Docket No. 10-1011

In the

SUPREME COURT OF THE UNITED STATES

HECTOR ESCATONH,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Writ of Certiorari to the
Supreme Court of the United States

BRIEF FOR RESPONDENT

Team R8
Counsel for Respondent

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Supreme Court Cases

Circuit Court Cases

District Court Case

Other Authorities

QUESTION PRESENTED

I. Whether the Fourth Amendment requires that government officers must have reasonable suspicion before conducting forensic searches of electronic devices at an international border.

II. Whether 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*, 585 U.S. __ (2018).

OPINION BELOW

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

COSTITUTIONAL PROVISIONS AND RULES

The Fourth Amendment of the U.S. Constitution:

"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.

§ 2703 Required disclosures of customer communications and records:

(d) A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and

articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

18 U.S.C. § 2703 (d) (West).

INTRODUCTION

This Court should affirm the decision of the Fourteenth Circuit because it correctly held that the Fourth Amendment does not require reasonable suspicion to conduct forensic searches of electronic devices at international borders and does not apply to the use of historical cell-site location information requests for fewer than seven days.

The Petitioner was convicted of bank fraud, conspiracy to commit bank fraud, and aggravated identity theft. He now timely appeals from the Fourteenth Circuit's ruling, arguing that the court erred in denying his motion to suppress because the forensic search of his electronic devices and CSLI requests violated his Fourth Amendment right to be free from unreasonable searches and seizures.

The Fourteenth Circuit properly held that emerging technology has not escaped Fourth Amendment scrutiny when the search and seizure occur at the border. The Fourth Amendment commands that searches and seizures be reasonable. What is reasonable depends upon balancing the intrusion on the individual's Fourth Amendment interests against the promotion of legitimate governmental interests.

Additionally, the Fourteenth Circuit properly held that the broad contours of the scope of searches at our international borders are rooted in the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country. Historically such broad powers have been necessary to protect the integrity of the border from the entry of contraband. Ordinarily, searches at the border are reasonable simply because they occur at the border, and therefore, require no showing of reasonable suspicion. Furthermore, because the government has a heightened interest in preventing the entry of unwanted persons and effects across the international border, the expectation of privacy at the border is significantly diminished compared to the interior. Moreover, the Fourth Amendment does not guarantee the right to travel without great inconvenience.

Due to technological advancement, concealing contraband only heightens the need of the government to search property at the border. To hold otherwise would allow digital contraband a pass, no matter how potentially dangerous, while physical property still remains subject to penetrating searches.

Furthermore, the Fourteenth Circuit also properly affirmed the district court's order permitting cell-site location information (CSLI) and tower dump records because *Carpenter* and the Stored Communications Act permitted these requests. Congress regulates these new and complex technologies, and it clearly balanced privacy with security upon finding that citizens' interest in public safety outweighs their interest in certain stored communications. Where wireless carriers can provide records to promote public safety, they should do so under judicial guidance and a court order.

In *Carpenter* the Court held that SCA requests for more than seven days or 168 hours require a warrant. This means that requests for fewer than seven days do not require a warrant and may be obtained by court order. However, the Court did not address tower dumps. It expressed no reason why citizens might have a reasonable expectation of privacy in their number appearing on a list of geographically related numbers from a cell tower. Because Respondent never requested an order for more than 100 hours of Petitioner's CSLI and precedent approves of tower dumps, the Court should affirm the Fourteenth Circuit's order denying the motion to suppress.

Lastly, Respondent met Petitioner's reasonable expectation of privacy in the whole of his physical movements because it tailored its requests to the short-term and to locations relevant to the investigation. Very few towers were utilized in this request because the requests targeted only towers near the infiltrated bank branches. This produced a relatively fixed location of the search and did not create an "intimate window" into Petitioner's personal life. Ultimately, Petitioner did not have a reasonable expectation of privacy in any of the information that his wireless carrier provided to police, and this information was indispensable to find a suspect and corroborate other evidence in the investigation.

