DOCKET NO. 10-1011

IN THE

Supreme Court of The United States

HECTOR ESCATON,

PETITIONER,

V.

UNITED STATE OF AMERICA,

RESPONDENT.

ON WRIT OF CERTIORARI FROM THE UNITED STATES COURT OF APPEALS,
FOURTEENTH CIRCUIT

BRIEF FOR PETITIONER

COUNSEL FOR PETITIONER
FEBRUARY 10, 2019

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Secondary Sources

Codes and Statutes

QUESTIONS PRESENTED

I. The Fourth Amendment prohibits the Government from conducting nonroutine searches of electronic devices on the border when it lacks reasonable suspicion. Hector Escaton was subject to a comprehensive forensic search of his computer, hard drives, and USB devices, when the CBP had no reason to suspect him. Did the forensic search of these devices violate the Fourth Amendment when it was not preceded by suspicion?

II. Under *Carpenter v. United States*, Government acquisitions of CSLI under 18 U.S.C. § 2703(d) must be supported by a warrant to satisfy the Fourth Amendment. The Government acquired three days of Escaton's CSLI, one-hundred cumulative hours of CSLI over two weeks, and CSLI collected from tower dumps. Did the Government violate Escaton's Fourth Amendment right to privacy when it acquired this information without a warrant?

OPINIONS BELOW

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

CONSTITUTIONAL PROVISIONS AND RULES

The Fourth Amendment to the United States Constitution provides:

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

U.S. Const. amend. IV.

INTRODUCTION

Petitioner, Hector Escaton, Appellant 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 reverse the Fourteenth Circuit's decision below.

Summary of the Argument

The case at bar presents two important issues involving the application of the Fourth Amendment to the United States Constitution. This Court should reverse the circuit court's decision because Government agents violated Escaton's Fourth Amendment rights in two distinct instances. Both the suspicionless search of Escaton's electronic devices at the border and the Government's subsequent S.C.A. §2703(d) requests for his cell site location information were unreasonable and unwarranted under the Constitution.

When the Government subjected Escaton's personal computer, hard drives, and USB devices to forensic searches at the border, it did so with no suspicion of illegal activity. In this case, Escaton complied in every way with Government agents' basic search of his vehicle and luggage as he crossed the Mexican border. While Escaton was on notice of such a typical, routine search, he was not on notice that his electronic devices would be scanned, copied, and analyzed by the Government's powerful forensic software in order to break into his password-protected folders. Here, the Government's arbitrary and unjustified use of nonroutine search technology on Escaton's devices violated his Fourth Amendment rights.

The border is not a Constitution-free zone. It is well established by this Court that reasonableness is the touchstone analysis for all searches and seizures conducted by Government officials, both on the border and in the interior. Here, Escaton's Constitutional right to be secure in his papers and effects is not abrogated, but must be balanced with the Government's legitimate

interests. Indeed, Escaton's privacy interest was elevated because information contained in electronic devices is so personal, sensitive, and comprehensive, that the Government must show reasonable suspicion to justify accessing it. Therefore, the circuit court inappropriately held that Escaton had no real privacy interest at the border. Accordingly, their ruling that no reasonable suspicion is required for property at the border is in clear error.

The Government again trespassed Escaton's Fourth Amendment rights when it accessed his cell site location information (CSLI) in violation of this Court's binding precedent. In a recent landmark case, this Court unequivocally held that individuals have a legitimate expectation of privacy in their location information as collected by cell towers and service providers. Because this privacy interest is now protected by the Fourth Amendment, the Government must get a warrant before requesting it, otherwise its request is invalid.

It is clear that the circuit court critically misapplied the CSLI warrant requirement laid out in *Carpenter v. United States* when it found Escaton had no expectation of privacy in his location information. Here, the Government impermissibly made a tower dump request, followed by two separate CSLI requests, without warrant or probable cause. After *Carpenter*, Escaton should have been secure in the whole of his movements. Hence, the Government should never have obtained three tower dumps establishing Escaton's location, and over one-hundred-and-fifty hours of his minute-to-minute movements because this gave the Government an intimate window into his private life. Subsequently, the Government used these progressively more invasive requests to build a case against Escaton implicating him in a year-old bank fraud event.

In both instances, Government agents overstepped their authority without justification. Government agents repeatedly ignored Escaton's right to privacy under the Fourth Amendment, and deliberately tried to circumvent this Court's binding precedent. In light of recent

technological developments, this Court should continue in the steps of *Carpenter* to protect individual's privacy rights against a "too permeating police surveillance."

For the reasons explained in detail below, the Petitioner respectfully asks the Court to reverse the Fourteenth Circuit decision.

Standard of Review

This Court deems questions of law reviewable under a de novo standard. *Ornelas v. United States*, 517 U.S. 690, 697 (1996). Both issues on appeal turn on questions of law, therefore, this Court should review them de novo.

STATEMENT OF THE CASE

Statement of Facts

On September 25, 2019, Hector Escaton, a United States citizen, was on his way home to his residence in West Texas when he entered a customs checkpoint located on the border between Mexico and West Texas. (R. at 2). Customs and Border Patrol (CBP) subjected Escaton to a routine border stop and a routine search and identified a variety of Escaton's personal electronic devices. (R. at 2). CBP officer Ashley Stubbs found that Escaton was carrying an iPhone and transporting, his personal laptop, three external hard drives, and four standard USB devices. (R. at 2). Officer Stubbs placed Escaton's iPhone in airplane mode and disconnected his laptop from wireless service before conducting a routine manual search, without assistive technology, of all his electronic devices. (R. at 2-3).

Finding both the iPhone and laptop accessible without a password, Officer Stubbs manually searched Escaton's iPhone, recorded its telephone number, and returned it to him. (R. at 2-3). Officer Stubbs' initial examination of Escaton's laptop revealed a paper note attached

beneath the keyboard. (R. at 2). Searching through the laptop's contents, Officer Stubbs discovered some individual files that were password protected. (R. at 3). Officer Stubbs recorded the contents of the paper note which contained a first name, telephone number, and some dollar symbols. (R. at 2). Officer Stubbs could not access the contents of the USB devices and the record does not reflect whether he attempted to access Escaton's hard drives. (R. at 3).

