No. 18-3939

IN THE SUPREME COURT OF THE UNITED STATES

March Term 2023

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 THE PETITIONER

Team R18

Counsel for the Petitioner

TABLE OF CONTENTS

TABLE OF AUTHORITIES

UNITED STATES SUPREME COURT CASES

FEDERAL CIRCUIT COURT OF APPEALS CASES

CONSTITUTIONAL PROVISIONS

STATUTES

OTHER AUTHORITIES

QUESTIONS PRESENTED

1. Does the Fourth Amendment require that government officers have reasonable suspicion before conducting forensic searches of electronic devices at an international border?
2. Do the government's acquisitions pursuant to 18 U.S.C. § 2703(d) of 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 violate the Fourth Amendment of an individual in light of this Court's limitation on the use of cell-site location information in *Carpenter v. United States*, 138 S. Ct. 2206 (2018)?

OPINION BELOW

The United States Court of Appeals for the Fourteenth Circuit issued its opinion on November 2, 2021. The opinion is reported in *Escaton v. United States*, 1001 F.3d 1341 (14th Cir. 2021).

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

This case involves the Fourth Amendment:

> 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

A. Standard of Review

This case involves review of the Fourteenth Circuit's denial of a motion to suppress; because motions to suppress involve mixed questions of fact and law, the appropriate standard of review for legal conclusions is the de novo standard while the factual determinations should be reviewed for clear error. *United States v. Muglata*, 44 F.3d 1530, 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)).

B. Summary of Argument

The Fourteenth Circuit Court of Appeals (Fourteenth Circuit) was incorrect in its decision to deny Petitioner Hector Escaton's (Escaton) motion to suppress the results of the forensic search. The Fourth Amendment demands particularized suspicion to conduct forensic searches of electronic devices, even at border crossings. Modern day laptops and other electronic devices provide more insight into a person's life than their own home can, at times. Society's reliance on and attachment to these devices has arguably made them an extension of the human body itself. As such, the search and seizure of these devices is protected under the Fourth Amendment. Consequently, the government must demonstrate a degree of interest, arguably meeting the reasonable suspicion standard, before being allowed to search these types of sensitive devices.

The Fourteenth Circuit was also incorrect it its decision to deny Escaton's motion to suppress the cell-site data requested from Delos Wireless. This Court has established that, under the Fourth Amendment, an individual maintains a reasonable expectation of privacy in some cell-site location information (CSLI). The Fourteenth Circuit was incorrect in finding that the cumulative hours of law enforcement requests fell within the constitutional limits deemed appropriate in *Carpenter*. A reasonable expectation of privacy exists to protect against arbitrary and continuous

searches beyond the seven-day limit. The cumulative searches included tower dumps that relied upon each other, in succession, to work around the warrant requirement (totaling 169 hours of CSLI). Finally, the tower dump information in this case was highly-specific due to the nature of the physical geography in Sweetwater, West Texas. The circumstances of this ongoing investigation did not rise to meet the "exigent circumstances" exception. Thus, an error of law is present throughout the ruling and requires this Court to reverse.

This Court should reverse the Fourteenth Circuit's decision to deny Escaton's motion to suppress the results of the forensic search and the cell-site data requested from Delos Wireless.

STATEMENT OF THE CASE

A. Statement of Facts

On September 25, 2019, Escaton, a West Texas citizen and resident, returned to the United States from Mexico through a West Texas border checkpoint. (R. at 2). Customs and Border Patrol (CBP) Agent Ashley Stubbs (Stubbs) searched Escaton's vehicle during a routine border stop and found three large suitcases in the back. *Id*. Stubbs discovered several electronic devices: an iPhone, a laptop, three external hard drives, and four USB devices. *Id*. After ensuring that they were disconnected from wireless service and placing them on airplane mode, Stubbs proceeded to conduct a manual search of the iPhone and laptop. *Id*. A paper note was placed below the keyboard of the laptop with the message "Call Delores (201) 181-0981 $$$." *Id*. Stubbs made note of the message and number and then submitted everything except the iPhone to a forensic search without reasonable suspicion of criminal activity. *Id*. The search revealed tools and financial information that implicated Escaton in a financial fraud. *Id*.