STATEMENT OF THE CASE

I. Statement of Facts

On September 25, 2019, Hector Escaton ("Petitioner") returned to the United States from Mexico through a West Texas border checkpoint. R. at 2. Customs and Border Protection (CBP) Officer Ashley Stubbs ("Officer Stubbs") conducted a routine border search of Petitioner's vehicle and found three large suitcases in the back of his car. *Id*. After subsequent search of Petitioner's suitcases, Officer Stubbs found an iPhone, a laptop, three external hard drives, and four USB[1] devices. *Id.* Officer Stubbs placed the iPhone on airplane mode, ensured the laptop was disconnected from wireless service, and manually searched both devices without assistive technology. *Id.* He then also noticed a paper note which was placed just below the keyboard of the laptop with the message "Call Delores (201) 181-0981 $$$." R. at 2-3. Officer Stubbs recorded the message and the iPhone telephone number and returned the phone to Petitioner, but detained the laptop, hard drives, and USB devices. R. at 3. No passwords were needed to open the devices, but certain folders on the laptop and the contents of USB devices were password protected. *Id.*

Officer Stubbs then delivered the electronics to Immigration and Customs Enforcement (ICE) Senior Special Agent & Computer Forensic Examiner Theresa Cullen ("Forensic Examiner") who was stationed at the border checkpoint and used forensic software to access the contents of Petitioner's devices. *Id.* Upon examining Petitioner's devices, Forensic Examiner

[1] USB refers to any device that can store data in flash memory with USB integrated interface. Flash drives, external hard drives, digital cameras and scanners are a few examples of USB devices. https://www.cleverfiles.com/howto/what-is-usb-device.html

found that the laptop held documents containing individuals' bank account numbers and pins. *Id.* The forensic analysis also revealed that the USB devices contained traces of malware. *Id.* She reported her findings to Officer Stubbs, who then notified the Federal Bureau of Investigation (FBI) Special Agent Catherine Hale ("Agent Hale"), who had been investigating "ATM skimming"[2] of Mariposa Bank ATMs in Sweetwater during October of 2018. *Id.*

On October 13, 2018 an ATM engineer determined that the Sweetwater Mariposa Bank branch ATM at Boswell sweet had been cut open and infected with USB malware that read users' information. *Id.* An immediate internal investigation by a nation-wide bank—Mariposa Bank—revealed that skimming occurred at five Mariposa ATMs in Sweetwater—two with foreign skimmers, two with USB malware, and one with sophisticated USB malware—and three Mariposa ATMs in the neighboring city, Escalante. R. at 3-4. The investigation revealed that the skimming occurred during early October, 2018, but security surveillance was only available from the three Sweetwater ATMs that had been infected with malware. R. at 4. The surveillance photos from the Escalante ATMs were destroyed by a malfunction during the investigation. *Id.* USB malware is particularly dangerous because it allows fraudulent cash withdrawals in addition to identity theft. R. at 3. Mariposa Bank estimated that the skimming resulted in $50,000 of losses from cash withdrawals and hundreds of identities stolen from Mariposa Bank customers. R. at 4.

[2] ATM skimming is a criminal activity that costs U.S. banks hundreds of millions of dollars annually and affects thousands of bank customers. Skimming technology varies from crude to complex. It can be done by "shoulder surfing"—standing behind a customer when they enter their pin. Another tactic involves "skimmers" reading information from debit cards as they enter ATM card readers. Criminals may also infect ATM terminals by uploading malware from USB devices. Malware-laden ATMs collect customer bank account numbers and pins. With this information, criminals create fake credit and debit card accounts or directly withdraw funds from ATM terminals using existing accounts.

Mariposa Bank reported these findings to Agent Hale, including the malware used in the Sweetwater ATMs and the surveillance photos with images of a man in a black sweatshirt. *Id.* Agent Hale requested and received three Stored Communications Act (SCA) tower dumps for 30 minutes before and 30 minutes after the man in the black sweatshirt approached each ATM. *Id.* A tower dump consists in a list of every phone number that used a tower. *Id.* Agent Hale matched Petitioner's phone number to a number in the tower dump. *Id.* Petitioner's USB malware was similar to the malware used at the infiltrated Sweetwater ATMs, although it was not identical. *Id.*

Agent Hale applied for a court order under the SCA to obtain Petitioner's cell phone records, cell-site location information (CSLI). *Id.* A federal magistrate judge issued the order directing Delos Wireless to disclose Agent Hale's records from October 11, 2018 through October 13, 2018 (Three-day Records). *Id.* These hours totaled 72. *Id.* The records only placed Petitioner in the area of the Sweetwater Boswell Branch ATM on October 12. *Id.*

