Escanton's laptop in the absence of reasonable suspicion.

At the time the CBP officers, conducted their forensic search on September 25, 2019, of Mr. Escanton's electronic devices, the Department of Homeland Security had already adopted a policy (as of January 4, 2018) that treats forensic searches of digital devices as nonroutine border searches, insofar as such searches now may be conducted only with reasonable suspicion of activity that violates the customs laws or in cases raising security concerns.[5] The adoption of these requirements by U.S. Customs and Border Protection suggests that the distinction between manual and forensic searches, *is* manageable, and that treating forensic phone searches as non-routine does not need to interfere with the agency's mission at the border. *Cotterman*, 709 F.3d at 967; *U.S. v. Saboonchi*, 990 F.Supp.2d at 570 (D.Md.2014).

[5] U.S. Customs and Border Prot., CBP Directive No. 3340-049A, *Border Search of Electronic Devices* 5 (2018).

The Supreme Court made clear in *Ramsey* that the Constitution restricts the border search exception "*subject to substantive limitations imposed by the Constitution." Ramsey*, 431 U.S. at 620. The Supreme Court has already recognized a category of "nonroutine" border searches that are constitutionally reasonable only if based on individualized suspicion. *Montoya de Hernandez,* 473 U.S. at 541**.** To allow "non-routine" border searches to be conducted absent reasonable suspicion is a clear violation of the Fourth Amendment and denies "the right of the people to be secure in their persons, houses, papers, and effects."

III. Escaton's Cell-Site Location Information

Law Enforcement requested, via court order, records of Escaton's historical Cell-Site Location Information ("CSLI") for (1) Ten days (< 100 hours), (2) Three-days (October 11-13, 2018), and (3) Cell Tower Dumps (30 min. before/after the skim). The court order was obtained utilizing The Stored Communications Act (SCA), a provision of the Electronic Communications Privacy Act, which allows law enforcement to obtain various types of non-content, cellular subscriber proprietary data. (Stored Communications Act, 18 U.S.C. §§ 2701-2712).

Cell Site Location Information (CSLI)

A cell phone's location can be detected through cell site location information ("CSLI") or global positioning system (GPS) data. CSLI refers to the information collected as a cell phone identifies its location to nearby cell towers. [6] CSLI from nearby cell towers can indicate a cell

[6] (Eric Lode, *Validity of Use of Cellular Telephone or Tower to Track Prospective, Real Time, or Historical Position of Possessor of Phone Under Fourth Amendment*, 92 A.L.R. Fed. 2d 1, *2 (2015).

phone's approximate location. [7] With information from multiple cell towers, a technique called "triangulation" is used to locate a cell phone with greater precision. [8]

The City of Sweetwater has many Delos Wireless cell towers, that are able to capture cell-site location information in five-to ten-minute increments within 50 feet of the location of a phone. There are many tall buildings within Sweetwater that block access to cell service, buildings have smaller towers that can locate individuals on a given floor or room of a building. Because of the density of the towers in Sweetwater, cell-site location information is often *more* accurate than global positioning system (GPS) location.

GPS v. CSLI: Public Expectation of Privacy Is Reasonable

The courts in *Carpenter* describe CSLI in comparison to global position system technology ("GPS") as, "tracking a person's past movements through CSLI partakes of many of the qualities of GPS monitoring considered in *Jones*—it is detailed, encyclopedic, and effortlessly compiled." *United States v. Jones*, 565 U.S. 400 (2012); *Carpenter v. U.S.* 138 S.Ct. at 2209 (2018). In fact, historical cell-site records may present greater privacy concerns than the GPS monitoring discussed in Jones: "They give the Government near perfect surveillance and allow it to travel back in time to retrace a person's whereabouts, subject only to the five-year retention policies of most wireless carriers." *Jones*, 565 U.S. 400 (2012).

In Carpenter, the government contends that CSLI data is less precise than GPS information, yet the data was deemed accurate enough, to highlight in its closing that the CSLI data placed Carpenter in proximity to the scene of the crime. The facts of the case at bar have differing aspects of the accuracy of the CSLI information. *Carpenter v. U.S.* 138 S.Ct. at 2209

[7] Jerry Grant, Cell Site Analysis (Live Demo) Federal Public Defender's Office Training Materials, 10 (Mar. 7, 2015)
[8] Grant, supra