CBP notified the Federal Bureau of Investigation (FBI), which had been investigating "ATM skimming" of Mariposa Bank ATMs in Sweetwater, West Texas during October of 2018. *Id*. at 3. FBI Special Agent Catherine Hale (Hale) began examining the connections between the forensic evidence discovered and that reported by Mariposa Bank. *Id*. Hale then received information regarding the malware used to hack into the ATMs and surveillance photographs near the ATMs, revealing a man in a black sweatshirt. *Id*. at 4. Using all of the information gathered, she requested three tower dumps from the cell sites near three Sweetwater ATMs pursuant to 18 U.S.C. §2703(d) of the Stored Communications Acts (SCA) for 30 minutes before and 30 minutes after the man in the black sweatshirt approached the ATMs. *Id*.

Stubbs reported Escaton's information to the FBI for potential bank fraud and identity theft claims. *Id*. at 5. The malware found on his USB devices was similar to the malware used to hack

into the Sweetwater ATMs. *Id*. His phone number also matched one of the numbers generated from the tower dumps. *Id*. Using this information, U.S. Attorney Hughes applied for court orders under the SCA to obtain Escaton's cell phone records. *Id*. A federal magistrate judge issued an order directing Delos Wireless (Escaton's wireless carrier) to disclose cell site records corresponding to Escaton's phone number from October 11, 2018 to October 13, 2018. *Id*.

Suspecting that the "Delores" identified on the note from the laptop may have abetted the skimming, the government requested that the magistrate judge issue an additional order to Delos Wireless to disclose cell/site sector information for Escaton's and Delores's phone number for all weekday records between October 1 and 12 between the hours of 8 am and 6 pm as well as subscriber information for Delores's phone. *Id*. Using all of this information collectively, the government was able to link Escaton and Delores to the ATM skimming scheme in Sweetwater. *Id*.

B. Procedural History

Escaton moved to suppress the evidence from both the forensic border search and the CSLI requests, but the district court denied the motion. *Id*. at 6. A jury convicted Escaton of bank fraud, 18 U.S.C. § 1344, conspiracy to commit bank fraud, 18 U.S.C. § 1349, and aggravated identity theft, 18 U.S.C. § 1028A. *Id*.

Escaton appealed his convictions on the grounds that the district court erred in denying his motion to suppress because the forensic search of his electronic devices and CSLI requests pertaining to him violated his Fourth Amendment rights. *Id*. The Fourteenth Circuit Court of Appeals found that law enforcement acted properly and within the bounds of Fourth Amendment protections. *Id*. Accordingly, it affirmed the district court's ruling denying Escaton's motion to suppress. *Id*.

ARGUMENT

I. THE FOURTH AMENDMENT DEMANDS REASONABLE SUSPICION TO CONDUCT FORENSIC EXAMINATIONS OF ELECTRONIC DEVICES AT BORDER CROSSINGS.

The Fourth Amendment ensures "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures …" U.S. Const. amend. IV. Historically, border searches "have been considered to be 'reasonable' by the single fact that the person or item in question had entered into our country from outside." *United States v. Ramsey*, 431 U.S. 606, 619 (1977). Although there has never been any additional requirement that the reasonableness of a border search depend on the existence of probable cause, courts have begun to acknowledge that old laws need to adapt to modern developments in technology when they are applied.

In the opinion below, the Fourteenth Circuit argued that "a person expects less privacy upon entering and exiting the United States than in his movements and affairs within the United States." (R. at 7). Furthermore, the court contends that "there is a significant national security interest in using the border to screen for risks to the United States." *Id*. As a result, it did not find that *Riley v. California*, 134 S. Ct. 2473 (2014) provided any clarification for border forensic searches because it interpreted *Riley* to address a different question, unrelated to searches at the border.

In contrast, we urge this Court to consider the fact that laptops (and other electronic devices) are unique pieces of technology that demand particularized suspicion because of their level of intrusion. We find that there are several reasons to apply the reasonable suspicion standard to border searches of electronic devices. Finally, we argue that this Court's decision in *Riley* is applicable to the facts of the present case.

A. Neither A Lower Expectation of Privacy nor A Heightened Threat to National Security at the Border Justify the Search of Electronic Devices Without Reasonable Suspicion.

i. Laptops are Unique Pieces of Technology that Demand Particularized Suspicion in Order to Protect the Fourth Amendment Rights of Their Owners.

Laptops are unique pieces of technology that allow people to save their most precious memories, important files, and confidential information all in one place. In the past, courts have tried to analogize laptops with closed containers, which have already been determined not to require particularized suspicion. Rasha Alzahabi, *Should You Leave Your Laptop at Home When Traveling Abroad?: The Fourth Amendment and Border Searches of Laptop Computers*, 41 Ind. L. Rev. 161, 181 (2008).