Still seeking to find the identity of the man in the black sweatshirt, Agent Hale requested another SCA court order. *Id.* Agent Hale developed the theory that an additional suspect, Delores, had abetted the skimming. *Id.* The federal magistrate judge issued the additional order for Petitioner's and Delores's weekday phone records during the hours 8 AM MDT and 6 PM MDT from October 1 to 12. *Id.* These hours totaled 100 for Delores. *Id.* For Petitioner, these hours totaled 80 new hours because 20 hours from October 11 and 12 overlapped with the previous request. *Id.* Agent Hale selected business hours because the ATMs are located within the Bank's entryway that is locked outside of business hours. *Id.*

These records revealed Delores Abernathy's surname, phone number, and placed her in the area of the Escalante ATMs. *Id.* The records also placed Petitioner with Abernathy at the relevant times under the Boswell Street investigation. *Id.* Abernathy was indicted, and her home was searched pursuant to a warrant. *Id.* This search revealed cash, and the same malware that Petitioner stored on his USB devices. R. at 5. Delores was arrested and entered a plea agreement, cooperating with Respondent in its case against Petitioner. R. at 5-6.

II. Procedural Posture

The Government indicted Petitioner for 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. Prior to trial in the District of West Texas, Petitioner filed a motion to suppress the results of the forensic search and the cell-site data requested from Delos Wireless. *Id.* The district court denied the motion on both issues. *Id.* Following a jury trial, Petitioner was convicted on all charges, and he now appeals. *Id.* The Petitioner now asks this Court to review the Fourteenth Circuit's legal conclusions under the *de novo* standard and its factual determinations for clear error because motions to suppress involve mixed questions of fact and law.

ARGUMENT

I. THE FOURTH AMENDMENT DOES NOT REQUIRE REASONABLE SUSPICION TO CONDUCT FORENSIC BORDER SEARCHES OF ELECTRONIC DEVICES BECAUSE GOVERNMENT INTEREST IN PROTECTING THE INTEGRITY OF ITS BORDERS OUTWEIGHS ANY PRIVACY INTERESTS OF TRAVELERS.

In the era of technological advancement, the Internet, cellular phones and computers, and Universal Serial Bus (USB) devices, have become the pervasive and insistent part of the daily life of many Americans, and they have changed the way we communicate, transmit and store information. *Riley v. California,* 134 S. Ct. 2473, 2484 (2014). In her concurrence in *United*

States v. Jones, Justice Sotomayor properly noted that technology "may alter the relationship between citizen and government in a way that is inimical to democratic society." *United States v.* Jones, 565 U.S. 400, 416 (2012). Thus, the courts had to redefine constitutional rights of individuals, absent the precise guidance from the founding era, on the scope of the border searches in the modern digital era. *Riley* at 2484.

Since the founding of our Republic, 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. Reasonableness is "'the ultimate touchstone of the Fourth Amendment,'" *Riley* at 2482. (quoting *Brigham City v. Stuart*, 547 U. S. 398, 403 (2006)), and it requires obtaining a search warrant based on probable cause, unless the search falls within specific exceptions to the warrant requirement. *Riley* at 2482; *See Kentucky v. King*, 563 U. S. 452, 459-60 (2011) (identifying exceptions to the warrant requirement); *United States v. Ramsey*, 431 U.S. 606, 622 (1977) (explaining that border searches fall under the border search exception to the warrant requirement). Congress has granted the Executive plenary power to conduct routine forensic searches at the border without requiring the showing of reasonable suspicion or probable cause to obtain a search warrant, thereby giving rise to the border-search doctrine. Act of July 31, 1789 ch. 5, § 24, 1 Stat. 29, 43. *See also Ramsey* at 616-17, 619 (reaffirming the longstanding recognition of border searches without the requirement of probable cause or warrant); *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985) (holding that "routine searches of persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant."). *But see Riley* at 2495 (holding that a search warrant was required to search digital information on a cell phone when it was seized incident to arrest for traffic violation).

i. Border searches fall under the border search exception to the warrant requirement and hence require no showing of reasonable suspicion.

Border searches have long been deemed reasonable by virtue of the fact that the search occurred at the border. *See United States v. Flores-Montano*, 541 U.S. 149, 153 (2004) (holding that the removal, dismantle, and reassembly of the gas tank at the international-border port of entry was reasonable). Border searches are further reasonable "by the single fact that the person or item in question had entered into our country from outside," *See Ramsey* at 619, 622 (holding that the search of the contents of international mail falls under the "border search" exception because it is "neither 'unreasonable' nor 'embraced within the prohibition of the [Fourth] [A]mendment.'"). Indeed, the sovereign has an elevated interest in protecting the American people from the entry of unwanted persons and illegal contraband by stopping and examining them as they cross the border. *Id.* at 616, 620.

