No. 10-1011

In the Supreme Court of the United States

Hector Escaton,
Petitioner

v.

United States of America,
Respondent

ON WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE FOURTEENTH CIRCUIT

BRIEF FOR RESPONDENT

R10, *Attorneys for Respondent*

TABLE OF CONTENTS

TABLE OF AUTHORITIES

United States Supreme Court

United States Court of Appeals

United States District Court

State Court

Constitutional Provisions

Statutes

QUESTIONS PRESENTED

I. Under the Fourth Amendment, must government officers have reasonable suspicion before conducting forensic searches of electronic devices at an international border?

II. Following *Carpenter v. United States*, 138 S. Ct. 2206 (2018), do the government's acquisitions pursuant to 18 U.S.C. § 2703(d) of cell-site location information collected from cell tower dumps, three days of cell-site location information, and one-hundred cumulative hours of cell-site location information over ten days violate the protections guaranteed by the Fourth Amendment?

OPINION BELOW

The opinion of the United States Court of Appeals for the Fourteenth Circuit is reported 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

Summary of the Argument

Respondent, United States of America, Appellee in *Escaton v. United States*, 1001 F.3d 1341 (14th Cir. 2017), before the United States Court of Appeals for the Fourteenth Circuit, respectfully submits this brief on the merits and asks this Court to affirm the Fourteenth Circuit's decision.

The Fourteenth Circuit correctly decided the two issues presented in this case. First, that the Fourth Amendment does not require reasonable suspicion for forensic searches of electronic devices at the international border. Second, that Respondent's acquisitions pursuant to 18 U.S.C. § 2703(d) of the cell-site location information from cell tower dumps and from records provided by Delos Wireless did not violate the Fourth Amendment following *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

The Fourth Amendment does not require reasonable suspicion for forensic searches of electronic devices at the border. The Fourth Amendment generally requires obtaining a warrant before conducting a search, but there are certain exceptions to this requirement. A border search is one historically recognized and prevailing exception. The border search exception allows the government to search individuals entering or exiting the country without reasonable suspicion. This exception is based on the sovereign's inherent authority to protect its people by controlling who and what comes into the country.

In border searches, the government interest is weighed against an individual's expectation of privacy. Individuals crossing the border have a low privacy expectation that is significantly outweighed by the government interest. Therefore, border searches require no level of suspicion and are considered per se reasonable simply because they take place at the border. The search of Petitioner's electronic devices took place at the international border, so the border search

exception applied. Petitioner had notice that the search would occur but chose to cross the border anyway. Any privacy expectations Petitioner may have had were outweighed by the government's interest in preventing him from bringing the ATM skimming malware into the United States.

Additionally, the Fourteenth Circuit correctly held that the government's acquisition pursuant to 18 U.S.C § 2703(d) of the location information from cell tower dumps and from cell-site location information collected in the Three-Day Records and the Weekday Records did not violate the Fourth Amendment following *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

A person whose records are obtained from cell tower dumps has no reasonable expectation of privacy, because the records indicate no more than what a pole camera might when surveilling a public space. Further, there is no proprietary interest in tower dumps, because the third-party doctrine applies. Tower dumps operate like a pen register, only identifying the subscriber and the number he uses. The FBI requested cell tower dumps after recovering images of a man in a black sweatshirt near the affected ATMs. These tower dumps were simply the next step in the FBI's investigation that were used to determine what persons were in the general area at the times the man in the black sweatshirt was at the ATMs. Therefore, the records obtained from the cell tower dumps did not violate the Fourth Amendment.

The acquisition of the Three-Day Records did not constitute a search and, consequently, did not violate the Fourth Amendment. The Three-Day Records were not precise and comprehensive in the way that the seven-day records were in *Carpenter*. The government requested these records after finding the malware and bank information on Petitioner's electronics and placing him near the Sweetwater ATM when it was tampered with. Further, only

three days of records were requested. Petitioner had no reasonable expectation of privacy in such a limited time period and where he knowingly exposed this information to the public.

For similar reasons, the Weekday Records did not constitute a search under the Fourth Amendment. Although multiple days of information were collected, the specific number of hours was limited to only what was needed for the investigation. The 100 total hours collected was fewer than the 168 hours collected in *Carpenter*. Ultimately, this Court's holding in *Carpenter* was narrow and limited to the specific facts of that case. The *Carpenter* holding should remain narrow because the government's strong security interest outweighs individual's expectation of privacy in the public sphere.

For these reasons explained in detail below, Respondent respectfully asks the Court to affirm the Fourteenth Circuit's decision.