But laptops are *more* than closed containers. In fact, a laptop computer can "contain as much information about us as our homes contain – perhaps more." Brief for Ass'n of Corporate Travel Executives & Elec. Frontier Found. as Amici Curiae Supporting Defendant-Appellee at 12, *United States v. Arnold*, 533 F.3d 1003 (9th Cir. 2008) (No. 06-50581). When searches are conducted of the files contained on a person's laptop, the government is able to extract as much information as it would be able to if it had extensively searched that person's home. *Id*. at 16. Some courts have even recognized the privacy concerns that computers implicate by stating that "for most people, their computers are their most private spaces." Alzahabi at 180 (citing *United States v. Ziegler*, 474 F.3d 1184, 1189 (9th Cir. 2007)). Even when people are traveling, they presume the privacy of their homes is protected under the Fourth Amendment. Brief for the Amici Curiae at 12. Laptops and other sophisticated electronic devices are no different.

If laptops are to be analogized with something, this Court should find that they are more accurately analogized to the human body. Kindal Wright, *Border Searches in A Modern World: Are Laptops Merely Closed Containers, or Are They Something More?*, 74 J. Air L. &

Com. 701, 722 (2009). Because particularized suspicion is required when an alimentary canal search is conducted, it should be required when a laptop search is conducted as well. *United States v. Arnold*, 533 F.3d 1003, 1007 (9th Cir. 2008). In *United States v. Arnold*, the district court determined that the search of personal information stored on a laptop or other electronic storage device "can be just as much, if not more, of an intrusion into the dignity and privacy interests of a person." *Id*. The court reasoned that these privacy interests were implicated because a laptop or an electronic storage device functions "as an extension of our own memory." *Id*. Laptop searches are invasive in that they expose "vast amounts of private, personal and valuable information." *Id*.

However, this Court need not analogize a laptop to anything in order to provide protection for private information stored on a laptop. As previously noted, laptops are unique and demand particularized suspicion in order to protect the Fourth Amendment rights of their owners. This Court has previously discussed the need "that constitutional projections must evolve with modern technology and social practices." Brief for the Amici Curiae at 24 (quoting *Katz v. United States*, 389 U.S. 347, 352 (1967): "To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication."). Since then, electronic devices have come to play a vital role in modern society, and this Court should recognize and apply constitutional standards as such.

ii. Reasonable Suspicion Is the Appropriate Standard for Customs Agents and Other Law Enforcement Officials to Adopt in Regard to Electronic Devices.

Reasonable suspicion is a standard already used in other warrantless search and seizure situations and, thus, is a standard with which customs agents and other law enforcement agents are already familiar. Customs agents must possess reasonable suspicion of wrongdoing by an individual in order to perform a body-cavity or strip search. *See United States v. Guadalupe-Garza*, 421 F.2d 876, 879 (9th Cir. 1990) (describing the Ninth Circuit's real suspicion

requirement for strip searches at the border); *United States v. Asbury*, 586 F.2d 973, 975-76 (2d Cir. 1978) (stating the Second Circuit reasonable suspicion requirement for strip searches at the border; providing a circuit survey on strip search cause requirements); *United States v. Smith*, 557 F.2d 1206, 1208 (5th Cir. 1977) (stating the Fifth Circuit reasonable suspicion requirement for strip searches at the border).

Arnold recognizes that laptops contain information that convey an individual's private beliefs, thoughts, emotions and sensations. *Arnold*, 533 F.3d at 1007. In *Katz v. United States*, this Court established that "the Fourth Amendment protects people, not places." *Katz v. United States*, 389 U. S. 347, 351 (1967). Justice Brandeis, in his dissenting opinion in *Olmstead v. United States*, noted that "the makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations." *Olmstead v. United States*, 277 U.S. 438, 478-79 (1928) (Brandeis, J., dissenting). An individual's inner thoughts and feelings conveyed into a laptop must be protected because the Fourth Amendment guards people from searches that we, as a society, have come to expect.

Later decisions like *United States v. Ramsey*, allowed the government to search international mail through the border search exception, but required reasonable suspicion *before* a package could be opened; even then, the mail's contents could not be read. *Ramsey*, 431 U.S. at 636. Like the letters in *Ramsey*, electronic documents on laptop computers provide recorded snapshots of the thoughts, beliefs, emotions and sensations of individuals. Electronic documents are the self, captured on a medium, which may change in form over time, but like letters, never in substance. Restricting government access to the medium by requiring reasonable suspicion will protect the individual.