(2018). The records placed Escanton in urban Sweetwater, "densely populated with cell towers," which allowed enforcement to achieve "near perfect surveillance, as if it had attached an ankle monitor to the phone's user." *Id.* at 2218. In Sweetwater, for example, the cell towers can place a person so exactly as to reveal what floor of what building they occupy. Many courts, having found that GPS tracking implicates the fourth Amendment, believe also that "CSLI implicates the same nature of privacy concerns as GPS tracking..." *Commonwealth v. Augustine*, 4 N.E.3d 846, 861 (Mass. 2014)

Here, Petitioner's cellular telephone number was used to place him at the scene of three bank fraud conspiracies and without having to even use the phone was linked to the Sweetwater bank in question. Once the initial weekend records failed to place Escaton at the scene for both crimes, law enforcement sought additional CSLI totaling nearly two weeks. The court should find that technology as exacting as this implicates one's expectation of privacy. "[C]itizens of this country largely expect the freedom to move about in relative anonymity without the government keeping an individualized, turn-by-turn itinerary of our comings and goings." [9]

In *Jones*, the government attached a wireless GPS device to the vehicle driven by Jones, who was suspected of drug trafficking out of a nightclub he owned. *Jones*, 565 U.S. 400 (2012). The issues considered were whether the use of the GPS tracking device constituted a "search" under the Fourth Amendment. The indicators which help to glean a determination in this case are whether (1) the space being occupied on Jones's vehicle constituted a physical trespass and consequently a "seizure" for Fourth Amendment purposes and (2) whether the length of the monitoring made the activity more invasive.

[9] Renée McDonald Hutchins, Tied Up in Knotts? GPS Technology and the Fourth Amendment, 55 UCLA L. Rev. 409, 455 (2007).

The crime took place one year before law enforcement made the request for the Three-day Records or Weekday Records. In Carpenter, the Court considered with unease "the retrospective quality of the data" which allowed law enforcement to access "information otherwise unknowable." *Carpenter*, 585 U.S (2018). In the same way that people expect their cars will not be tracked, they expect even less that their personal phones will be tracked—namely because Americans bring their phones with them everywhere.

Like GPS, CSLI Can Follow You Home

Cell phones have largely replaced "home" phones, as a recent survey found 31.6% percent of American households are "wireless only," meaning no landline telephone service inside the home.[10] Cell users treat their cell phones as a body appendage, it follows them everywhere. Unlike GPS monitoring of a vehicle, CSLI is generated constantly without regard for the location of the user, the examination of historical CSLI can permit the government to "track a person's movements between public and private spaces, impacting one's interests in both the privacy of their movements and the privacy in their home." *Tracey v. State,* 152 So.3d 504 at 524 (Fla. 2014)

In Jones, this Court established that when government agents engage in "tracking of an individual" or "where the tracking reveals information about a private space which otherwise might not be revealed," that constitutes a search in violation of the fourth amendment. *United States v. Jones,* 132 S.Ct. 945 (2012). "Owners of…smartphones do not contemplate that these devices will be used to enable covert surveillance of their movements." *Id at 947.* In *Karo*, the government's warrantless GPS monitoring of an individual in a private residence, was an

[10] Womble Bond Dickinson (US) LLP *Supreme Court: Warrant Now Required to Obtain Historical Cell Site Location Information | Lexology*. (2019). *Lexology.com*. Retrieved 10 February 2019, from https://www.lexology.com/library/detail.aspx?g=b8c989d6-83d5-4a2e-9b63-64d0744b6ca7

unreasonable search violating the fourth amendment. *Karo at 714*. CSLI, like the GPS monitoring in *Karo*, can reveal to the government detailed information about constitutionally protected locations, where individuals enjoy the highest level of constitutional protection [that] the government [would otherwise be] prohibited from obtaining without a warrant. *Id at 714.*

CSLI Obtained via The Stored Communications Act (SCA) §§ 18 U.S.C. §2703(d)

The requests for CSLI, granted under the Stored Communications Act (SCA),' present a substantial threat to fundamental notions of privacy, as the statute's requirements to access these records fall short of those proscribed under the Fourth Amendment. A warrant is required unless the search qualifies under an exception to the warrant requirement *Riley*, at 2482 (2014). Requests under the SCA for CSLI promote warrantless searches of information with no judicial oversight, there are no limits to the amount of data included in each request or limits on the number of requests for data.