The Fourteenth Circuit was correct in applying these well-settled principles. Similarly to border searches in *Ramsey* and *Flores-Montano*, the search of Petitioner's property occurred upon the entry into the United States from Mexico at the international physical border-port of entry, where Customs and Border Protection (CBP) was authorized to search the Petitioner's vehicle and its contents. R. at 2. In *Ramsey*, Customs officials not only seized incoming international mail from Thailand, but also opened it and searched its contents. *Ramsey* at 607,609. The Supreme Court held that Customs officials had the power to "characteristically inspect luggage and their power [to do so was] not questioned. *Id.* at 618. In *Flores-Montano*, Customs inspector stopped the vehicle at an international-border port entry in southern Carolina and searched not only the contents inside the vehicle, but also the vehicle's gas tank, which was subsequently disassembled and reassembled. *Flores-Montano* at 150-51. The Supreme Court

held in both cases that the border search was reasonable—especially when it yielded no damage to the property—and therefore, required no showing of reasonable suspicion. *Id.* at 155-56.

Although *Ramsey* and *Flores-Montano* do not *per se* govern border searches of electronic devices, they nonetheless, provide better guidance on the scope of the border searches in the modern digital era than *Riley* because inland searches away from the border are a different matter. *See Riley* at 2495 (holding that reasonable suspicion was required to search digital information on a cell phone that was seized incident to arrest for a traffic violation). Absent **a** declaratory precedent governing border searches of electronic devices, the courts have struggled to define how the Fourth Amendment applies to border searches of digital information. *See United States v. Touset*, 890 F.3d 1227, 1229, 1233 (11th Cir. 2018) (holding that a "suspicionless" search of the cell phone was reasonable because the Fourth Amendment does not require reasonable suspicion to search personal property at the border); *But see United States v. Kolsuz*, 890 F.3d 133, 140 (4th Cir. 2018) (holding that reasonable suspicion was required to search the cell phone when there was "temporal and spatial distance between the off-site"); *United States v. Cotterman*, 709 F.3d 952, 967 (2013) (holding that mining "every last piece of data" on the defendant's laptop at the border search required reasonable suspicion).

The facts of the present case align better with the holding in *Touset*, which relied heavily on the holdings of *Ramsey* and *Flores-Montano*, because the search of Petitioner's electronic devices occurred at the international border, rather than sometime off-site like in *Kolsuz*. R. at 2. Thus, Officer Stubbs was within his rights to search not only the Petitioner's vehicle, but also the contents of his electronic devices. R. at 2- 3. Furthermore, the holding in *Cotterman* does not apply because since the Petitioner's laptop and hard drives were password protected, Officer

Stubbs was unable to conduct the routine search of Petitioner's devices, which required the Officer to resort to the help of the forensic examiner. *Id.*

The rule is simple and mentions nothing about the requirement of reasonable suspicion at the border searches: "[p]ersons and merchandise encountered by CBP at the international border are not only subject to inspection under U.S. law; they also have been or will be abroad and generally subject to the legal authorities of at least one other sovereign." U.S. Customs and Border Protection, CBP Directive No. 3340-049A (Jan. 4, 2018), https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBPDirective- 3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf (citing *United States v. Boumelhem*, 339 F.3d 414, 423 (6th Cir. 2003)). To hold otherwise would allow digital contraband a pass, no matter how potentially dangerous, while physical property would still remain subject to penetrating searches. *United States v. Alfaro-Moncada*, 607 F.3d 720, 728 (11th Cir. 2010). Therefore, the border-search doctrine mandates that border searches are reasonable and require no showing that government officers must have reasonable suspicion before conducting forensic searches of electronic devices.

ii. Border searches require no showing of reasonable suspicion because privacy interests of persons entering the United States are diminished at the border