This notion was furthered in *United States v. Cotterman*, where the Ninth Circuit held that a forensic digital border search is nonroutine and requires reasonable suspicion. *United States v. Cotterman*, 709 F.3d 952, 968 (9th Cir. 2013). The court concluded that "the comprehensive and intrusive nature of a forensic examination … trigger[s] the requirement of reasonable suspicion." *Id*. at 962. The majority explained that the "painstaking analysis" involved in the forensic examination, which included copying and searching Cotterman's hard drive in its entirety, including ostensibly deleted files, "is akin to reading a diary line by line looking for mention of criminal activity--plus looking at everything the write may have erased." *Id*. at 962-63.[1] A forensic search provides law enforcement with access to a traveler's information in ways that are quantitatively and qualitatively different from routine border searches of physical belongings, requiring the heightened standard.

iii. Absent Exigent Circumstances, A Significant National Security Interest Is Not Enough to Allow Searches of Electronic Devices Without Reasonable Suspicion.

Historically, exigent circumstances present situations where an exception to the warrant requirement exists. This exception applies when the "exigencies of the situation" make the needs of law enforcement so compelling that a warrantless search is considered to be objectively reasonable under the Fourth Amendment. *Kentucky v. King*, 563 U.S. 452, 460 (2011). In determining whether this exception applies, courts consider imminent harm, imminent destruction of evidence, and pursuing a suspect in certain, fact-specific, situations. *Id*. It is clear

[1] In this case, "Stubbs delivered the electronics to Immigration and Customs Enforcement (ICE) Senior Special Agent & Computer Forensic Examiner Theresa Cullen who was stationed at the border checkpoint. She used forensic software to copy and scan the devices, which typically takes several hours." (R. at 3).

that, here, none of the above-mentioned factors were present. Escaton was detained at the border for several hours and, later, willingly released. (R. at 3).

In *Cotterman*, the Ninth Circuit concluded that the characteristics of a forensic digital search implicate important privacy and dignity interests protected by the Fourth Amendment because of the "uniquely sensitive nature of data on electronic devices". *Id*. at 966. The court rejected *Arnold*'s categorical approach to property searches, finding that what is reasonable under the Fourth Amendment "must account for differences in property." *Id*. Critically, the court also noted that while travelers expect searches of physical property at the border, they do not expect border agents to "mine every last piece of data on their devices or deprive them of their most personal property days" absent *some* particularized suspicion. *Id*. at 967-68.

The government's interest may be heightened by national crises but "reasonableness remains the touchstone" of the Fourth Amendment, even at the border. *Id*. at 966-67. Further, the majority defended the reasonable suspicion requirement as a "modest, workable standard" that law enforcement officials already apply in other contexts. *Id*. at 966. Ultimately, the court concluded that the substantial privacy and dignity interests people have in digital information outweigh the government's interests in conducting a forensic digital border search without any suspicion and we urge this Court to do the same. *Id*. at 967-68.

B. This Court Should Follow the Rationale Here That It Previously Applied in *Riley v. California*.

i. The Balancing Test Applied in *Riley v. California* Serves as a Useful Guide in Evaluating the Government's Interests.

This Court held in *Riley* that police must obtain a warrant before searching the digital information on a cell phone incident to an individual's arrest. *Riley*, 134 S. Ct. at 2495. A search of digital information in a cell phone is categorically different from a search of one's person or physical effects. *Id*. at 2489-91. To determine whether to exempt searches of cell phones incident

to arrest from the warrant requirement, the Court applied a balancing test weighing the state's interests in security and retaining evidence against the individual's privacy interest. *Id*. at 2484-85. The Court concluded that digital information carries substantial privacy interests and, consequently, found that the government's interests in officer safety and preventing the destruction of evidence with regard to digital information are not significant enough to justify a departure from the warrant requirement. *Id*. at 2485-91.

The balancing test mentioned above instructs courts to identify the relevant governmental interests as those that make up the traditional rationale for the exception, rather than the broader array of general law enforcement interests the government claims. *Id*. at 2484. *Riley* also counsels courts to examine the extent to which compliance with the warrant requirement would burden the government's ability to promote its traditional interests at the border. Thomas Mann Miller, *Digital Border Searches After Riley v. California*, 90 Wash. L. Rev. 1943, 1991–92 (2015).