The inadequacy of these limitations on the accessibility of this information are apparent when visiting Verizon's "about" United States report which lists the frequency of law enforcement demands for customer data by year.[11] There is a significant disparity between the use of subpoenas, warrants and general orders (like those obtained through the SCA) by law enforcement to obtain CSLI data. This is likely due to the evidentiary requirements associated with obtaining a warrant versus that of a general order or subpoena. Allowing law enforcement to take advantage of the lower standard required by SCA of "specific and articulable facts" to obtain CSLI information undermines the integrity of police investigation and encourages fishing expeditions of CSLI data. Law enforcement officers are currently not required to 'exhaust,' traditional methods of investigation such as in person surveillance prior to resorting to more intrusive methods, such as

[11] See Appendix B

CSLI data. In 2013, a panel of the Fifth Circuit reviewed a district court's decision that the "SCA violates the Fourth Amendment because the Act allows the United States to obtain a court order compelling a cell phone company to disclose historical cell site records merely based on a showing of `specific and articulable facts,' rather than probable cause." [12]

In *Carpenter,* law enforcement procured over 121-days' worth of CSLI along with a Tower Dump and sought records from two separate providers by utilizing the general order requirement under the SCA. *Carpenter*, 585 U.S. (2018). A line was drawn, narrowly for purposes of the *Carpenter* case at the 7-day request, but the Court declined to offer any universal or even alternative application to address this issue. *Supra.* Even if in *Carpenter*, the Court had provided a "bright-line restriction", a universal rule, to a permissible amount of days or hours of CSLI data that could be contained by law enforcement under the SCA, there would still be insufficient judicial oversight to mitigate the voluminous requests or limit the number of requests submitted by each agency. *Supra.*

***i.* Three Day Records**

Two possible analyses of the three-day record are appropriate, here. The first is an analysis under Katz theory of reasonable expectation of privacy in the home. Under "Mosaic" theory, as espoused by Justice Breyer in Jones, the three-day records, having satisfied the limitation of six days under the Carter standard would likely not constitute a search whether they were weekend days or otherwise. However, if we analyze the three-day weekend record requests and the weekday records in the aggregate, it provides a complete picture if an individual's life.

[12] In re U.S. for Historical Cell Site Data, 724 F.3d 600, 605-606 (5th Cir.2013) (citations omitted).

Law Enforcement requested a set of records for the dates of October 11 – October 13, 2018, which were the following days of the week: Thursday – Saturday. The Government asserted that the records do not implicate Escaton's penumbra rights because the records encompassed three "weekend days," and satisfied an erroneously-assumed bright-line rule extracted from *Carpenter*. On the contrary, courts have held that "Three-day Records still provide an intimate view," on an individual's life and as such are worthy of fourth amendment protection. *Carpenter*, 585 U.S. (2018).

Although the records do not exceed the limits established by *Carpenter*, the use of *Carpenter* as a gauge is inappropriate. It specified that the circumstances in that case was determinative only in that instance and did not extend its reasoning as any type of bright line standard to be adopted. One court has drawn a line in the context of historical cell site location records, and it has concluded (as a matter of state constitutional law) that anything more than six hours is "long term" and therefore constitutes a search. *Commonwealth v. Estabrook*, 38 N.E.3d 231, 237 (Mass. 2015). The court in *Estabrook* noted that "the salient consideration" for "reasonable expectation of privacy," is the "length of time for which a person's CSLI is requested," rather than the time covered by the person's CSLI. *Supra.* Thus, the actions of law enforcement and the size of their initial request (or multiple requests) must be considered. This standard and reasoning should be applied here.

In *Skinner*, the defendant voluntarily used a phone while traveling on public thoroughfares, allowing police to track that signal over *three-day period* because that same information could have been obtained through visual surveillance. *United States v. Skinner,* 690 F.3d 772 (6th Cir. 2012). The court noted that privacy should be assessed by "looking at what the defendant is disclosing to the public," rather than what is known to the police. Here, there is no

evidence to show that Mr. Escaton made any outward manifestations or actions which, had the government been following him, would have alerted them to his presence or actions. As such, under this standard, his CSLI should have been protected.

***ii.* 100 Cumulative Hours of CSLI Records Over Two Weeks**

The Fourteenth Circuit relies on the Supreme Court's holding in *Carpenter* that law enforcement conducts a "search" under the Fourth Amendment when the government obtains seven days of historical cell-site records to create a detailed account of the user's past movements (R. at 10). However, the Court declined to say whether there was a "limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny," and decided only that accessing seven days or more worth of information was enough (R. at 11). The Fourteenth Circuit has mistakenly perceived the determination of the Supreme Court that seven days of CSLI data constitutes a search, as equating to that anything less than seven days of CSLI data may not be a search and therefore may not require a warrant. The Supreme Court admonishes in its holding in *Carpenter* that its decision is "narrow." *Carpenter*, 585 U.S (2018). In the dissenting opinion of Justice Kennedy, Thomas and Alito, they address that the Court has suggested that less than seven days of location information may not require a warrant without explaining why that is. *Carpenter*, 585 U.S (2018). It is this concern that manifests itself in the Fourteenth Circuit's holding in this case as it concludes that "the Court determined that it was the accumulation of seven days of records that violated a person's expectation of privacy." (R. at 12).