STATEMENT OF THE CASE

Statement of Facts

On October 13, 2018, Mariposa Bank branch manager, Maeve Millay, discovered ATM tampering at the branch located on Boswell Street in Sweetwater, West Texas. R. at 3. A Mariposa Bank customer had noticed that adjacent ATMs displayed different screens, so Millay called the ATM engineer, and he found that the ATM had been cut open and infected with malware through its USB port. *Id.* After an internal investigation, Mariposa Bank discovered that ATM skimming occurred at four additional ATMs in Sweetwater and three ATMs in Escalante. *Id.*

Based on the engineer's maintenance records, Millay determined that the ATM at the Boswell Branch was tampered with between October 11 and October 13, 2018. *Id.* at 3. Due to a storage malfunction, the ATMs in Escalante lost all surveillance data, and Mariposa Bank

managers could only determine that the skimming occurred in early October 2018. *Id.* at 4. Between the eight ATMs, several different methods were used to steal information and cash. *Id.* Two of the Sweetwater ATMs had foreign "skimmers" that overlaid the debit card readers. *Id.* Two other Sweetwater ATMs had malware installed through the USB port, which gave the skimmers access to information belonging to the customers who used the infected ATM. *Id.* at 3, 4. The last ATM had a sophisticated malware that emptied the cash from the ATM. *Id.* at 4. Upon discovering $50,000 of losses and hundreds of stolen identities, Mariposa Bank reported its findings to the FBI. *Id.*

FBI Special Agent Catherine Hale began investigating the ATM skimming. *Id.* Surveillance photographs near three of the ATMs captured images of a man in a black sweatshirt. *Id.* Pursuant to 18 U.S.C. § 2703(d) of the Stored Communications Act (SCA), Agent Hale, along with U.S. Attorney Elsie Hughes, requested three tower dumps[1] from the cell sites near three Sweetwater ATMs for thirty minutes before and thirty minutes after the man in the black sweatshirt was at the ATMs. *Id.*

On September 25, 2019, Petitioner, Hector Escaton, was returning to the United States from Mexico through a West Texas border checkpoint. *Id.* at 2. Customs and Border Protection (CBP) Officer Ashley Stubbs performed a routine border search of Petitioner's car. *Id.* The search revealed three large suitcases in the back of Petitioner's car. *Id.* The suitcases contained a large number of electronic devices, including an iPhone, a laptop, three external hard drives, and

[1] Tower dumps provide a list of phone numbers that used a tower for any purpose, usually for a short time period. *R.* at 4 n.3. The tower dumps here contained an hour of cell-tower data per tower. *Id.* at 4.

four USB devices. *Id.* Officer Stubbs placed the iPhone on airplane mode, confirmed the laptop was disconnected from wireless service, and searched both devices manually. *Id.* A paper note was found on the laptop with the message, "Call Delores (201) 181-0981 $$$." *Id.* After recording the note and the iPhone number, Officer Stubbs returned Petitioner's phone but kept the remaining electronic devices. *Id.* at 2-3. While no passwords were required to open the devices, some folders on the laptop were password-protected. *Id.* at 3. Officer Stubbs was also unable to access the USB contents. *Id.*

Officer Stubbs gave the electronics to Theresa Cullen, the Immigration and Customs Enforcement (ICE) Senior Special Agent & Computer Forensic Examiner who was stationed at the border. *Id.* Agent Cullen used forensic software to find that Petitioner's laptop contained documents with bank account numbers and pins. *Id.* She also discovered traces of malware on the USB devices. *Id.* She reported her findings to Officer Stubbs, who immediately informed the FBI of the results. *Id.*

The FBI found that the malware on Petitioner's USB devices was similar to the malware used at Mariposa ATMs. *Id.* at 5. Further, Petitioner's phone number matched one of the numbers generated from the tower dumps. *Id.* After these findings, U.S. Attorney Hughes and Agent Hale obtained a court order pursuant to the SCA to obtain Petitioner's cell phone records. *Id.* This order (Three-Day Records) directed Delos Wireless to disclose Petitioner's cell site records[2] from October 11 to October 13, 2018. *Id*. These records placed Petitioner in the area of

[2] Even when a cell phone is not being used, the phone will tap into a wireless network several times per minute through cell sites, which will generate cell-site location information (CSLI). R. at 4 n.4.

the Sweetwater Boswell Branch ATM on October 12, 2018. *Id.* Depending on the number of cell sites in a particular region, CSLI varies in its accuracy. Where Sweetwater is more densely populated, there are more cell sites in the area, so CSLI is accurate within fifty feet. Hale Aff. ¶ 11. Alternatively, Escalante, is less populated, so CSLI is accurate only within 1,000 feet. Hale Aff. ¶ 12.