The government has a wide range of interests and obligations at the border, but not all of them justify the border search exception. *Id*. The longstanding rationale for the exception is based on the government's interests in protecting national security, regulating immigration, and preventing the smuggling of people or contraband. *United States v. Flores-Montano*, 541 U.S. 149, 153 (2004); *Ramsey*, 431 U.S. at 620 ("The border-search exception is 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.").

Applied in the present case, the balancing test demonstrates the lack of relevant governmental interests in searching Escaton's electronic devices. The parties agree that no reasonable suspicion existed at the time of the border search. (R. at 6). Officer Stubbs merely saw a paper note on Escaton's laptop with the message "Call Delores (201) 181-0981 $$$." (R.

at 2). Without further context validating a level of particularized suspicion, it was unreasonable for Officer Stubbs to proceed with detention and forensic search of the electronic devices.

Given the intrusiveness of digital searches, courts should adhere to the more specific interests this Court has used to justify the exception and resist conflating the statutory authority of border officials with the traditional justifications for the exception. Miller at 1991. At the border, there should be some nexus between the search and the interests this Court has recognized as the basis for the exception. Miller at 1992.

ii. *United States v. Touset* Is Distinguishable from Escaton's Case.

In May of 2018, the Eleventh Circuit caused a circuit split over whether the *Riley v. California* decision limited the border exception as applied to electronic devices. *See generally United States v. Touset*, 890 F.3d 1227 (11th Cir. 2018). In *United States v. Touset*, the court held that no suspicion is necessary to search electronic devices seized at the border. *Id*. at 1229. There, a defendant's cell phones, camera, laptops, external hard drives, and tablets were inspected at the airport. *Id*. at 1230. The Customs and Border Patrol agent manually inspected the cell phones and camera and returned the devices after finding nothing. *Id*. However, the remaining devices were sent to a computer forensic analyst that later discovered child pornography. *Id*.

In making its decision, the Eleventh Circuit looked to precedent holding that suspicion is not needed to conduct routine searches of the persons and effects of entrants at the border. *Id*. at 1234. The court found that, although this Court had stressed that a search of cell phones risk significant intrusion on privacy, the *Riley* decision did not apply to border searches. *Id*. The panel explained that they found no reason why the Fourth Amendment "would require suspicion for a forensic search of an electronic device when it imposes no such requirement for a search of other personal property." *Id*. at 1233. Alternatively, the panel found that the Customs

and Border Patrol agents had reasonable suspicion to search the defendant's electronic devices. *Id*. at 1237.

By laying out an alternative argument for the border patrol agents' reasonable suspicion in the *Touset* case, the Eleventh Circuit undermines the strength of its decision regarding the application of *Riley*. While the court there was able to state that even if reasonable suspicion was required, it would have been met, there can be no such finding in this case. This is because the parties agree that no reasonable suspicion existed at the time of the border search. (R. at 6). As such, *Touset* is distinguishable from the present case. This Court should consider the opinion in *Riley* over *Touset* and hold accordingly.

II. THE FOURTEENTH CIRCUIT COURT ERRONEOUSLY HELD THAT WARRANTLESS REQUESTS OF ESCATON'S CELL PHONE RECORDS UNDER THE STORED COMMUNICATIONS ACT, 18 U.S.C. 2703(d) DID NOT VIOLATE THE FOURTH AMENDMENT.

The critical error of the Fourteenth Circuit in denying the motion to suppress was the misapplication of the Fourth Amendment principle, which protects the "right of the people to be secure…against unreasonable searches and seizures." U.S. Const. amend IV. When this Court last visited electronic surveillance, it left open the question of both real-time CSLI and "tower dumps" (a download of information on all the devices that connected to a particular cell site during a particular interval)." *Carpenter v. United States*, 138 S. Ct. 2206, 2220 (2018). In light of *Carpenter v. United States*, and concerns of emerging technology's omnipotence as evidence, the Fourteenth Circuit framed the question in this case as the following challenge: "In a post-*Carpenter* world, courts now need to address an individual's Fourth Amendment protection as it applies to historical CSLI requests of six days or fewer and to different methods of requesting CSLI information. Law enforcement's *creativity* lands this case squarely in this territory." Emphasis added. (R. at 11).