After completing the routine search, Officer Stubbs retained possession of Escaton's laptop, hard drives, and USB devices and delivered them to Immigration and Customs Enforcement (ICE) Senior Special Agent & Computer Forensic Examiner Theresa Cullen. (R. at 3). Agent Cullen used forensic software to scan and copy all the digital contents and metadata available on Escaton's personal electronic devices. (R. at 3). This process ordinarily requires access to the devices for several hours. (R. at 3).

Agent Cullen personally examined the forensic results from Escaton's laptop, USB devices, and hard drives. (R. at 3). Through the assistance of the forensic program, Agent Cullen found that the laptop held documents containing individuals' bank account numbers and pins and the USB devices contained traces of malware. (R. at 3). After examining the contents of Escaton's hard drives, Agent Cullen deleted their scans because she did not find any incriminating information on them. (R. at 3). Agent Cullen reported the results of her forensic search to Officer Stubbs who immediately transmitted the results of both the routine search and the forensic search to the Federal Bureau of Investigation (FBI). (R. at 3).

FBI Special Agent Catherine Hale examined the connection between the search results and an investigation of "ATM skimming" from the previous year. (R. at 3). The FBI investigation initially uncovered evidence of several different ATM Skimming tactics used to either access currency or data from Mariposa Bank ATMs in the cities of Sweetwater and

neighboring Escalante during October 2018. (R. at 4). At that time, the FBI obtained surveillance photographs from several of the ATMs and identified a man in a black sweater near each ATM around the dates on which the bank manager suspected the ATMs were tampered with. (R. at 4). Relying on the forensic search information from CBP and the previous ATM investigation's findings, Agent Hale and U.S. Attorney Elsie Hughes promptly submitted a request under SCA § 2703(d) for three tower dumps of CSLI data. (R. at 4). Each tower was located near one of three affected ATMs in downtown Sweetwater. Pursuant to an order under SCA § 2703(d), the FBI received a cumulative hour of tower dump CSLI for each tower, 30 minutes before and after the surveillance photos showed the man in the black sweater near a proximate ATM. (R. at 4).

The FBI found Escaton's iPhone number in the tower dump records and used this connection to locate Escaton's physical presence in Sweetwater during early October 2018. (R. at 5). The tower dumps also provided the FBI with the exact date and time of Escaton's presence in Sweetwater. (R. at 4). Agent Hale also found that traces of malware on Escaton's USB devices were similar, but different, from malware used on several of the Mariposa ATMs. (R. at 5). Relying on these discovers, Agent Hale, together with U.S. Attorney Elsie Hughes, submitted a new SCA § 2703(d) request for the entire record of Escaton's personal CSLI generated from October 11, 2018 through October 13, 2018. (R. at 5). The cell towers in Sweetwater are so numerous that CSLI data collected there is accurate within fifty feet the user. (Hale Aff. ¶ 11.). A court order issued on November 10, 2019, compelled Escaton's wireless carrier to deliver three days (72 consecutive hours) of his historical CLSI to the FBI. (R. at 5). The FBI examined this record of Escaton's location data to discover his whereabouts on October 12, 2018, verifying that Escaton was in the area of a Sweetwater ATM on that day. (R. at 5).

The FBI found the three-day CSLI record insufficient to establish whether Escaton had traveled from Sweetwater to Escalante during early October 2018. (R. at 5). Attempting to place Escaton within proximity of the ATMs in Escalante, the government submitted a third SCA § 2703(d) request. (R. at 5). A magistrate judge granted the FBI's request for Escaton's CSLI generated between 8AM MDT and 6PM MDT on weekdays from October 1, 2018 through October 12, 2018 (100 cumulative hours over a ten-day period). (R. at 5). Receiving Escaton's CSLI for this new request, the FBI was able to establish Escaton's presence in Escalante in early October of 2018. (R. at 5). In total, the FBI obtained three hours of tower dump CSLI from three separate locations in Sweetwater and 152 hours over thirteen consecutive days of Escaton's personal CSLI records from October 2018. (R. at 5).

Procedural History

The government charged Escaton with committing Bank Fraud 18 U.S.C. § 1344, Conspiracy to Commit Bank Fraud, 18 U.S.C. § 1349, and Aggravated Identity Theft, 18 U.S.C. § 1028A. (R. at 6). Escaton filed a motion to suppress ("the Motion"), seeking to exclude both the evidence from a forensic border search of his electronic devices and the cell-cite data the FBI requested from Delos Wireless. (R. at 6). The District Court denied the Motion. (R. at 6). Escaton appealed. (R. at 2). A divided panel of the Fourteenth Circuit affirmed, finding that neither the forensic boarder search nor the requests for CSLI violated Escaton's Fourth Amendment rights. (R. at 14). This appeal followed.

ARGUMENT

The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. The primary purpose of this amendment "is to safeguard the privacy and security of individuals against arbitrary invasions by Government agents." *Camara v. Mun. Court of City & Cty. of San Francisco*, 387 U.S. 523, 528 (1967). It demands that "the usual inferences which reasonable men draw from evidence . . . . be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime." *Johnson v. United States*, 333 U.S. 10, 14 (1948). Although this Court originally measured Fourth Amendment violations on a theory of trespass and property rights, it has extended "Fourth Amendment protect[ion] [to] people," in addition to places, in order to protect "certain expectations of privacy." *Soldal v. Cook County*, 506 U.S. 56, 64 (1992); *Carpenter v. United States*, 138 S. Ct. 2206, 2213 (2018); *Katz v. United States*, 389 U.S. 347, 351(1967).

An individual has a reasonable expectation of privacy protected by the Fourth Amendment when he "seeks to preserve something as private," and his expectation of privacy is "one that society is prepared to recognize as reasonable." *Carpenter*, 138 S. Ct. at 2213 (quoting *Smith v. Maryland*, 442 U.S. 735, 740 (1979)). Any "official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause." *Carpenter*, 138 S. Ct. at 2213. By recognizing such expectations of privacy, the Court ensures that the Fourth Amendment achieves its historical purpose to secure "the privacies of life" against "arbitrary power," *Boyd v. United States*, 116 U.S. 616, 630 (1886), and "to place obstacles in the way of a too permeating police surveillance." *United States v. Di Re*, 332 U.S. 581, 595 (1948).