The Fourteenth Circuit even goes as far to assume that seven days is interchangeable with 168 hours total hours of historical cell-site records and because only 100 hours was requested of Escanton's cell site records it does not per se violate the holding in Carpenter. The Supreme Court never stated that seven days was analogous to 168 hours and that anything less than that was not a

search requiring a warrant. (R. at 11, see footnote 14). The Supreme Court could have further clarified their determination that seven days constitutes a fourth amendment search requiring a warrant (and anything less than seven days does not) but instead they state that the Government will generally need a warrant. The Fourteenth Circuit's reliance on the "narrow" holding by the Supreme Court in Carpenter, as a bright line determination for future cases as to the specific number of days or hours that require a warrant is an attenuation of the rationale provided by the Supreme Court in their conclusion of what constitutes a search as it pertains to CSLI data.

***iii.* Cell Tower Dumps**

A Cell Tower Dump ("Tower Dump") is a police request for all phone numbers that are connected to a specific cell tower within a specified range of time. Although there are no statutory provisions specifying how law enforcement may obtain "tower dump" information, most requests are lodged in the same manner as requests for CSLI—via subpoena under the SCA. Cell tower dumps have not been widely addressed by state and federal courts. Instead they are often loosely categorized under the umbrella of CSLI. However, case law suggests that the use of Tower Dumps has become a relatively "routine investigative technique," for law enforcement officials. [13]

This court, in Carpenter, specifically declined to express a view on Tower Dumps, saying "We do not express a view on matters not before us: real-time CSLI or 'tower dumps."[14] Decisions concerning whether a law enforcement officer must obtain a warrant to access these

[13] Jeffrey Brown, What Type of Process is Required for a Cell Tower Dump?, CYBERCRIME REV. (May 16, 2012), http://www.cybercrimereview.com/2012/05/what-type-of-process-isrequired-for.html

[14] Supreme Court Says Warrants Needed for Historical Cell-Site Location Data | Wolters Kluwer Legal & Regulatory (2019). Retrieved 10 February 2019, from *https://lrus.wolterskluwer.com/news/tr-daily/supreme-court-says-warrants-needed-for-historical-cell-site-location-data/54526/*

types of data remain unanswered at this time." *Carpenter*, 585 U.S (2018). This Court did determine that the information provided from a "tower dump" does not reveal detailed information about a person's location, except as it relates to that specific cell tower. *Id at 2211.* This Court compared the records obtained from "tower dumps" as being similar to red light cameras or "E-Z pass monitors," for which, there is no probable cause standard required to obtain those records. See *Id* at 2221.

Respondent errs, however, in the assertion that tower dumps contain only non-personal information. According to Brian Owsley, a former judge and current law professor at Texas Tech University of Law, police can use tower dumps to collect not only direct personally identifiable information, name; address; telephone call records, including times and durations; lengths and types of services; subscriber number or identity, means and source of payment, including bank account number or credit card number; date of birth; social security number; and driver's license number. [15] Because a tower dump does not reveal more than a location and a cell number, we see no need to add an increased level of scrutiny for an effective and useful police tool.

IV. Expectation of Privacy

Chief Justice Roberts stated in *Carpenter*, that CSLI gives "the ability to chronicle a person's past movements through the record of his cell phone signals" and that "historical cell-site records present *even greater privacy concerns* than the GPS monitoring of a vehicle we considered in Jones. While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time." *Carpenter*, 585 U.S (2018) [*emphasis added*].