After these findings, an additional court order (Weekday Records) was issued directing Delos Wireless to disclose Petitioner's cell site sector information for all weekday records between October 1 and October 12, 2018, between the hours of 8 AM and 6 PM. R. at 5. The order also requested subscriber information and the same sector information for the telephone number attributed to Delores on Petitioner's laptop. *Id.* These records revealed the phone number from the laptop note belonged to Delores Abernathy, who had been previously convicted of ATM skimming. *Id.* Further, the records placed Abernathy in the area of the three Escalante ATMs in early October. *Id.* The records also placed Petitioner with Abernathy in Escalante during the same time period. *Id.*

Abernathy was then indicted and a search warrant for her house was obtained. *Id.* There, law enforcement found cash and malware identical to that found on Petitioner's USBs. *Id.* After Abernathy was arrested, she entered a plea agreement and cooperated with the government in its case against Petitioner. *Id.* at 6.

Procedural History

Petitioner was indicted 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. *Id.* Petitioner filed a motion to suppress the forensic search results and the CSLI records. *Id.* The district court denied the motion, and a jury found Petitioner guilty on all charges. *Id.* Petitioner appealed this conviction, and the Fourteenth Circuit affirmed. *Id. at 14.*

Standard of Review

Both issues on appeal involve questions of law, which are reviewable under the de novo standard of review. *Pierce v. Underwood*, 487 U.S. 552, 558 (1988). Therefore, this Court should apply the de novo standard to both legal issues.

ARGUMENT

I. The Fourteenth Circuit Properly Held that the Fourth Amendment Does Not Require Government Officers to Have Reasonable Suspicion Before Conducting Forensic Searches of Electronic Devices at an International Border.

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. The Fourth Amendment reasonableness standard generally requires that the government obtain a warrant prior to a search. *Riley v. California*, 134 S. Ct. 2473, 2482 (2014). This warrant requirement has a few specific exceptions. *Id.* Searches that occur at the international border fall under one of these exceptions, referred to as the border search exception. *United States v. Ramsey*, 431 U.S. 606, 619 (1977).

As old as the Fourth Amendment is the recognition that border searches without probable cause or a warrant are per se reasonable. *Id.* In 1789, Congress enacted the first customs statute that granted customs officials "full power and authority, to enter any ship or vessel, in which they shall have reason to suspect any goods, wares or merchandise subject to duty shall be concealed." *Id.* at 616 (quoting Act of July 31, 1789, c. 5, 1 Stat. 29).

Justice Rehnquist asserted, "There has never been any additional requirement that the reasonableness of a border search depended on the existence of probable cause." *Ramsey*, 431 U.S. at 619. Searches at the border are assumed to be reasonable "simply by virtue of the fact that they occur at the border." *United States v. Flores-Montano*, 541 U.S. 149, 152-53 (2004) (quoting *Ramsey*, 431 U.S. at 616).

Reasonableness is the benchmark of the Fourth Amendment. *Riley*, 134 S. Ct. at 2482. When looking at exceptions to the Fourth Amendment's warrant requirements, courts weigh the legitimate government interests furthered by the search against the individual privacy interests infringed upon by the search. *Id.* at 2484. The Fourth Amendment's balancing analysis between government interest and individual privacy is different at the border than it is in the interior of the United States. *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985). At the international border, this balance is "struck much more favorably to the government." *Id.* at 540.

A. A Person Expects Less Privacy Upon Entering and Exiting the United States, and There Is a Significant National Security Interest in Using the Border to Screen for Risks to the United States.

The border search exception is grounded in the right of the sovereign to dictate who and what may enter the country. *Ramsey*, 431 U.S. at 620. This right is based on the nation's interest in "self protection reasonably requiring one entering the country to identify himself . . . and his belongings." *Id.* at 618 (quoting *Carroll v. United States*, 267 U.S. 132, 154 (1925)). In *Ramsey*, the defendant was involved in a "heroin-by-mail enterprise." *Id.* at 608. A United States customs officer noticed eight envelopes from Thailand that were bulky and decided to inspect them. *Id.* at 609. The customs officer found heroin in the envelopes, and the defendant was indicted. *Id.* at 10. In affirming the defendant's conviction, this Court focused on the "limited justifiable expectations of privacy for incoming material crossing United States borders." *Id.* at 623. The Court held the customs officer's search of the envelopes fell within the border search exception. *Ramsey*, 431 U.S. at 623-25 n.17. As the Fourteenth Circuit discussed in its review of the present case, this limited privacy expectation at the border is due in part to the notice of a search that is provided to those crossing the border. *Escaton v. United States*, 1001 F.3d 1341 (14th Cir. 2021).