I. REASONABLE SUSPICION IS REQUIRED FOR FORENSIC SEARCHES OF ELECTRONIC DEVICES AT THE BORDER.

A. While routine border searches may be suspicionless, nonroutine border searches require individualized suspicion to be Constitutional.

"[A] warrantless search is *per se* unreasonable under the Fourth Amendment, unless one of 'a few specifically established and well-delineated exceptions' applies." *United States v. Wurie*, 728 F.3d 1, 3 (2013) (quoting *Arizona v. Gant*, 556 U.S. 332, 338 (2009)). Routine searches occurring at the border are one such exception, "grounded in the recognized right of the sovereign to control, subject to substantive limitations imposed by the Constitution, who and what may enter the country." *United States v. Ramsey*, 431 U.S. 606, 620 (1977).

As with searches in the interior, border searches must be "reasonable," and the Court must weigh "legitimate government interests" against "the degree to which [the search] intrudes upon an individual's privacy." *Riley v. California*, 134 S. Ct. 2473, 2484 (2014) (quoting *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999)). Although border searches "have been considered … 'reasonable' by the single fact that the person or item in question . . . entered into our country from the outside," *Ramsey*, 431 U.S. at 619, this warrant exception is not without limit. *Id.*at 620 (noting that border search is "subject to substantive limitations imposed by the Constitution"). Hence, the controlling analysis for determining the reasonableness of a search requires balancing the competing interests of the Government and the privacy interest of the individual. *United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985).

Congress has, since the beginning, "granted the Executive plenary authority to conduct *routine* searches and seizures at the border, without probable cause or a warrant, in order to regulate the collection of duties and to prevent the introduction of contraband into this country." *Id*. (emphasis added) (citing *Ramsey*, 431 U.S. at 616-617 (citing Act of July 31, 1789, ch. 5, 1 Stat. 29)). To this day, Congress maintains that this 'plenary authority' is bound by individualized suspicion, allowing customs officers to "stop, search, and examine . . . any vehicle, beast, or person, *on which or whom . . . 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." 19 U.S.C.A. § 482: Customs Duties (2002) (original enactment: 1866) (emphasis added). Consequently, the authority vested in Government agents to detain and search travelers is limited to those "whom they shall suspect."

The Petitioner here does not challenge the Government's legitimate authority to effect "routine searches" of entrant "persons and effects," without "reasonable suspicion, probable cause, or warrant." *Hernandez*, 473 U.S. at 538; *see also United States v. Ramsey*, 431 U.S., at 616-619; *Almeida-Sanchez v. United States*, 413 U.S. 266, 272-273 (1973); *Carroll v. United States*, 267 U.S. 132, 154 (1925) Section 482 of the USCA articulates, and *Ramsey* affirms, that the Government's authority at the border is based on its interest in "prevent[ing] smuggling," "exclud[ing] aliens," *Ramsey* at 619, and "excluding illegal articles from [entering] the country." *Ramsey* at 618 (quoting *United States v. Thirty-seven Photographs*, 402 U.S. 363, 376 (1971). Accordingly, the "balance between the interests of the Government and the privacy right of the individual is … struck much more favorably to the Government at the border." *United States v. Alfaro-Moncada*, 607 F.3d 720, 727-28 (11th Cir. 2010) (quoting *Hernandez*, 473 U.S. at 539-40).

Indeed, routine searches are standard at the border because they effect the Government's reasonable ends. Routine searches are classified "as those which do not seriously invade a traveler's privacy." *United States v. Cardenas*, 9 F.3d 1139, 1148 n. 3 (5th Cir. 1993). Thus, a traveler crossing the border has a lower expectation of privacy in those articles typically subject to a routine search, e.g. his luggage, *United States v. Thirty-seven Photographs*, 402 U.S. 363, 376 (1971), vehicle, *Flores-Montano* 541 U.S. at 155, and the clothing he wears. *United States v. Whitted*, 541 F.3d 480, 485-86 (3d Cir. 2008) (holding "patdowns, frisks, luggage searches, and automobile searches, involving neither a high expectation of privacy nor a seriously invasive search, are routine"). Accordingly, CBP Policy considers the routine search of electronic devices to be "manual," where "officers review the contents of the device by interacting with it as an ordinary user would, through its keyboard, mouse, or touchscreen interfaces." U.S. Customs and Border Protection, Border Search of Electronic Devices, CBP Directive No. 3340-049A at ¶ 5.1.4 (Jan. 4, 2018).

This is the scope of the search Escaton reasonably expected as he re-entered the country. The search he was subject to by CBP began as routine, with Officer Stubbs looking through his vehicle and the contents of his luggage. (R. at 2). The search was routine even when Officer Stubbs manually searched Mr. Escaton's electronic devices by turning them on, disconnecting them from the internet, and reviewing the available content present before them. This search was routine because Stubbs was careful to review the devices "without assistive technology." (R. at

2); (U.S. Customs and Border Protection, Border Search of Electronic Devices, CBP Directive No. 3340-049A at ¶ 5.1.4 (Jan. 4, 2018).

In contrast, the search became nonroutine when Officer Stubbs, without any suspicion of wrongdoing, hidden contraband, or danger to national security, sent Mr. Escaton's laptop, USB devices, and hard drives to ICE for forensic inspection. (R. at 3). The only reason cited for delivering the devices to ICE was that some folders were password protected and the USB devices were inaccessible. (R. at 3).

In a nonroutine search, the individual's privacy interest is elevated to one which requires greater protection under the Fourth Amendment. Specifically, a nonroutine search requires individualized suspicion according to Congress (section 482, above), Supreme Court cases *Flores-Montano* and *Hernandez*, an array of appellate circuit decisions, and, finally, according to CBP policy.

This Court has acknowledged that, under section 482, an individual is "entitled to be free from unreasonable search and seizure" when "present[ing] [him]self at the border for admission." *Hernandez*, 473 U.S. at 539. Thus, reasonable suspicion is required for the detention of a traveler at the border "beyond the scope of a routine customs search," *Id*. at 541, "by virtue of [its] significant intrusion on an individual's privacy." *Whitted*, 541 F.3d at 485. Ultimately, this Court concluded that the reasonable suspicion standard "effects a needed balance between private and public interests" on the border where probable cause is not present or necessary. *Hernandez*, 473 U.S. at 541.