[15] Owsley, Brian, The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in its Electronic Surveillance (2013). University of Pennsylvania Journal of Constitutional Law, Vol. 16, 2013. Available at SSRN: *https://ssrn.com/abstract=2307525*

Application of the Fourth Amendment under a privacy theory depends on whether the person invoking its protection can claim a reasonable, or a legitimate, expectation of privacy that has been invaded by government action. *Ford v. State,* 477 S.W.3d 321, 334-35. Historical CSLI allows the government to "monitor and track our cell phones, and thus ourselves, with minimal expenditure of funds and manpower, [which] is just the type [of] gradual and silent encroachment into the very detail of our lives that we as society must be vigilant to prevent." *Tracey v. State*, 152 So.3d 504 at 524 (Fla. 2014). A search occurs when a government actor violates a person's reasonable expectation of privacy. In Tracey v. State, the Florida Supreme Court held that CSLI implicates both a "subjective expectation of privacy and one that society is now prepared to recognize as objectively reasonable." *Id.* "The privacy interests affected by long-term GPS monitoring … apply with equal or greater force to historical CSLI for an extended time period." *Commonwealth v. Augustine*, 4 N.E.3d 846, 861 (Mass. 2014)

Justice Sotomayor suggested that most Americans hold "a reasonable societal expectation" that the "sum of one's public movements" will not be "recorded and aggregated" in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits." *Carpenter v. U.S.* 138 S. Ct. 2206 At 2209 (2018). "Given the unique nature of cellphone location information, the fact that the government obtained the information from a third party does not overcome *Carpenter's* claim to Fourth Amendment protection," Justice Roberts wrote. *Id.* A panel of five justices in *Jones,* held that "conducting GPS tracking of a cell phone would raise privacy concerns." Further, they stated that because the government monitored their every move, tracking to that degree would "impinge[] on expectations of privacy" even though, Jones has disclosed his movements to the public by traveling on public highways. *U.S. v. Jones 132 S. Ct. 947 (2012)*

V. The Third-Party Doctrine Does Not Apply

The "Third Party Doctrine" states that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979). The Third-Party Doctrine concerns whether an individual has (1) a legitimate privacy interest in documents held by a third party, and (2) whether the information was voluntarily relayed to the third party, thus undermining any privacy interests established in (1).

In *Smith*, where defendant's telephone became automated and he used the telephone to make threatening phone calls, the court found no expectation of privacy in numbers dialed even absent a live operator. *Smith*, 442 U.S. 744–45 (1979). The court likened the role of the Cell Service Provider ("CSP") to that of an operator when using rotary telephones. The individual making the call is aware of the presence of a third-party intermediary who physically dials the requested numbers which are thus not confidential: "We are not inclined to hold that a different constitutional result is required because the telephone company has decided to automate." *Knotts*, 460 U.S. at 283. Now that telecommunication technology has advanced, the argument has been made that the CSP replaces the 'operator,' so individuals may not be immediately cognizant that their desired connection is still being 'routed' through a third party for purposes of making the connection. Yet, on some level, there exists an unspoken awareness and agreement that the numbers and even the messages being transmitted are parsed through the hands of a third party and therefore, one can have no reasonable expectation of privacy.

Escaton Did Not "Voluntarily Convey" CSLI to Providers

The Government contends that because Escanton chose to utilize a cellular phone network, which is required for use of the phone, that he somehow voluntarily also relinquished any interests he may have held in the location information generated by the phone. Also, that an individual

voluntarily conveys location information to telephone companies in the course of making and receiving calls on their cell phone. *US v Davis*, 785 F.3d 498 at 512 (2015). Like the numbers dialed and logged via pen register in *Smith*, Defendants had no reasonable expectation of privacy in the CSLI generated as a by-product of this activity. *Smith*, 442 U.S. 744–45 (1979).

Most cell phone users no longer even dial numbers but instead, utilize speed dial or pre-programmed 'contacts' lists. Thus, the courts in *Augustine* reasoned that, "cell phone users do not knowingly—let alone voluntarily—transmit location data to cell providers." *Augustine*, 4 N.E.3d 846, 861 (Mass. 2014). Further, a California court reasoned, passive recipients of calls and texts by individuals does not constitute a voluntary conveyance." [16] Customers are likely unaware because CLSI is "transmitted automatically during the registration process, entirely independent of the user's input, control, or knowledge." [17] The courts in Bynum, similarly, held that "third-party information relating to the sending and routing of electronic communications does not receive Fourth Amendment protection." *United States v. Bynum,* 604 F.3d 161, 164 (4th Cir 2010). The courts in Carpenter, reasoned that "Given the unique nature of cellphone location information, fact that the government obtained the information from a third party does not overcome Carpenter's claim to Fourth Amendment protection," *Carpenter,* 585 U.S. (2018).

When powered on, a cell phone continually searches for a cell tower signal while autonomously running applications in the background. With every connection, a time-stamped record is created. Most CSLI is "generated by passive activities such as automatic pinging, continuously running applications ("apps"), and the receipt of calls and text messages." Although

[16] In re: Application for Telephone Information Needed for a Criminal Investigation. 2015 N.D. Cal. Opinion, 119 F. Supp. 3d at 1029.
[17] In Re Application for Pen Register and Trap/Trace, 396 F. Supp.2d at 756 (S.D. Tex. 2005).