The reasonableness of the longstanding practice of automobile border searches in the United States dates back to 1925, where in *Carroll v. United States*, the United States Supreme Court held that "[t]ravelers may be so stopped in crossing an international boundary because of national self-protection reasonably requiring one entering the country to identify himself as entitled to come in, and his belongings as effects which may be lawfully brought in." 267 U.S. 132, 154 (1925). Reasonableness of the border search is determined by balancing the legitimate government interests against privacy expectations of an individual, where the balance between

the two is struck more favorably to the government at the border. *Montoya de Hernandez* at 540 (finding that "detention of a traveler at the border, beyond the scope of a routine customs search and inspection, is justified at its inception"). The Supreme Court has long adhered to this principle by reasoning that:

> Of what avail would it be that every passenger . . . is compelled to sign a declaration before landing, either that his trunks and satchels in hand contain nothing liable to duty . . . if the mail is to be left unwatched, and all its sealed contents . . . are to be exempt from seizure.

Ramsey at 620 (quoting *Von Cotzhausen v. Nazro*, 107 U.S. 215, 218 (1882)).

The sovereign thus, has the paramount interest in protecting the integrity of international borders by stopping and examining persons and their illegal contraband entering the United States, thereby rendering them with a diminished expectation of privacy. *See Flores-Montano* at 154 (holding that a person's "expectation of privacy is less at the border than it is in the interior."); *Ramsey* at 616, 620 (holding that "[n]ot only is there the longstanding, constitutionally authorized right of customs officials to search incoming persons and goods, but there is no statutorily created expectation of privacy" at the border). *But see Montoya de Hernandez* at 540-41 (holding that "nonroutine" border searches that involve monitoring of the bowel movement of an alimentary canal smuggler required reasonable suspicion).

Those who cross physical borders into the United States expect that they will be subjected to the search and seizure of their persons and effects, just as they would be, should they enter into the United States through a non-physical border at the airport. *See Almeida-Sanchez v. United States*, 413 U.S. 266, 272-73 (1973) (holding that "suspicionless" searches and seizures are reasonable at border's "functional equivalent"—airport); *United States v. Thirty-Seven Photographs*, 402 U.S. 363, 376 (1971) (holding that a traveler's "right to be let alone neither prevents the search of his luggage nor the seizure of unprotected, but illegal, materials

when his possession of them is discovered during . . . a search" at the airport); *Alfaro-Moncada*, 607 F.3d at 732 (reasoning that when travelers cross a border they are on notice that a search will occur).

The facts of the present case illustrate the reasonableness of the search of Petitioner's electronic devices because just like privacy interests of travelers in *Flores-Montano* and *Ramsey*, Petitioner's privacy interests were diminished by the virtue of the fact that the search occurred at the border. R. at 3; *See also Ramsey* at 619 fn.17 (holding that the search of the contents of the incoming material did not constitute an invasion of privacy); *Flores-Montano* at 154 (holding that the disassembly and reassembly of the fuel tank reasoning that the search was not more of an invasion of privacy than the search of the vehicle's glove compartment). Unlike in *Montoya de Hernandez*, here, Officer Stubbs carefully conducted a routine search of Petitioner's devices, without implicating his dignity by searching the contents of his laptop and hard drives. R. at 3. Moreover, *Montoya de Hernandez* is not applicable here, because that case, involved the border search of the person and not the property. *Montoya de Hernandez* at 540-41.

Despite factual dissimilarity with the present case, the holdings in *Ramsey* and *Flores-Montano* laid the foundation to the issue of privacy at border searches and were applied in *Touset*, which involved the search of the traveler's cell phone at the border. *Touset* at 1230. In that case, the Eleventh Circuit reasoned that "the advent of sophisticated technological means for concealing contraband only heightens the need of the government to search the property at the border." *Id.* at 1235. *But see Cotterman* at 965 (noting that it would be "impractical, if not impossible, for individuals to make meaningful decisions regarding what digital content to expose to the scrutiny that accompanies international travel"); *Kolsuz* at 145 (explaining that it is neither "realistic nor reasonable to expect the average traveler to leave his digital devices at

home when traveling."). The rationale of the Ninth and Fourth Circuits is unpersuasive because a traveler's expectation of privacy is less at the border, and the Fourth Amendment does not guarantee the right to travel without inconvenience. *Touset* at 1235. Indeed, the sovereign has an elevated interest in protecting the American people from the entry of unwanted persons and illegal contraband by stopping and examining them as they cross the border. *Ramsey* at 616. Therefore, because the traveler's privacy interest is not given greater weight at the border, border searches are reasonable and require no showing that government officers must have reasonable suspicion before conducting forensic searches of electronic devices.