The government's interest in prohibiting unwanted persons and contraband "is at its zenith" at the border. *Flores-Montano*, 541 U.S. at 153. In *Flores-Montano*, the defendant's

vehicle was searched when he attempted to enter the United States at a Port of Entry in southern California. *Id.* at 150. A customs inspector asked defendant to exit his vehicle, and the vehicle was taken to a secondary inspection station. *Id.* When the gas tank was tapped, it sounded solid, so the inspector requested a mechanic to search the gas tank. *Id.* at 151. The search revealed over eighty pounds of marijuana in the defendant's gas tank. *Id.* at 150. This Court, referencing the sovereign's "inherent authority to protect" and "paramount interest in protecting" its territory, held that the government had the authority to perform the suspicionless search of the defendant's gas tank. *Id.* at 153-55.

Moreover, a suspicionless search of a crew member's cabin on a foreign cargo ship at a port of entry into the United States was reasonable under the Fourth Amendment. *United States v. Alfaro-Moncada*, 607 F.3d 720, 732 (11th Cir. 2010). In *Alfaro-Moncada*, Customs and Border Protection conducted an agricultural re-boarding search of a foreign cargo ship docked in Miami, Florida. *Id.* at 723. As part of the search, the officers inspected the crew members' cabins. *Id.* at 724. The officers found child pornography in the defendant's cabin, and the defendant was ultimately found guilty of possession of child pornography. *Id.* at 725-26. Because the search took place at a "functional equivalent of the border," the border search exception applied. *Id.* at 727. The Eleventh Circuit discussed the significant privacy interest the defendant had in his vessel, stating that "a cabin is a crew member's home—and a home 'receives the greatest Fourth Amendment protection.'" *Id.* at 729 (quoting *United States v. McGough*, 412 F.3d 1232, 1236 (11th Cir. 2005). However, this significant privacy interest was still outweighed by the government's inherent interest in preventing illegal contraband from entering the country. *Id.* at 732. Nevertheless, the Eleventh Circuit held that the suspicionless search of the crew

member's living space was subject to the border search exception and upheld defendant's conviction. *Id.*

At the border, the government interest in controlling who and what enters the country is significantly greater than an individual's expectation of privacy under the Fourth Amendment.

Petitioner's expectation of privacy was substantially lowered when he arrived at the border. Similar to the search in *Ramsey*, the search of Petitioner took place at the border. Petitioner was returning to the United States when his car was searched at a border checkpoint. Furthermore, the forensic search of Petitioner's electronics was also conducted at the border. Like the defendant's privacy expectations in *Ramsey*, Petitioner's privacy expectations were minimal when he arrived at the border. Petitioner had notice that his car would be searched upon entering the country. Assuming the risk that his vehicle, luggage, and belongings would be searched, Petitioner still chose to enter the United States.

Weighed against Petitioner's limited privacy interest at the border, the government's interest in protecting its people was paramount. Similar to the balance of interests in *Flores-Montano*, the balance here significantly tilted in favor of the government's interest in controlling its country and prohibiting illegal contraband. The government's legitimate interest in national security far outweighed Petitioner's limited privacy expectations.

Additionally, Petitioner has a lower privacy interest in his electronic devices than a crewmember has in his living space on a ship. Similar to the crewmember's privacy interest in *Alfaro-Moncada*, Petitioner had a privacy interest in his cell phone and laptop. But Petitioner's privacy expectations in his electronics did not reach the level of the crewmember's privacy expectations in his living area in *Alfaro-Moncada*. Because a search of a home, which requires the greatest level of protection under the Fourth Amendment, does not require reasonable

suspicion when at the border, a search of electronics also requires no reasonable suspicion when at the border. Therefore, the forensic search of the Petitioner's electronics at the border was reasonable under the Fourth Amendment.

B. The Test Which Balances the Government Interest Against Individual Privacy Expectations Is the Sole Test Used in Analyzing Border Searches.

In dealing with the issue of border searches, this Court used the term "routine" to describe permissible, suspicionless searches at the border. *Almeida-Sanchez v. United States*, 413 U.S. 266, 272 (1973) (holding that routine inspections of persons seeking to cross the border were permissible). In *Ramsey*, the Court used this term again, stating that the government's authority to exclude unwanted persons and contraband could "be effectuated by routine inspections and searches of individuals or conveyances seeking to cross our borders." *Ramsey*, 431 U.S. at 619 (quoting *Almeida-Sanchez*, 413 U.S. at 272). The Court left open the question of whether a border search could be unreasonable due to the "particularly offensive manner in which it is carried out." *Id.* at 618 n.13.