"Nonroutine" searches have been defined as "highly intrusive," exceeding a routine search, where the individual's "dignity and privacy interests" are infringed. *Flores–Montano*, 541 U.S. at 152; *United States v. Kolsuz*, 890 F.3d 133, 144 (4th Cir. 2018). Any search which can be classified as nonroutine must be justified by individualized suspicion. *Kolsuz*, 890 F.3d at 144 (quoting *Flores–Montano*, 541 U.S. at 152). Subsequently, federal circuits applied this higher standard and held that nonroutine searches at the border lacking individualized suspicion are illegitimate, and evidence discovered thereby is suppressible. *United States v. Cotterman*, 709 F.3d 952, 962 (9th Cir. 2013) (finding that comprehensive analysis of hard drive was nonroutine and invasive, requiring reasonable suspicion); *Davis v. United States*, 564 U.S. 229, 231-232 (2011) (affirming that evidence stemming from unreasonable search is generally inadmissible and thereby suppressible).

Furthermore, CBP policy itself requires that customs officers have "reasonable suspicion" of illegal activity or a "national security concern" to justify the escalation of a basic routine search to an advanced, nonroutine search U.S. Customs and Border Protection, Border Search of Electronic Devices, CBP Directive No. 3340-049A at ¶ 5.1.4 (Jan. 4, 2018). In the case at bar, Officer Stubbs was bound by CBP policy which prohibited him from conducting an advanced search, lacking, as he did, reasonable suspicion of any kind. (R. at 3). It was at that point that he sent the electronic devices over to ICE, which is bound by no such reasonableness standard. (R. at 3). (U.S. Customs and Border Protection, Border Search of Electronic Devices, CBP Directive No. 3340-049A at ¶ 5.1.4 (Jan. 4, 2018) (§6.1 "ICE Special Agents acting under border search authority may search, detain, seize, retain, and share electronic devices, or information contained therein, with or without individualized suspicion" and §6.2, stating that ICE agents are not bound by CBP policy). Here, the CBP acknowledges that travelers do retain a privacy interest in material that would require "advanced" intrusion, and that this interest should be protected by the reasonable suspicion standard. U.S. Customs and Border Protection, Border Search of Electronic Devices, CBP Directive No. 3340-049A at ¶ 5.1.4 (Jan. 4, 2018).

That people have a heightened privacy interest in their electronic devices is no longer in question. *See Riley*, 134 S. Ct. at 2491 (finding that search of electronic device in question is "far *more* exhaustive" than the "search of a house"); *see also Kolsuz*, 890 F.3d at 145 (reasoning that "unparalleled breadth of private information" on digital device establishes privacy interest). That individuals maintain this privacy interest upon crossing the border is likewise settled. *See Kolsuz*, 890 F.3d at 144. "The nature of the contents of electronic devices differs from that of luggage" since "they contain the most intimate details of our lives: financial records, confidential business documents, medical records and private emails." *Cotterman*, 709 F.3d at 962. Finally, it has been established that the individual's privacy interest in such cases is weightier on the border than Government interests. *See Cotterman*, 709 F.3d at 968 (finding "such a thorough and detailed search of the most intimate details of one's life is a substantial intrusion upon personal privacy and dignity" requiring "a showing of reasonable suspicion."); *see also Kolsuz*, 890 F.3d at 147 (noting Government interests lessen the reasonableness requirement for searching electronic devices from warrant requirement in the interior to reasonable suspicion on the border, but does not subsume it altogether).

The threshold is therefore set: the Fourth Amendment is not a dead language at the border; it will continue to protect travelers' privacy and dignity by requiring individualized suspicion for nonroutine electronic device searches. The Government should have shown that it had individualized suspicion of Escaton's wrongdoing before the search.

B. A forensic search is inherently nonroutine and must be justified by reasonable suspicion to be constitutional.

On a daily basis, more than a million people cross American borders. In the United States, ninety-five percent of adults own a cell phone and at least fifty percent own tablets "which are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Riley*, 134 S. Ct. at 2485; *Alasaad v. Nielsen*, No. 17-CV-11730-DJC, 2018 WL 2170323, at *2 (D. Mass. May 9, 2018. In 2017 alone, CBP conducted over thirty thousand border device searches, "more than triple the number of just two years earlier." *Court Rejects Government Bid To Dismiss ACLU-EFF Suit Challenging Warrantless Phone Searches At U.S. Border*, ACLU: News (May 10, 2018), https://www.aclu.org/news/court-rejects-government-bid-dismiss-aclu-eff-suit-challenging-warrantless-phone-searches-us. Maintaining that trajectory, CBP will search nearly 100,000 digital devices in 2019.

In the face of these staggering statistics, the critical question before the court today is whether it will limit "the power of technology to shrink the realm of guaranteed privacy." *Kyllo v. United States*, 533 U.S. 27, 34 (2001). The *Cotterman* court aptly answered this problem by concluding that a "person's digital life ought not [to] be hijacked simply by crossing a border," *Cotterman*, 709 F.3d at 965, and the Petitioner here requests this Court similarly conclude.

Once CBP sent Escaton's devices to ICE, they were subject to a forensic search. (R. at 3). A forensic search begins when officers "use sophisticated tools, such as software programs or specialized equipment, to evaluate information contained on a device." *Alasaad v. Nielsen*, No. 17-CV-11730-DJC, 2018 WL 2170323, at *2 (D. Mass. May 9, 2018). Classified as an "advanced search" in CBP policy, the forensic search is defined as "any search in which an Officer connects external equipment … to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents." CBP policy §5.1.4. This process is precisely described in the facts of the instant case: upon receipt of Escaton's electronic devices, ICE Special Agent and Computer Forensic Examiner, Cullen, "used forensic software to copy

and scan" all eight devices. (R. at 3). The Government admits to having no reasonable suspicion when its agent conducted this advanced search. (R. at 6).