This illustration demonstrates the Fourteenth Circuit's approach to *Carpenter*, brushing aside an interpretation that would likely require a warrant, in favor of government "creativity." Weary of arbitrariness, the Fourth Amendment protects "the privacies of life" against "arbitrary power." *Boyd v. United States*, 116 U.S. 616, 630 (1886). This Court recognized that the law should guard against unreasonable searches in new technology: "[W]e hold that 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. Where the third-party doctrine intersects with emerging technology, the Fourth Amendment should not fall prey to creativity to reset an arbitrary line.

The Fourteenth Circuit's argument had three points which, for several reasons, are misconstrued and demonstrate error. First, the court argued that *Carpenter* only placed limits on government requests for "historical CSLI" under six days. (R. at 11). Second, the court found that only more than seven days of historical CSLI violates a person's expectation of privacy. (R. at 12). Third, the court asserted that tower dumps do not provide a chronicle of an individual's movements. (R. at 13).

The Fourteenth Circuit was incorrect in finding that the cumulative hours of law enforcement requests fell within the constitutional limits deemed appropriate in *Carpenter*. Furthermore, the nature of historical CSLI is unconstitutional because it enables continuous surveillance. Unlike the characterization that tower dumps are only generalizable, the information in this case was highly-specific. Lastly, the circumstances of the ongoing investigation in this case did not rise to meet the standards of the "exigent circumstances" exception. Thus, error of law is present throughout the Fourteenth Circuit's ruling and requires this Court to reverse.

A. The Fourteenth Circuit Was Incorrect in Finding That the Cumulative Hours of Law Enforcement Requests in This Case Fell Within the Constitutional Limits Deemed Appropriate in *Carpenter*.

The Government may compel a wireless carrier, under the Stored Communications Act, to disclose records of cell phone communications where law enforcement provides "specific and articulable facts show 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." 18 U.S.C. § 2703(d). The standard under the Stored Communications Act is below the probable cause requirement of the Fourth Amendment. *Id.* "Law enforcement need only show that the cell-site evidence might be pertinent to an ongoing investigation – a "gigantic" departure from the probable cause rule…". *Carpenter*, 138 S. Ct. at 2221. Therefore, an order issued under Section 2703(d) of the Act is not a mechanism for simply accessing historical cell-site records. "Before compelling a wireless carrier to turn over a subscriber's CSLI, the government's obligation is a familiar one – get a warrant." *Id.*

Accordingly, the sum total of cell phone records requested under the Stored Communications Act require a warrant. Without one, Escaton's Fourth Amendment rights to a reasonable expectation of privacy were violated because the cumulative searches exceeded seven days. Justice Thomas, dissenting in *Carpenter*, argued that while "access to seven days' worth of information does trigger Fourth Amendment scrutiny…Why is the relevant fact the seven days of information the government asked for instead of the two days of information the government actually saw? Why seven days instead of ten or three or one...We do not know." *Carpenter*, 138 S. Ct. at 2266–67. The Framers' intention was "to place obstacles in the way of a too permeating police surveillance." *United States v. Di Re*, 332 U.S. 581, 595 (1948). Thus, the majority "kept this attention to Founding-era understandings in mind when applying the Fourth Amendment to innovations in surveillance tools." *Carpenter*, 138 S. Ct. at 2214.

i. The Fourteenth Circuit Mischaracterizes the Standard in Favor of Law Enforcement Creativity; Cumulative Searches Violate the Fourth Amendment.

The danger of circumventing the Fourth Amendment arises from within the court's own misguided interpretation of *Carpenter*. "[L]ower courts and law enforcement would be forced to repeatedly answer the same question that purportedly decided, yet on iteratively smaller scales, a legal matryoshka doll." (R. at 11-12). Here, the Fourteenth Circuit conflates the analysis of *Carpenter* with the complexity of CSLI technology itself. Thus, Circuit Judge Weber, in dissenting, correctly points out the majority's flawed conclusion: "[u]nder the majority's logic, law enforcement can request one hour of CSLI a day for 168 consecutive days." (R. at 16).

The broad nature of this standard should be readily recognized, as the unstated rationale for law enforcement's searches was to avoid the warrant requirement altogether. "Law enforcement, therefore, limited the request to business hours in a transparent effort to circumvent the seven-day period forbidden in *Carpenter*." (Weber, J., dissenting at 16). Here, the government met the Stored Communications Act's standard, a lesser standard than probable cause, in each of its requests. The CSLI acquired from the tower dumps does not require a warrant. But the *creativity* of law enforcement mechanisms, taken together, *should* require a warrant subject to the Fourth Amendment.