In another case, this Court explicitly stated that it was not deciding "what level of suspicion, *if any*, is required for nonroutine border searches such as strip, body-cavity, or involuntary x-ray searches." *Montoya de Hernandez*, 473 U.S. at 541 n.4 (emphasis added). This language lead lower courts to analyze border search cases on the basis of whether the search was routine or nonroutine. *See United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013); *United States v. Sandler*, 644 F.2d 1163 (5th Cir. 1981); *see also United States v. Braks*, 842 F.2d 509 (1st Cir. 1988).

Recently, this Court suggested that the "routine" versus "nonroutine" distinction is not relevant to searches of property at the border. *Flores-Montano*, 541 U.S. at 152. In *Flores-Montano*, the Ninth Circuit used a balancing test to determine that the search of the defendant's

gas tank was nonroutine and therefore required reasonable suspicion. *Id.* at 152. This Court reversed, stating that "complex balancing tests to determine what is a 'routine' search of a vehicle . . . have no place in border searches of vehicles." *Id.* Further, the policies "that might support a requirement of some level of suspicion" for highly intrusive searches of a person do not correlate to searches of property. *Id.* at 152. Because the privacy and dignity interests that apply to searches of persons do not carry over to vehicles, the "routine" versus "nonroutine" distinction should not be applied to border searches of property. *Id.*

Petitioner may argue that this Court should follow *Cotterman* and classify the forensic search of Petitioner's electronics as a nonroutine search, but this Court has been clear that this distinction is not relevant or determinative. Further, the classification would be incorrect. In *Montoya De Hernandez*, this Court listed examples of nonroutine border searches, such as strip searches, body cavity searches, and involuntary x-ray searches. While this list was not exhaustive, all of the examples given involve searches of a person's body. None of the examples involved searches of property. Therefore, a search of electronics would be classified as a routine search.

Although the search of Petitioner's electronics would classify as routine, this distinction is irrelevant. Similar to the search in *Flores-Montano*, the search at issue here involved property. Because this complex analysis has no place in border searches of property, this test is not applicable to Petitioner's search. The only balancing test that should be applied at the border is the one used in *Ramsey*, which looks at the government interest weighed against the individual's privacy interest.

C. At the Border, an Individual's Privacy Interest in his Electronic Devices Is Still Outweighed by the Inherent Government Interest in Protecting Its People.

A warrant is *generally* required before a search of a cell phone. *Riley*, 134 S. Ct. at 2493 (emphasis added). In *Riley*, an officer pulled over the defendant for driving with expired registration tags. *Id.* at 2480. After learning that the defendant's license was suspended, the defendant's car was impounded and searched. *Id.* The defendant was arrested for possession of concealed and loaded firearms, and the officer performed a search incident to the arrest. *Id.* The officer seized and searched a cell phone found in the defendant's pocket. *Id.* The search uncovered evidence linking the defendant to a gang and a vehicle that was suspected to be involved in a recent shooting. *Id.* at 2481. This Court held that the warrantless search of defendant's cell phone, although incident to arrest, was unreasonable and therefore a violation of the Fourth Amendment. *Id.* at 2493. The Court expressed concern with "cloud computing," that would allow officers to view data that is not stored on the phone but stored on a remote server. *Id.* at 2491. The justifications for the search incident-to-arrest exception—officer safety and preventing destruction of evidence—did not apply to digital information on cell phones. *Id.* at 2484-85. The Court noted that "other case-specific exceptions may still justify a warrantless search of a particular phone." *Id.* at 2494.

Recently, the Fourth Circuit applied *Riley* to a forensic search of a cell phone at the border and held that reasonable suspicion was required to conduct such a search. *United States v. Kolsuz*, 890 F.3d 133 (4th Cir. 2018). Conversely, the Eleventh Circuit found that the Fourth Amendment does not "require suspicion for a forensic search of an electronic device" at the border. *United States v. Touset*, 890 F.3d 1227, 1233 (11th Cir. 2018). In *Touset*, border agents forensically searched the defendant's two laptops, two external hard drives, and two tablets at the airport when he arrived on an international flight. *Id.* at 1230. The forensic searches revealed

child pornography on the laptops and hard drives. *Id.* Defendant filed motions to suppress the evidence obtained from the forensic searches, but the motions were denied. *Id.* at 1231. The Eleventh Circuit affirmed, finding that, although there was reasonable suspicion in this case, reasonable suspicion was not required for a forensic search of electronics at the border. *Id.* at 1233. The Eleventh Circuit applied the balancing test used in *Ramsey*, weighing the "diminished privacy interests of travelers" against the government interest "in preventing the entry of unwanted persons and effects." *Id.* at 1235 (quoting *Flores-Montano*, 541 U.S. at 152).