CSLI is generated through active use of the phone, much of it is also generated, "with far less intent, awareness, or affirmative conduct on the part of the user." [18] Such passive, unknowing generation of CSLI does not amount to a "voluntary conveyance" under the third-party doctrine. *Id*.; see also *Davis*, 785 F.3d at 534 (Martin, J., dissenting); *Tracey*, 152 So. 3d at 525–26.

Neither Conveyance, Nor Ownership Determine Privacy Interests

The Supreme Court "has twice held that individuals have no Fourth Amendment interests in business records which are possessed, owned, and controlled by a third party." *Carpenter,* 585 U.S. (2018). The Government contends that no search has occurred because an individual has no reasonable expectation of privacy in the records held by a third party and that the records *belong* to that third party. The presumption that a party may not have a privacy interest in records held by another is erroneous. The Government relies on the property-based framework, that an individual has interest in property that they control.

The third-party doctrine has analogized the concept of telephone communications with that of sending a letter. The sender knows that the parcel or correspondence is being placed in the care of a third party and so it is "held" by a third party. However, mail tampering and mail fraud penalties are quite severe, as our history aims to protect one's privacy interest in "papers, and effects…' U.S. CONST. amend. IV. An objective expectation of privacy is "one that society is prepared to recognize as reasonable." *United States v. Jacobsen,* 466 U.S. 109 at 117 (1984).

One may have privacy and confidentiality rights in records held by another. Some cases even assert that the property-based framework with which we've grown accustomed is ill-fitted to the technological advances at issue. Justice Kennedy opined in Jones, that *Katz* moved beyond

[18] In re: Application for Telephone Information Needed for a Criminal Investigation. 2015 N.D. Cal. Opinion, 119 F. Supp. 3d at 1029.

the "property-based concepts," which are, by no means, "fundamental" or "dispositive" in determining which expectations of privacy are legitimate. He went on to emphasize that "privacy interests do not rise and fall with property rights. *Jones*, 565 U.S. 400 (2012)

The Mosaic Theory

The Government's request for "three-day" weekend records in this case increased the likelihood of tracking a subject while they occupy a protected space, such as their home. In *Carpenter*, the court alluded to the mosaic theory when it asserted that, "the Government could, in combination with other information, deduce a detailed log of Carpenter's movements, including when he was at the site," of the crime, hereby acknowledging in its analysis not only the contemplation of the duration of captured data but the *aggregation*. *Carpenter*, 585 U.S. (2018). Under the mosaic theory, when weekend records are added to weekday records, a cumulative scan of over ten days would provide a perfect window into what a full week of life is like for Mr. Escaton, and that information should be protected.

Motion to Suppress Evidence: Defendant's Rights vs Officer's Good Faith

However, despite this conclusion, the court further held that the records needn't be suppressed because the government acted in good faith under the Stored Communications Act, triggering the good faith exception to the exclusionary rule. The Fourth Circuit parted from the Third Circuit by concluding that the Act gives the government the option to get intermediate orders instead of warrants for cell tower data from providers. Thus, Graham will not get a reversal, but future defendants may have better luck, as the court wrote in a footnote that their decision means the government "may no longer rely" on the Act to justify a failure to procure a warrant.

In *Wheeler* and *US v Daniels* (7th circuit appeals) The courts declined to take up a Fourth Amendment issue because the other courts were split on the decision. In Daniels the current argued both be good faith exception to the exclusionary rule and that the Defendant said failed to preserve the exclusionary issue on appeal, so it was not addressed. Circuit Judge Jones reasoned that "most federal judges" likely had decided against fourth Amendment protection of cell site data and mandated denial of the suppression motion saying, "We have yet to address whether cell-tower information that telecommunication carriers collect is protected by the Fourth Amendment." The courts failure however, to rule and establish a bright line Jeopardizes constitutional freedoms. This court had advised the lower courts to address the merits of Fourth Amendment claims when necessary to guide future options by law enforcement and other magistrates.

CONCLUSION

Petitioner Hector Escaton respectfully requests this Court to reverse a decision of the Court of Appeals for the Fourteenth Circuit, which erred when it denied Petitioner's motion to suppress of his electronic devices.