Lacking reasonable suspicion, a forensic border search is a *per se* violation of the Fourth Amendment because its "comprehensive and intrusive nature" triggers Constitutional protection. *Cotterman*, 709 F.3d at 144. Forensic searches take, within their exhaustive scope, every iota of data stored or viewed, internet browsing history, photos, calendars, and notes, including "active files, deleted files, files in allocated and unallocated storage space, metadata … password-protected or encrypted data, and log-in credentials and keys for cloud accounts." *Alasaad v. Nielsen*, No. 17-CV-11730-DJC, 2018 WL 2170323, at *2 (D. Mass. May 9, 2018). The storage capacity of laptops sold in 2017 reached two terabytes of data, easily storing over half a billion pages, or the equivalent of all the pages contained in a fifteen-floor academic library. *Cotterman*, 709 F.3d at 964; Orin S. Kerr, *Searches and Seizures in A Digital World*, 119 Harv. L. Rev. 531, 542 (2005). Yet, "[e]ven a car full of packed suitcases with sensitive information cannot hold a candle to the sheer, and ever-increasing, capacity of digital storage." *Kolsuz*, 890 F.3d at 145.

More importantly, the nature of the digital data stored in these endless annals sets it apart from the physical subjects of routine border searches. Essentially, electronic devices "contain the most intimate details of our lives: financial records, confidential records, confidential business documents, medical records, and private [correspondence]." *Cotterman*, 709 F.3d at 964. Sensitive information stored on digital devices share in the protection of "papers and effects," held sacrosanct in the Constitution from warrantless intrusion. U.S. Const. amend. IV.; *Cotterman*, 709 F.3d at 964. In fact, it was this right to be free from warrantless intrusion that triggered the American Founders to denounce writs of assistance, "which James Otis pronounced, 'the worst instrument of arbitrary power, the most destructive of . . . liberty' since they placed 'the liberty of every man in the hands of every petty officer.'" *Boyd*, 116 U.S. at 630. The *Boyd* Court found that "the search for and seizure of stolen or forfeited goods" is "totally different … from a search for and seizure of a man's private books and papers for the purpose of obtaining information therein contained, or of using them as evidence against him." *Id*. This personal, sensitive information is man's "dearest property," *Id*., and therefore his most dearly protected privacy interest. The Government conducting a forensic search is therefore "akin to reading a diary line by line looking for mention of criminal activity – plus looking at everything the writer might have erased." *Cotterman*, 709 F.3d at 962–63.

When Government agents conduct a forensic search of a traveler's laptop at the border, the nature of this search is *per se* intrusive, justifiable only upon a showing of reasonable suspicion. *Cotterman*, 709 F.3d at 962. As he drove across the border from Mexico, Cotterman's laptop was subject to a search that began as cursory, then transformed into a forensic examination of his hard drive. *Cotterman*, 709 F.3d at 957. Using computer forensic software to copy Cotterman's hard drive and analyze it in its entirety, including deleted data, Government agents found 75 deleted images of child pornography and 378 more in password-protected files. *Cotterman*, 709 F.3d at 958-59. Before commencing the forensic search, customs agents discovered through TECS (Treasury Enforcement Communication System) that Cotterman had been convicted on seven counts relating to child molestation, and was potentially involved in child sex tourism. The Ninth Circuit reversed the lower court finding that the search was impermissible, but only because the Government agents had reasonable suspicion that this particular traveler might be harboring such contraband based on his prior convictions. *Cotterman*, 709 F.3d at 962.

While some facts in *Cotterman* are reminiscent of the instant case, the determinative facts are readily distinguishable. Like *Cotterman*, customs agents initially conducted a cursory search of Escaton's laptop which escalated into an advanced search using computer forensic software. (R. at 2-3). Like Cotterman, Escaton had password-protected files on his computer. (R. at 3) The pivotal difference between these cases lies in the fact that the forensic search of Cotterman's computer was justified by reasonable suspicion based on his criminal history which pointed specifically to a crime like harboring child pornography. *Cotterman*, 709 F.3d at 962. The forensic search of Escaton's computer was not preceded even by an "inchoate and unparticularized suspicion or hunch of criminal activity," let alone an individualized suspicion of any crime. (R. at 3); *Cotterman*, 709 F.3d at 970 (quoting *Hernandez*, 473 U.S. at 542) (internal quotation omitted).

Moreover, the fact that CBP and ICE worked in concert to break through the defenses of Escaton's password-protected files and devices compounds the violation wrought by the forensic search. (R. at 3). "By using a password," the respondent "affirmatively intended to exclude ... others from his personal files." *United States v. Buckner*, 473 F.3d 551, 554 (4th Cir. 2007) (quoting *Trulock v. Freed*, 275 F.3d 391, 403 (4th Cir. 2001)). It is not only reasonable, but well established that an individual has an actual expectation of privacy in files which he takes steps to

exclude from others as confidential. *Buckner*, 473 F.3d at 554 (affirming lower court holding comparing password-protected files to a "locked box" in common space). Since the existence of a password-protected file does not by itself suggest criminal activity, Escaton's password-protected files gave rise to no legitimate suspicion. *Cotterman*, 709 F.3d at 969. Furthermore, the Government concedes to having no suspicion vested in the contents of Escaton's files when it sought to trespass his confidential "locked box," giving them no legal excuse or defense whatsoever. (R. at 3).

The decision below maintains that it does not make a ruling on searches of information not "presently before" the searching customs agent. (R. at 9). This is hard to reconcile when it accepts as reasonable forensic searches which unearth deleted material from computer user's unallocated storage space. Once a person deletes something from their computer, they believe that it is gone. How can it reappear before customs agents at some removed time in the future, and be considered "presently before" them then? Moreover, with the forensic software technology's ability to bring new life to deleted data, how can we be reassured in the fact that customs agents "delete scans" that they take from our computers. In essence, they keep our information forever.

In contrast, the decision below aligns itself with *United States v. Touset*, holding that forensic computer searches at the border require no reasonable suspicion. (R. at 7); *Escaton v. United States*, 1001 F.3d 1341 (14th Cir. 2021); *United States v. Touset*, 890 F.3d 1227 (11th Cir. 2018). The Eleventh Circuit reasoned that since the Supreme Court has not yet required reasonable suspicion for property searches at the border, the Fourth Amendment "touchstone" reasonableness analysis is meritless in such cases. *Id*. In so doing, the *Touset* court dispenses with the better part of the Fourth Amendment protections for the sole reason that searches occur at the border. This runs in the face of every Supreme and federal Circuit Court decision extensively weighing the reasonableness of border property searches, e.g. *Flores-Montano*, 541 U.S. 149; *Kolsuz*, 890 F.3d 133; *Romm*, 455 F.3d 990. Despite holding the reasonableness analysis unnecessary, the Eleventh Circuit examined whether customs agents reasonably suspected Touset of illegal activity prior to the forensic search of his computer, and found that they did. *Touset*, 890 F.3d 1227.