Further, the Eleventh Circuit determined that *Riley*, which was specific to searches incident-to-arrest, did not apply to border searches. *Id.* at 1234. Although there was an intrusion of privacy in a cell phone search, this privacy interest was still outweighed by the government interest at the border. *Id.* at 1235. Digital contraband at the border poses the same risk as "its physical counterpart," so the justifications for the border exception still applied. *Id.* The advancement of technology that allows for contraband to be concealed "only heightens the need of the government to search property at the border." *Id.* Requiring reasonable suspicion for forensic searches of electronics would "create special protection" for digital contraband. *Id.* Relying on the basis that the "Supreme Court has never required reasonable suspicion for a search of property at the border, however non-routine and intrusive," the Eleventh Circuit affirmed. *Id.*

At the border, the border search exception, not *Riley*, applies and allows forensic searches of electronics without reasonable suspicion.

Petitioner may argue that this Court should follow *Kolsuz* and apply *Riley* to border searches, but this would be an incorrect application of the law. Whereas the search in *Riley* occurred incident to arrest, the search of Petitioner took place upon his attempted entry into the

United States. Though the government has a legitimate interest during an arrest, that interest is at its peak when at the border. Further, the concern in *Riley* that officers might access cloud information was not a concern in Petitioner's search. Officer Stubbs turned Petitioner's iPhone on airplane mode and disconnected his laptop from wireless service, ensuring that only information actually on the devices was accessible. This Court in *Riley* explicitly stated that some warrantless searches of phones may still be justified. The historically recognized border search exception is one exception that justifies a warrantless search of a phone.

This Court should follow the reasoning in *Touset* and hold that no reasonable suspicion is required to perform a forensic search of electronics at the border. The border search exception is as old as the Fourth Amendment itself, and the precedent regarding this issue stresses the inherent authority and significant interest of the sovereign to protect its people. Straying from this historical precedent and requiring reasonable suspicion at the border for forensic searches of electronics would give criminals the ability to shield their crimes. Similar to the risk posed by the digital contraband in *Touset*, Petitioner's malware and bank information contained on his electronics posed a significant threat to the people of West Texas. As the justifications for the border search exception applied to the defendant's electronics in *Touset*, those same justifications—prohibiting contraband—applied to the search of Petitioner's electronics. Therefore, any privacy interest that Petitioner retained in his electronics was significantly outweighed by the government interest in protecting against the malware and bank information that Petitioner was attempting to bring into the United States.

In evaluating searches under the Fourth Amendment, courts weigh the government interest against the individual's privacy interest. At the border, the government interest is at its peak and is substantially greater than any individual privacy interest. The government interest in

controlling what enters its country does not vary depending on whether the contraband is in physical or digital form. As technology advances, creating any exception for electronic devices at the border would create a means for individuals to conceal their crimes and contraband when entering the United States. The government's inherent authority to search individuals at the border is one of the oldest and soundest principles of this country, which should not be diminished simply because technology advances. Therefore, Respondent respectfully asks this Court to affirm the Fourteenth Circuit and hold that forensic searches of electronic devices at the border require no reasonable suspicion.

II. The Fourteenth Circuit Properly Held that Respondent's Acquisitions Pursuant to 18 U.S.C. § 2703(d) of the Location Information from Cell Tower Dumps, the Three-Day Records, and the Weekday Records Did Not Violate the Fourth Amendment Following *Carpenter*.

A Fourth Amendment violation can only occur after "government officers violate a person's 'reasonable expectation of privacy'." *United States v. Jones*, 565 U.S. 400, 406 (2012) (citing *Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring)). This test shifted the focus of the analysis away from strictly property interests towards a connection between persons and property. *Carpenter*, 138 S. Ct. at 2227 (dissent, J. Kennedy). These protections, however, may not be afforded to that which a person "knowingly exposes to the public." *Katz*, 389 U.S. at 351. Though there is a balance in interests between security and privacy, the scale often tips in favor of security. *United States v. Garcia*, 474 F.3d 994, 998 (7th Cir. 2007). To determine when electronic monitoring violates a person's reasonable expectation of privacy, it is first necessary to review when the government's use of technology in surveillance may constitute a search under the Fourth Amendment.

A. The Government May Use Technology to Enhance Their Investigation Without Conducting a Search under the Fourth Amendment When a Person Has No

Reasonable Expectation of Privacy and the Privacy Interest Does Not Outweigh the Interest of Security.