The Fourteenth Circuit Court of Appeals determined that reasonable suspicion was not required for border agents to conduct a "non-routine search" on an individual's electronic devices upon entry into the United States. (R. at 6). This Court should reverse the Fourteenth Circuit Court of Appeals decision to deny the motion to suppress of Mr. Escanton's electronic devices. The forensic search conducted at the border on Mr. Escanton's electronic devices was a *highly intrusive* "non-routine search" and therefore reasonable suspicion was required. Petitioner Hector Escaton respectfully requests this Court to reverse a decision of the Court of Appeals for the Fourteenth Circuit, which erred when it denied Petitioner's motion to suppress the evidence obtained from his electronic devices. The Fourteenth Circuit Court of Appeals

determined that reasonable suspicion was not required for border agents to conduct a "non-routine search" on an individual's electronic devices upon entry into the United States. (R. at 6). The forensic search conducted at the border on Mr. Escanton's electronic devices was a *highly intrusive* "non-routine search" that required reasonable suspicion. The utilization of this evidence in Mr. Escanton's criminal proceedings should be excluded.

Further, Petitioner respectfully requests that this Court also reverse the Fourteenth Circuit Court of Appeals decision to deny the motion to suppress: three days of cell-site location information, one-hundred cumulative hours of cell-site location information over two weeks, and cell-site location information collected from cell tower dumps pursuant to 18 U.S.C. § 2703(d). This Court held that "an individual maintains a legitimate expectation of privacy, for fourth amendment purposes, in the record of his physical movements as captured through CSLI." *Carpenter*, 585 U.S. (2018). This Court determined that 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." *Carpenter,* 585 U.S. (2018)**.** The third-party doctrine is not applicable as Mr. Escanton can demonstrate a subjective expectation of privacy in his historical CSLI, which entitles it to fourth amendment protection. To allow privacy rights to be infringed upon a standard less than probable cause, regardless of the duration hearkens to the dangers John Adams fought to protect against with the drafting of the constitution.

Dated: February 10, 2018 Respectfully submitted,

Attorneys for Petitioner

APPENDIX A

UNITED STATES CONSTITUTION, AMENDMENT IV

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.

CONSTITUTIONAL PROVISIONS AND RULES

The Fourth Amendment of the United States Constitution guarantees "[t]he 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.

THE STORED COMMUNICATIONS ACT, 18 U.S.C. § 2703

The Stored Communications Act, 18 U.S.C. § 2703, provides in relevant part:

(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—

(a) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; [or]

(b) obtains a court order for such disclosure under subsection (d) of this section;

(d) Requirements for court order.– A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.

SEARCH OF VEHICLES AND PERSONS, 19 U.S.C. § 482

(a) Any of the officers or *persons* authorized to board or search *vessels* may stop, search, and examine, as well without as within their respective districts, any *vehicle*, beast, or *person,* on which or whom he or they shall suspect there is *merchandise* which is subject to duty, or shall have been introduced into the *United States* in any manner contrary to law, whether by the *person* in possession or charge, or by, in, or upon such *vehicle* or beast, or otherwise, and to search any trunk or envelope, wherever found, in which he may have a reasonable cause to suspect there is *merchandise* which was imported contrary to law; and if any such officer or other *person* so authorized shall find any *merchandise* on or about any such *vehicle,* beast, or *person,* or in any such trunk or envelope, which he shall have reasonable cause to believe is subject to duty, or to have been unlawfully introduced into the *United States*, whether by the *person* in possession or charge, or by, in, or upon such *vehicle,* beast, or otherwise, he shall seize and secure the same for trial.

(b) Any officer or employee of the *United States* conducting a search of a *person* pursuant to subsection (a) shall not be held liable for any civil damages as a result of such search if the officer or employee performed the search in good faith and used reasonable means while effectuating such search.

POWERS OF IMMIGRATION OFFICERS AND EMPLOYEES, 8 U.S.C. §1357

(c) Search Without Warrant

Any officer or employee of the *Service* authorized and designated under regulations prescribed by the *Attorney General*, whether individually or as one of a class, shall have power to conduct a search, without warrant, of the person, and of the personal effects in the possession of any person seeking admission to the *United States,* concerning whom such officer or employee may have reasonable cause to suspect that grounds exist for denial of admission to the *United States* under this chapter which would be disclosed by such search.