Each of the successive requests by the Government under the Stored Communications Act built upon the previous. First, the Government compelled tower dumps of one hour (30 minutes prior and after the attacks) for each ATM – a total of three hours – in order to match the petitioner's phone number to those locations. Second, the Government applied for and was granted a court order for the Three-Day CSLI on the basis of those tower dumps. Third, the Government sought CSLI records for the Weekdays of October 1 to October 12, from 8 AM to 6 PM, a total of 100 hours (ten days multiplied by ten hours, Monday through Friday). Each of

those warrantless searches alone may be sufficient to satisfy *Carpenter*, but cumulatively they do not. Creativity is not sufficient to escape the Fourth Amendment.

ii. This Court Should Decline to Extend the Flawed Analysis Utilized by the Fourteenth Circuit in Parsing the Math in Determining Whether the Cumulative Searches Exceeded the Seven-Day Limit.

A liberal interpretation by this Court should still reverse the lower court and require the government to obtain a warrant for Escaton's CSLI. To begin, the majority of the Fourteenth Circuit correctly points out that Weekday Records in this case only reflect a total of 100 hours, from 8 AM to 6 PM, added together. "[Escaton] argues that the 10-day request is a per se violation of *Carpenter*. The particular request, however, only amounts to 100 hours." (R. at 11, footnote 14).

The point of contention is not the 100 hours, but the cumulative hours requested under the SCA. The tower dump, three-day, and weekday requests for CSLI viewed collectively amount to 172 hours. Although each of the government's requests arguably do not require a warrant standing alone, it defies logic to hold separate segments should count separately. As the majority concedes, "the Court [in *Carpenter*] determined that it was the *accumulation* of seven days of records that violated a person's expectation of privacy. We follow that determination." Emphasis added. (R. at 12). The selectivity that the court is willing to engage in constitutes reversible error. Therefore, taken together, the Weekday Records and the Three-Day Records reflect 172 total hours of information and are subject to a warrant requirement.

The Government lawfully has obtained third-party records from the cell tower in the tower dumps. Those tower dumps were the basis for the Three-Day records and are conterminous with at least three hours of those records. A liberal approach to this argument might be: excise the 3 hours of lawfully obtained third-party information (post-hoc), in order to attempt to fulfill the *Carpenter* 168-hour requirement. In so doing, 3 hours subtracted from 172

equals 169 hours. Nevertheless, allowing the Government to do this math has two enormous implications: first, the individual CSLI obtained from Devos Wireless (Escaton's wireless carrier) the cell tower dumps are, in fact, discrete types of evidence. Tower dumps and CSLI are not identical. Second, under this standard, a series of lawfully obtained third-party searches could be added together and, in order to avoid Fourth Amendment concerns, excised from the whole. This opens the flood gates to unconstitutional searches in favor of creativity.

B. The Powerful Nature of Historical CSLI As Circumstantial Evidence Is Unconstitutional Because It Enables Continuous Surveillance.

i. Congressional Inaction Is Not Persuasive, And Deference to Congress on A Future Amendment to the Stored Communications Act Does Not Prohibit This Court From Applying the Proper Standard.

The Fourteenth Circuit committed error by relying on the possibility of future Congressional amendments to the Stored Communications Act. "[T]he Senate has a current bill to amend the Stored Communications Act to require a search warrant for geolocation data among other amendments…we find it would be proper to defer to Congress to determine the appropriate standard." (R. at 12). The opinion then then cited to the future enactment of the Electronic Communications Privacy Modernization Act of 2017 ("ECPA") for support. *Id.* But this Court has often observed that Congressional inaction is unpersuasive. *Girouard v. United States,* 328 U.S., 61, 69 (1946) ("It is at best treacherous to find in congressional silence alone the adoption of a controlling rule of law"); *Johnson v. Transportation Agency*, 480 U.S. 616, 672 (1987) (Scalia, J. dissenting) ("vindication by congressional inaction is a canard"); *Helvering v. Hallock,* 309 U.S. 106, 129-32 (1940). ("to explain the cause of non-action by Congress when Congress itself sheds no light is to venture into speculative unrealities"); *see also* William N. Eskridge, Jr. *Interpreting Legislative Inaction*, 87 Mich. L. Rev 1, 92-3 (1989). Therefore, this Court should not wait for the Congress to interpret the law under existing precedent Fourth Amendment.