Advancements in technology can be beneficial to security and privacy, and thus "the meaning of a Fourth Amendment search must change to keep pace with the march of science." *Garcia*, 474 F.3d at 997; see *United States v. Kyllo*, 533 U.S. 27, 34 (2001) (holding police use of sense-enhancing technology constitutes a search under the Fourth Amendment where that technology is not in general public use). Nevertheless, the Fourth Amendment does not limit law enforcement from using technology to more efficiently conduct their investigations. *United States v. Houston*, 813 F.3d 282, 288 (6th Cir. 2016). In *Houston*, police affixed a stationary camera to a utility pole in a rural area to observe the defendant's activities outside his home for a period of ten weeks. *Id.* at 286. This surveillance did not constitute a search under the Fourth Amendment, as it would have been possible for any member of the public to observe these activities. *Houston*, 813 F.3d. at 290; see also *State v. Rigel*, 97 N.E.3d 825, 830 (Ohio Ct. App. 2017) (holding there was no violation of a property owner's reasonable expectations of privacy as the utility pole was on a public road).

As technology has developed, this Court has used this framing to examine what it believed was an intersection of person and property in cellular phone data. *Riley*, 134 S. Ct. at 2484. This Court's analysis in *Riley* was primarily focused on how technology has permitted the convenient storage of sensitive data within a cell phone, and this calls for an increased privacy interest. *Id.* at 2489. Its decision was based in part on the view that, to the metaphorical Martian, the cell phone would appear to be "an important feature of human anatomy." *Id.* at 2484.

As a result, this Court opened the door to possible challenges to the permissible gathering of electronic information under the Stored Communications Act ("SCA"). See 18 U.S.C. §§ 2701-2712 (2018). Among other forms of electronic communication, the SCA "authorizes law

enforcement access to cell tower logs and associated account information," including telephone number or other subscriber information or identity. 18 U.S.C. § 2703(c)(2); *In re Cell Tower Records Under 18 U.S.C. 2703(D)*, 90 F. Supp. 3d 673, 676-677 (S.D. Tex. 2015). Law enforcement can request these records by court order upon a showing of "specific and articulable facts" that it would be reasonable to believe that their content is "relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). Moreover, there is no federal statute which grants the customer proprietary rights in her cell phone number or account information. *Cell Tower Records*, 90 F. Supp. 3d at 675.

In *Carpenter*, the Court stretched the Fourth Amendment to protect a specific form of cellular data in holding that the request of seven days of cell-site location information (CSLI), pursuant to 18 U.S.C. § 2703(d), constitutes a Fourth Amendment search. 138 S. Ct. at 2217 n.3, 2223. The prosecution applied for two court orders pursuant to the SCA in order to obtain CSLI from the defendant's two cell service providers, including a request for 152 days of records from one carrier, and for seven days of records from the other carrier. *Id.* at 2212. From these requests, the orders revealed records spanning 127 days and two days, respectively. *Id.* This information was used to analyze whether the defendant was at the same location of several banks at the times they were robbed. *Id.* The prosecution compiled these data points onto a map, which was presented at trial and ultimately lead to the defendant's conviction. *Id.*

In its analysis, this Court examined the convergence of two lines of cases: other forms of electronic location tracking and the relevant exclusions provided by the third-party doctrine. *Id.* at 2214-15. First, the Court focused specifically on instances of location tracking using GPS and determined that due to its "deeply revealing nature" and its "comprehensive reach," the acquisition of seven days of historical CSLI was a search under the Fourth Amendment. *Id.* at

2223. This Court relies mostly on its reasoning in *Jones*, where it held that the installation of a GPS device on a target's vehicle and the subsequent tracking of its movements for twenty-eight days constituted a search. 565 U.S. at 404. In her concurring opinion in *Jones*, Justice Sotomayor opined that GPS monitoring "generates a precise, comprehensive record" which reflects details about a person's "familial, political, professional, religious, and sexual associations." *Id*. at 415. This Court in *Carpenter* used this description to compare the information revealed in CSLI to the ability of GPS tracking to support its holding. 138 S. Ct. at 2217-2218.

This Court also held in *Carpenter* that the third-party doctrine would not apply to CSLI records. *Id.* at 2217. The third-party doctrine allows for a reduced privacy interest in information which is revealed to a third party, such as to bank employees "in the ordinary course of business," even when the records are provided on the assumption that they will be used in confidence and for limited purposes. *United States v. Miller*, 425 U.S. 435, 443 (1975). This doctrine was extended to include records held by telephone companies, such as a pen register. *Smith v. Maryland*, 442 U.S. 735, 745-746 (1979). In *Smith*, the Court reasoned that although these records were meant to track the subscriber making the phone call, the subscriber ultimately assumes the risk that his information may be shared with the Government. 442 U.S. at 743-744. In *Carpenter*, however, this Court chose to not apply the third-party doctrine to historical CSLI, primarily because there was no voluntary "assumption of risk" regarding this type of data, as the only way to evade the record was to disconnect the cell phone from its network entirely. 138 S. Ct. at 2220.