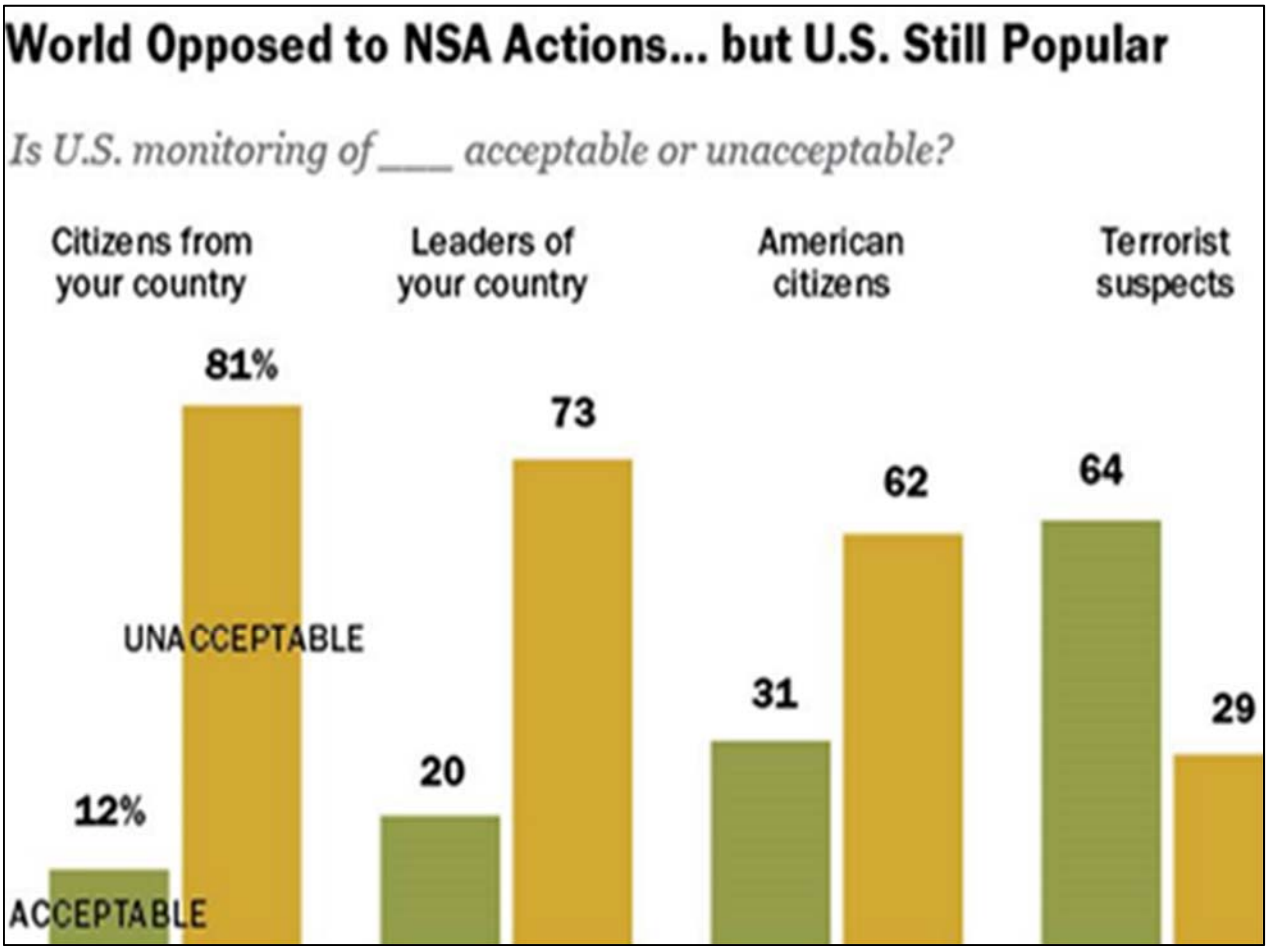
EXAMINATION OF BAGGAGE, 19 U.S.C. §1496

The appropriate *customs officer* may cause an examination to be made of the baggage of any *person* arriving in the *United States* in order to ascertain what articles re contained therein and whether subject to duty, free of duty, or prohibited notwithstanding a declaration and *entry* therefor has been made.

SEARCH OF PERSONS AND BAGGAGE; REGULATIONS, 19 U.S.C. §1582

The *Secretary* of the Treasury may prescribe regulations for the search of *persons* and baggage and he is authorized to employ female inspectors for the examination and search of *persons* of their own sex; and all *persons* coming into the *United States* from foreign countries shall be liable to detention and search by authorized officers or agents of the Government under such regulations.

APPENDIX B


World Opposed to NSA Actions... but U.S. Still Popular
Is U.S. monitoring of ____ acceptable or unacceptable?
Citizens from your country
Leaders of your country
American citizens
Terrorist suspects
81%
73
62
64
UNACCEPTABLE
31
29
20
12%
ACCEPTABLE