Finally, federal circuit courts have consistently interpreted the *Flores-Montano* allowance for "particularly offensive" or "highly intrusive searches of the person" to apply an

individualized suspicion standard to forensic computer searches. The Ninth Circuit considered a traveler's history of related criminal conduct sufficient to support reasonable suspicion for forensic computer border search. *United States v. Romm*, 455 F.3d 990, 994 (9th Cir. 2006). The Fourth Circuit found that computer search at the border was justified after traveler's criminal record was revealed. *United States v. Ickes*, 393 F.3d 501, 507 (4th Cir. 2005). The Second Circuit found the border search of computer diskettes legitimate after agents suspected a convicted pedophile of transporting child pornography. *United States v. Irving*, 452 F.3d 110, 115 (2d Cir. 2006). Comparatively, the Ninth District held that a non-forensic border search of a laptop was legitimate without reasonable suspicion, regardless of the fact that reasonable suspicion existed in that case. *United States v. Arnold*, 533 F.3d 1003, 1008 (9th Cir. 2008).

In conclusion, forensic searches of electronic devices are nonroutine because they are "highly intrusive" in scope. The nature of a forensic search allows the searcher to plumb the depths of electronic device history with detailed and comprehensive clarity, and with it, the private history of its user. Nonroutine border searches require a showing of reasonable, individualized suspicion to satisfy the Fourth Amendment "reasonableness" requirement. The customs agents conducting the forensic search of Escaton's devices had no such suspicion.

No federal court has found a nonroutine border search to be justified in a case where there was no reasonable suspicion. This is a Government search which directly implicates the "dignity and the privacy of the person being searched," *Flores-Montano*, 541 U.S. at 152, and the intimacy of a person's "papers and effects." U.S. Const. amend. IV. Therefore, we respectfully request that this Court adopt the reasoning of circuit courts, above, and hold that a forensic search of electronic devices must be justified by reasonable suspicion at the border.

"But if there is one enduring lesson in the long struggle to balance individual rights against society's need to defend itself against lawlessness, it is that "[i]t is easy to make light of insistence on scrupulous regard for the safeguards of civil liberties when invoked on behalf of the unworthy. It is too easy. History bears testimony that by such disregard are the rights of liberty extinguished, heedlessly at first, then stealthily, and brazenly in the end." Davis v. United States, 328 U.S., at 597, 66 S.Ct., at 1263 (Frankfurter, J., dissenting).

I. THIS COURT SHOULD REVERSE BECAUSE THE GOVERNMENT'S ACQUISITIONS OF HISTORICAL AND TOWER DUMP CSLI WERE WARRANTLESS SEARCHES UNDER THE FOURTH AMENDMENT

When the Government invades a legitimate expectation of privacy, this generally qualifies as a search under the Fourth Amendment requiring a warrant supported by probable cause. *Carpenter,* 138 S. Ct. at 2213 (citing *Smith,* 442 U.S. at 740). Accordingly, *Jones* held that "individuals have a reasonable expectation of privacy in the whole of their physical movements." *United States v. Jones,* 565 U.S. 400, 430 (2012). Consequently, *Carpenter* found that "allowing Government access to cell-site records . . . contravenes that expectation." *Carpenter,* 138 S. Ct. at 2210.

Modern technology allows the "inquisitive eyes" of the Government to see further than the Fourth Amendment Founders could have anticipated. Hence, the Government's ability to track an individual's location and movement gives rise to Fourth Amendment concerns. To this point, a modern cell phone generates location-based data on a minute-to-minute basis, creating a seamless log of an individual's location and movement. Rachel Levinson-Waldman, *Cellphones, Law Enforcement, and the Right to Privacy*, Brennan Center for Justice: Liberty and National Security Report, (Dec. 2018) ttps://www.brennancenter.org/sites/default/files/publications/2018_12_CellSurveillanceV3.pdf. This cell-site location information (CSLI) is generated every time a cell phone user texts, calls, or relies on cellular data for internet connection or the functionality of mobile apps and updates, even when left in standby mode. *Id*. The resulting data provides a log of an individual's location collected in continuous intervals with a possible accuracy of fifty feet from the user's actual location. (Hale Aff. ¶ 11.). Most carriers keep CSLI data records for an average of five years. *Carpenter,* 138 S. Ct. at 2218. Thus, CSLI data is capable of providing near-perfect,

retrospective surveillance of an individual's locations and movements over several years. *Id*. (finding that this data achieves the "near perfect surveillance" of an ankle monitor).

A. Escaton had a reasonable expectation of privacy in the historical CSLI that the Government obtained without a warrant.

Carpenter identified CSLI as a unique type of data that unequivocally implicates the privacy right established in *Jones.* Thus, "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI." *Carpenter*, 138 S. Ct. at 2217. Consequentially, the Government's acquisition of historical CSLI constitutes a search and its "obligation is a familiar one -- get a warrant." *Id*. at 2217, 2222–23.

1. The Government's acquisitions of Escaton's historical CSLI pursuant to 18 U.S.C. § 2703(d) were unreasonable searches for lack of probable cause.

Under *Carpenter*, the Government's search is unreasonable when it obtains historical CSLI under the Stored Communications Act (SCA), 18 U.S.C. § 2703(d). In *Carpenter*, the Government requested and received an individual's historical CSLI data per a court order under 18 U.S.C. § 2703(d), requiring only that the Government demonstrate "reasonable grounds to believe" that the records sought are "relevant and material to an ongoing criminal investigation." *Carpenter*, 138 S. Ct. at 2212; 18 U.S.C. § 2703(d). Similarly, the FBI relied exclusively on an 18 § 2703(d) order when it obtained historical CSLI records for three days and 100 cumulative hours over ten days from Escaton's cell carrier. (R. at 5). *Carpenter* reasoned that the showing for SCA requests "falls well short of the probable cause required for a warrant" which the "Government must generally obtain . . . before acquiring [CSLI]." *Carpenter*, 138 S. Ct. at 2221.