II. THE FOURTEENTH CIRCUIT PROPERLY AFFIRMED THE DISTRICT COURT'S ORDER PERMITTING CSLI AND TOWER DUMP RECORDS BECAUSE *CARPENTER* AND THE SCA PERMITTED THESE REQUESTS.

Petitioner respectfully asks the Court to affirm the Fourteenth Circuit's ruling permitting CSLI and tower dump records. Historically, Congress has passed pertinent legislation when new technology required extensive rules to balance citizens' security and privacy interests, such as when it enacted the Omnibus Crime Control Act of 1968. 18 U.S.C.S. § 2510-23. (Lexis 2019). Justices of the U.S. Supreme Court have called on Congress to take such action. *Olmstead v. United States*, 277 U.S. 438, 465-66 (1928).

The U.S. Supreme Court recently declined to "decide whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny." *United States v. Carpenter*, 138 S. Ct. 2208, 2217 n.3 (2018). Instead, the Court held that "accessing seven days of CSLI constitutes a Fourth Amendment search." *Id*. While the Court acknowledged that "fact-specific threats will likely justify the warrantless collection of CSLI," it did not exhaustively delineate exceptional circumstances. *Id*. at 2223.

Furthermore, the Court applied this narrow holding in the context of the SCA that permits a judge to oversee disclosure of telecommunications records when the Government "offers specific and articulable facts showing that there are reasonable grounds to believe… [the records] are relevant and material to an ongoing criminal investigation." 18 U.S.C.S. § 2703 (d) (Lexis 2019).

i. The Court should defer to congress for the appropriate standard because Congress intended the SCA to be comprehensive

The Fourteenth Circuit properly determined that "[i]mposing additional restrictions [on the SCA] would serve an adverse purpose." R. at 12. Congress may enact comprehensive legislation when new technology, privacy, and security intersect and raise public concern. In *United States v. Katz*, the Court applied the legal principle that "'the mandate of the [Fourth] Amendment requires adherence to judicial processes,' and that searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable." *United States v. Katz*, 389 U.S. 347, 357 (1967) (quoting *United States v. Jeffers*, 342 U.S. 48, 51 (1951).

The issue in *Katz* was whether a microphone and recording device attached to the outside of a public telephone booth constituted a 'search' under the Fourth Amendment when the Government did not have a warrant. *Id.* at 350. While this case extended the Fourth Amendment beyond its previous proprietary limitation of tangible items, *Katz* also addressed advancing electronic surveillance. *Id*. at 353-54. A year later, Congress passed the Omnibus Crime Control Act of 1968. 18 U.S.C.S. § 2510-23. "Each application for an order authorizing or approving the interception of a wire, oral, or electronic communication under this chapter shall be made in writing upon oath or affirmation to a judge of competent jurisdiction." *Id*. Since Congress

enacted this comprehensive statute, "the regulation of wiretapping has been governed primarily by statute and not by case law." *United States v. Jones*, 565 U.S. 400, 427-28 (2012).

Today, Congress continues to amend the SCA. R. at 12. This indicates its intent to comprehensively regulate disclosure of stored communications conditioned upon judicial supervision. Unlike *Katz*, here the Court may look to the SCA and utilize a well-reasoned statute that balances security and privacy with complex advancements in electronic surveillance. The Court should defer to Congress for the appropriate, judicially supervised standard.

ii. The government met Petitioner's reasonable expectation of privacy in the whole of his physical movements because it restricted each CSLI and tower dump request to less than 168 hours and locations relevant to investigation,

When the Government obtains electronic surveillance information, a relevant factor is whether the electronic device was in a fixed location that could not produce an "intimate window into the person's life, revealing his political, professional, religious, and sexual associations." *United States v. Kay*, No. 17-CR-16, 2018 WL 3995902, at **1, 7 (D. Wis. Aug. 21, 2018) (internal citations omitted). Long-term GPS monitoring may also contribute to "a degree of intrusion that a reasonable person would not have anticipated." *Jones*, 565 U.S. at 430. Tracking technology requires a Fourth Amendment analysis particularly when Congress has not enacted a regulating statute. *Id*.