The necessity of applying the current rule is articulated by Circuit Judge Weber's dissent which illustrates the issue that arises with historic CSLI: "[L]aw enforcement does not even need a subject in mind before it creates a record of a person's location." (R. at 16). In *Carpenter*, a suspected group of accomplices was linked to robberies of six RadioShack and T-Mobile stores in Detroit, Michigan that extended to Warren, Ohio. Historic CSLI led to the investigation of numerous similar robberies in the area over a span of seral years and without the historic CSLI, the government "did not know all of these details in 2011". *Carpenter*, 138 S. Ct. at 2225 (Kennedy, J., dissent). The government overcame geographic "dispersion" of the crimes, by utilizing "cell-site records uniquely suited to this task" as "powerful circumstantial evidence." *Id.*

The majority in *Carpenter* presented the conclusion clearly: "police need not even know in advance whether they want to follow a particular individual, or when… because location information is continually logged for all of the 400 million devices in the United States—not just those belonging to persons who might happen to come under investigation—this newfound tracking capacity runs against everyone." *Carpenter*, 138 S. Ct. at 2218. Thus, it is perhaps historical CSLI presents the greatest threat to privacy as it may never disappear.

ii. <u>The Location and Proximity of Cell Towers Can Reveal Significant Information About an Individual at Various Levels of Generality.</u>

Not all cell towers should be treated alike by the law because not all cell towers are alike. As an illustration of this point, the two cell towers in this case present a distinguishable example. First, there are the cell towers in the suburban town of Escalate, and secondly, the cell towers in densely populated Sweetwater, West Texas. Escalante's towers are located across broad territory, which provide information in "five-to-ten-minute increment…only accurate within 1000 feet of the individual." (Hale, Aff. ¶12, P. 4). If those were the only cell towers at issue, then the Fourteenth Circuit's characterization is fair, that "unlike the days of CSLI, this

information does not reveal detailed information about a person's life." (R. at 14). But there are also the Sweetwater towers, covering an area larger than San Diego, that "capture…five-to-ten-minute increments within 50 feet of the location of the phone" (Hale, Aff. ¶11, P. 3). Because the Sweetwater towers are physically smaller and located on tall buildings, they "locate individuals on a given floor or room of a building…often more accurate" than GPS. *Id.*

Given these examples, this Court should recognize that the cell tower dumps are capable of providing general and specific information about an individual. Here, the Fourteenth Circuit committed clear error when it misread the fact that the cell towers do offer a specific information about an individual. "[A] detailed chronicle of a person's physical presence compiled every day, every moment, over several years…implicates privacy concerns far beyond those considered in *Smith* and *Miller*." *Carpenter*, 138 S. Ct. at 2220. This Court has indicated that such a chronicle is significant beyond precedent. *Id*. Thus, while Escaton's movements were captured, the fact that the co-defendant's movements were only confirmed by Escaton's CSLI points to the significance of this evidence beyond, but also to their known associates. (R. at 5).

iii. Case-Specific Circumstances That May Support A Warrantless Search Are Inapplicable Because None of The Factors of Exigency Were Present.

Exigent circumstances may be a situation where an exception to the warrant requirement exists. "One well-recognized exception applies when the "exigencies of the situation" make the needs of law enforcement so compelling that [a] warrantless search is objectively reasonable under the Fourth Amendment.'" *Kentucky v. King*, 563 U.S. 452, 460 (2011). Among the factors the Court considers relevant to exigent circumstances are imminent harm (e.g. bomb threats), imminent destruction of evidence, and pursuing a suspect in certain

"fact-specific" situations that "likely" justify the warrantless collection of CSLI.[2] *Carpenter*, 138 S. Ct. at 2206; *Kentucky,* 563 U.S. at 460 (quoting *Mincey v. Arizona*, 437 U.S. 385, 394 (1978)). The record indicates that Escaton was detained at the border for several hours. (R. at 3). None of the factors in the present case would arguably fall under the exigent circumstances doctrine.

[2] "Such exigencies include the need to pursue a fleeing suspect, protect individuals who are threatened with imminent harm, or prevent the imminent destruction of evidence." *Kentucky*, 563 U.S., at 460.

CONCLUSION

As explained herein, the Fourth Amendment demands reasonable suspicion to conduct forensic searches of electronic devices at border crossings. Furthermore, the CSLI, collectively, exceeded the seven-day limit placed by this Court in *Carpenter*, violating Escaton's Fourth Amendment rights. We hereby ask this Court to reverse the ruling of the Fourteenth Circuit Court of Appeals.

Dated: February 10, 2023

Respectfully submitted,
Attorneys for Petitioner