Accordingly, *Carpenter* held that an "order issued under Section 2703(d) of the Act is not a permissible mechanism for accessing historical cell-site records" because it fails to establish probable cause. *Id*. Likewise in the present case, the FBI's acquisition of Escaton's historical CSLI records via SCA requests was unreasonable because it lacked probable cause and a

warrant. (R. at 2); see, e.g., *United States v. Goldstein*, No. 15-4094, 2019 WL 273103, at *2 (3d Cir. Jan. 22, 2019) (holding "that under *Carpenter*, acquiring Goldstein's CSLI was an unconstitutional search under the Fourth Amendment because the Government did not obtain a warrant supported by probable cause").

2. After *Carpenter*, SCA § 2703(d) requests are insufficient to support any Government acquisition of Escaton's historical CSLI.

The Tenth Circuit has interpreted the rule of *Carpenter* to effect a general warrant requirement before obtaining historical CSLI, and therefore nullifying the use of SCA requests altogether. *United States v. Thompson*, 740 F. App'x 166, 167 (10th Cir. 2018). In *Thompson*, the Supreme Court directed the Tenth Circuit to review, in light of *Carpenter*, its finding that the Government did not violate the Fourth Amendment when it obtained historical CSLI pursuant to an SCA § 2703(d) order. *Id*. The same question is certified to Petitioner in the instant case. *Thompson* concluded that *Carpenter's* holding was "largely based on 'the unique nature of cell phone location information'" necessitating probable cause, and held the CSLI search unconstitutional *Id*. at 168. Further, since "*Carpenter* supersedes our holding," the Tenth Circuit vacated its previous ruling in support of Government CSLI acquisition. *Id*. Here, as in *Thompson*, the FBI's SCA § 2703(d) request for historical CSLI violates the rule against SCA requests laid down in *Carpenter*. See, e.g., *United States v. Chambers*, No. 16-163-CR, 2018 WL 4523607, at *1 (2d Cir. Sept. 21, 2018) (applying *Carpenter* to find Government's use of SCA order did not comport with the Fourth Amendment).

3. Circuit courts interpret *Carpenter* as establishing a new general rule requiring the Government to get a warrant before obtaining any of an individual's CSLI.

Recent case law confirms that *Carpenter* functions as a new general rule providing individuals a legitimate expectation of privacy in the whole of their CSLI and requiring a warrant

for any Government acquisition of CSLI. The Third Circuit found that *"Carpenter* sets forth a *new rule* that defendants do in fact have a *privacy interest in their CSLI* and the *Government must generally obtain a search warrant* supported by probable cause to obtain this information." *United States v. Goldstein*, No. 15-4094, 2019 WL 273103, at *1 (3d Cir. Jan. 22, 2019) (emphasis added). The Second Circuit affirms that "*Carpenter* recognizes that individuals have a reasonable expectation of privacy in cell-site data," and "holds that the acquisition of that data requires "a warrant supported by probable cause."" *United States v. Chambers*, No. 16-163-CR, 2018 WL 4523607, at *1 (2d Cir. Sept. 21, 2018) (quoting *Carpenter*, 138 S. Ct. at 2220–21). The Eleventh, Fourth, and Tenth Circuits interpret *Carpenter* in an identical manner, confirming that *Carpenter's* main effect is to establish, without question, an individual's legitimate expectation of privacy in their CSLI and to limit the Government's access thereto with a warrant requirement. *See*, e.g., *United States v. Adams*, No. 17-13109, 2018 WL 6177151, at *1 (11th Cir. Nov. 26, 2018); *United States v. Burton*, No. 17-4524, 2018 WL 6719714, at *5 (4th Cir. Dec. 19, 2018); *Thompson*, 740 F. App'x at 167.

In the case at bar, the FBI accessed Escaton's individual hsitorical CSLI record twice: once for three days and a second time for 100 consecutive hours over ten days. (R. at 5). Because Escaton has an established privacy interest in all of his CSLI under *Carpenter*, all warrantless SCA requests are invalid. The invasion of Escaton's CSLI privacy interest unequivocally constitutes a Fourth Amendment search. Under *Carpenter*, the FBI's SCA§ 2703(d) requests immediately fail for lack of probable cause and are inherently unreasonable searches. Thus, in light of *Carpenter*, both acquisitions of Escaton's historical CSLI equally violated the Fourth Amendment.

In conclusion, *Carpenter's* new rule protects Escaton's reasonable expectation of privacy in the whole of his physical movements by requiring that the FBI get a warrant before accessing his historical CSLI. The FBI's SCA requests fail to satisfy the probable cause standard for a warrant. Thus, its searches of Escaton's CSLI were unreasonable and in violation of the Fourth Amendment.

B. Escaton had an equally reasonable expectation of privacy in his cell-location information acquired without a warrant through three tower dumps.

1. CSLI collected via tower dumps implicates the same privacy interests protected under *Carpenter.*

CSLI collected from tower dumps implicates the same reasonable expectations of privacy established in *Carpenter*. When the Government receives a tower dump, it collects all the CSLI data that an individual cell tower generated during the requested time period. The Honorable Brian L. Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in Its Electronic Surveillance*, 16 U. Pa. J. Const. L. 1, 1–2 (2013). This includes CSLI for all cellular users whose devices connect to that cell tower, regardless of their specific cellular carrier. *Id*. The Government typically uses tower dumps to compile lists of potential suspects or to prove a suspect's location at a particular date and time. *Id.* Although tower dump collections of CSLI are location specific rather than user specific, they provide access to the same type of private CSLI data that *Carpenter* protects.

Carpenter found that an individual has a legitimate expectation of privacy in the location information his cell phone generates because this continuous generation is recorded with such accuracy that it surpasses concerns raised by GPS monitoring. *Carpenter*, 138 S. Ct at 2210. The pervasive use of cellphones guarantees that location data is being collected, even while the user conducts his most private business in private places. *Riley v. California*, 134 S. Ct. 2473, 2484,

2490 (2014). Moreover, because location data generation is continuous, pervasive, and ever-increasing in accuracy, this unique "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.'" *Carpenter*, 138 S. Ct. at 2217 (quoting *Jones*, 565 U.S. at 415). Regardless of the purpose for requesting the data, whether to ascertain the continuous movement of a particular user or to get an exhaustive list of every cellular user in the area, the data and privacy interest remain the same.