Analysis of CSLI requires additional factors such as whether the records exceed an individual's "reasonable expectation of privacy in the whole of their physical movements. *Carpenter*, 138 S. Ct. at 2219. CSLI records will likely require a Fourth Amendment standard if they reach GPS-level precision. *Id.* The same requirement applies if the records include seven days or more of CSLI. *Id*. at 2217 n.3. Additionally, CSLI collected from urban cell towers raise more suspicion than rural cell towers because of the higher level of precision attributed to urban

towers. *See id*. at 2225 (Kennedy, J., dissenting) (noting that rural cell towers can be up to forty times more imprecise than urban cell towers). Finally, analysis of CSLI considers whether the records were used to corroborate information from an ongoing investigation. *United States v. Pembrook*, 876 F.3d 816, 818-19 (6th Cir. 2017).

In *United States v. Carpenter*, the Court analyzed CSLI records as applied to two request for 127 days and seven days of records that included several cell towers ranging from Michigan to northeastern Ohio. 138 S. Ct. at 2212, 2218. The government did not obtain a warrant, and it used the SCA and two orders from Federal Magistrate Judges to obtain the records from the wireless carrier. *Id*. at 2210, 2212. The Court held that "accessing seven days of CSLI constitutes a Fourth Amendment search." 138 S. Ct. at 2217 n.3.

A recent opinion from the Sixth Circuit addressed CSLI and tower dumps collected under the SCA. *Pembrook*, 876 F.3d 823. The government sought to corroborate surveillance videos of robberies with cell tower dumps from the locations of two robberies because the two suburban locations had potential to "reveal a common [cell phone] number that was active at each location around the time of the crime…[to] aid in identifying potential suspects involved in the robberies." *Id*. at 816, 823. Additional corroborating evidence included DNA testing, ballistic evidence, witness statements, a trail of blood drops, a credit card, time-stamp calls made by the number, and a Driver's License number. *Id.* at 816-18 n.5. The court permitted this use of cell tower dumps. *Id*. at 824.

United States v. Knotts and *United States v. Kay* both stand for the proposition that electronic surveillance does not violate a person's reasonable expectation of privacy when it has a limited use outside the private sphere and involves a fixed location. In *Knotts*, the government installed a radio frequency beeper on an object that the defendant bought, placed in his vehicle,

and transported to his secluded, illegal drug lab. *United States v. Knotts*, 460 U.S. 277, 277-79 (2018). The government used the beeper intermittently to supplement additional surveillance tools. *Id*. at 278-79. In holding this warrantless act to be legal, the Court noted the "limited use which the government made of the signals from this particular beeper." *Id*. at 284-85.

Similarly, in *Kay*, the Court permitted the government's use of surveillance technology, a pole camera placed outside the defendant's home during a drug trafficking investigation. *Kay,* 2018 WL 3995902, at *1, 8. The Court noted that the scope of surveillance permitted by the camera was relevant to the Fourth Amendment, there was "no indication that the camera recorded all activities occurring within the curtilage of home." *Id*. at 7 n.3. Law enforcement used the pole camera to corroborate other evidence such as cell phone records and placing known suspects at the residence, but the camera could not determine any particulars around the house such as the license plates of vehicles in defendant's driveway. *Id.* at 7 n.2.

Here, unlike *Carpenter*, *Kay*, and *Pembrook*, each of Respondent's information requests encompassed fewer than seven days or 168 hours of information about Petitioner. Distinctly, Petitioner's information was fragmented in one of the requests for only business hours that clearly prevented Respondent from crossing the line into Petitioner's reasonable expectation of privacy in the whole of his movements. Like *Kay*, Respondent's use of the surveillance technology was intermittent and limited.

Respondent used these tools in addition to its full investigation that included surveillance footage and an additional witness. Similar to *Knotts*, *Kay*, and *Pembrook*, the use of these surveillance tools in an active investigation was permissible.

Here, the use of tower dump information fits within the court's analysis in *Pembrook*. No personal information was revealed, and there is no indication that the list of cell phone numbers

revealed Petitioner's location in a private residence. Regarding CSLI information, these facts fit squarely within the seven-day rule from *Carpenter* because the number of hours of each request was fewer than seven days. The factors that the Court considers in *Carpenter* weigh in favor of Respondent because of the relatively fixed and intermittent nature of the surveillance, and the corroborative value of the evidence.

CONCLUSION

For the foregoing reasons, we respectfully ask this Court to affirm the Fourteenth Circuit's holding in regards to both issues.

Respectfully submitted,
Attorneys for Respondent