Whether collected as a tower dump or as historical CSLI, the location data is indistinguishable with respect to the individual's "privacies of life" for the purposes of the Fourth Amendment. Thus, the individual's legitimate privacy interest in CSLI persists, even when the Government obtains it through a tower dump.

2. ***Carpenter's* reasoning extends to all Government invasions of the individual's right to privacy via access to CSLI, tower dumps in particular.**

This Court found repugnant the Government's ability to access a "detailed chronicle of a person's physical presence compiled every day, every moment, over several years," without a warrant. *Carpenter*, 138 S. Ct. at 2220. Similarly, the Government requests tower dump CSLI specifically to establish "a person's physical presence" in a given location, and this information is "compiled every day" in an encyclopedic record. *Id*. Furthermore, the Government's ability to request tower dump information without a warrant allows it to retrospectively and with near-perfect accuracy pin-point an individual's location years in the past. *Carpenter*, 138 S. Ct. at 2210, 2218.

Here, the FBI conducted an unreasonable search for Escaton's physical presence recorded in his CSLI when it used tower dumps to confirm his exact whereabouts in the past. Under an SCA § 2703(d) request, the FBI acquired one cumulative hour of CSLI for each of three cell

towers requested. (R. at 5). Because of where these towers were situated, the FBI was able to verify Escaton's "physical location" in Sweetwater, within fifty feet, Hale Aff. ¶ 11, of his actual location. *Carpenter,* 138 S. Ct. at 2210. The tower dump gave the FBI the ability to "travel back in time" to discover Escaton's presence near the Mariposa ATMs a year prior to the date of the SCA request. *Carpenter*, 138 S. Ct. at 2218. The FBI relied on the information's locational and temporal accuracy as evidence of Escaton's specific location during a specific hour on a particular day in early October of 2018. (R at 5). Through these tower dumps the FBI illicitly gained access to a continuous, retrospective, and reliable record, of otherwise unknown details, about Escaton's physical presence during the previous year. In this case, the tower dumps invaded Escaton's right to privacy in the whole of physical location and movement. This invasion renders the FBI's reliance on an SCA request unreasonable under the Fourth Amendment.

Moreover, the privacy interests of Escaton are not the only privacy interests invaded here. Tower dumps raise an intimate issue of public policy that affects millions of cell users per annum. Tower dumps implicate the privacy interests, of not only suspects, but also countless innocents within cell tower range, who remain entirely unaware that the Government has catalogued their information for future use. Katie Hoss, *Cell Tower Dumps: Another Surveillance Technique, Another Set of Unanswered Questions,* UCLA: Free Future (Mar. 27, 2014, 11:58 AM) https://www.aclu.org/blog/national-security/privacy-and-surveillance/cell-tower-dumps-another-surveillance-technique. In this way, tower dumps are equivalent to a "tireless and absolute surveillance" that "runs against everyone" who carries a cellular device, not just those persons currently under investigation. *Carpenter*, 138 S. Ct. 2218. Therefore, the practical effect of Government access to tower dump CSLI is that "*whoever the suspect turns out*

to be, he has effectively been tailed every moment of every day for five years." *Id*. (emphasis added). Following the reasoning laid down in *Carpenter,* the Government invades the privacy interests of *every person* within range of tower dump by acquiring and cataloguing their CSLI without warrant or probable cause.

Ultimately, the privacy invasions tower dumps cause makes them unworkable under the Fourth Amendment. Tower dumps implicate the privacy interests of every individual whose information they collect for any single request. Considering that these requests "are likely to affect at least hundreds of individuals' privacy interests" and that a large carrier like "Verizon had more than 14,000 cell tower dump requests in both 2016 and 2017 and is on track for even more in 2018," this Court cannot turn a blind eye to the staggering number of innocent parties with privacy interests at risk from tower dumps. *In re Search of Cellular Tel. Towers*, 945 F. Supp. 2d 769, 770 (S.D. Tex. 2013); Rachel Levinson-Waldman, *Cellphones, Law Enforcement, and the Right to Privacy*, Brennan Center for Justice: Liberty and National Security Report Report, (Dec. 2018). In some cases, the number of bystanders affected is overwhelming. In 2010, with facts similar to the case at bar, "the FBI received over 150,000 numbers in a single dump in an effort to determine if a suspect had been near several banks that had been robbed." Katie Hoss, *Cell Tower Dumps: Another Surveillance Technique, Another Set of Unanswered Questions*, UCLA: Free Future (Mar. 27, 2014, 11:58 AM). These numbers are staggering considering that tower dumps have become a routine part of the Government's initial stages of criminal investigation, often requested before the Government has identified its first suspect.

In conclusion, tower dumps implicate both the individual privacy interests addressed in *Carpenter* and entirely new privacy issues resulting from the lump sum manner in which they compile CSLI. The FBI's acquisition of three tower dumps constitutes a clear invasion of

Escaton's privacy interest in the whole of his movement and CSLI record of his physical presence. Moreover, the agency's SCA request for the tower dump falls far short of the probable cause requirement for Government invasions of personal privacy. Such an invasion of privacy is facially unreasonable in the absence of an exigency or a warrant. In addition, because tower dumps are incapable of discriminating between criminals and law-abiding citizens, the FBI request likely subjected numerous innocent bystanders' cell location information to an unwarranted search. There is an argument that *Carpenter's* reasoning supports an outright restriction of Government access from tower dumps. However, it is sufficient for the present case that *Carpenter* clearly supports an extension of the warrant requirement to tower dump acquisitions.

CONCLUSION

The Fourteenth Circuit incorrectly applied Fourth Amendment law to Escaton's detriment. First, Government agents should have possessed reasonable suspicion of illegal activity or contraband before conducting a forensic search of Escaton's digital devices because this search was nonroutine and highly intrusive. Second, the Government's acquisition of Escaton's CSLI violated his right to be secure in the whole of his movements when the acquisition was unsupported by a warrant. For the foregoing reasons, Petitioner respectfully requests that this Court REVERSE the ruling of the Fourteenth Circuit. Respectfully submitted,

Attorneys for

Petitioner