Nevertheless, this Court refused to extend its holdings to other forms of CSLI, such as "real-time" CSLI or to other electronically-gathered location information, as with cell tower dumps. *Id.* It also declined to establish a bright-line rule to hold all requests for historical CSLI

records to the probable cause standard—no matter how few—and instead determined that the request for seven full days of records constitutes a search under the Fourth Amendment. *Id.* at 2217 n.3. Given the analysis in *Carpenter* and preceding cases, it is possible that a person will not have a strong proprietary interest in what he knowingly exposes to the public, even when that interest is related to his cell phone. Therefore, the government does not conduct a search under the Fourth Amendment by accessing some cell phone records when that person has no reasonable expectation of privacy by what he has exposed to the public, and the security interest would outweigh the interest of privacy.

B. The Acquisition of Location Information from Cell Tower Dumps Did Not Constitute a Search Under the Fourth Amendment and Consequently Did Not Violate the Fourth Amendment.

Because the Court in *Carpenter* declined to address whether tower dumps would be a search under the Fourth Amendment, the standard at the time Respondent sought the court order was governed by the SCA. Though the phrase "tower dump" is not used in the statute, the SCA permits government access to cell site logs and the associated subscriber information. Unlike CSLI, which can be used to monitor a person's movements through public thoroughfares, tower dumps simply provide a list of phone numbers that used that tower during a particular moment in time. Tower dump records indicate no more than what a simple video camera could display when surveilling the outside of a building in a public space. Here, as with the defendant in *Houston*, Petitioner knowingly exposed himself to a stationary location in public and was subject to what could be witnessed by any person. Where Petitioner holds no privacy interest in what he knowingly exposes to the public, he also has no protectable interest in his presence near a cell tower in public. Therefore, the information provided by tower dumps would not constitute a search under the Fourth Amendment, and the acquisition of these records do not violate the Fourth Amendment.

Even if these records were to be granted the proprietary interest necessary to invoke Fourth Amendment protections, that interest would be further reduced by the third-party doctrine. Like the pen register in *Smith*, tower dump records are primarily used in the ordinary course of business and do not provide more information beyond that which can be used to identify the subscriber. As a result, Petitioner has assumed the risk that this information might be shared with the Government. Where there is no reasonable expectation of privacy over these records, the security interest outweighs any possible proprietary interest, and the acquisition of these records do not violate the Fourth Amendment.

Petitioner may argue that the level of surveillance achieved using tower dumps is similar to CSLI and is thus comparable to the GPS tracking in *Jones*. Petitioner may also argue that just because a person is in a public space, law enforcement should not have free access to that person's property. However, tower dumps do not present the type of "precise, comprehensive record" which Justice Sotomayor advised would require a warrant to obtain. These records do not follow a person as he moves about the thoroughfares, imputing a pattern to identify their familial and political associations, for example. They do not show with what persons he is affiliating, what businesses he peruses in the area, or even how long he remains there. They simply provide lists of phone numbers that used the tower within a sixty-minute period. As this surveillance is more akin to a pole camera than to GPS, these tower dumps do not constitute a search under the Fourth Amendment and thus do not violate the Fourth Amendment.

C. The Acquisition of the Three-Day Records of CSLI Did Not Constitute a Search Under the Fourth Amendment and Consequently Did Not Violate the Fourth Amendment.

Under *Carpenter*, the request for three days of CSLI ("Three-Day Records") does not constitute a search under the Fourth Amendment. After establishing that Petitioner possessed similar ATM skimming malware and was near the Sweetwater ATMs when the surveillance

photographs were taken, the FBI had reason to believe that Petitioner was also at the Boswell Branch when the ATM was infected with the malware. In order to make this determination, the most efficient and effective method was to request CSLI for Petitioner's phone number. By requesting only three days of records, Respondent narrowed the timeframe to only what would have been necessary to show that result. While monitoring an individual for seven full days could be enough to establish a person's patterns and affiliations, three days of monitoring is hardly an all-encompassing record. Unlike the defendants in *Carpenter* and in *Jones*, Petitioner would not have a reasonable expectation of privacy to such a limited period.

Petitioner may argue that the Court should not rely on the volume of data collected but on the type: that, categorically, historical CSLI may only be obtained with a warrant. If this Court in *Carpenter* was concerned only about the type of data, or even about privacy interests in shorter periods of time, it would have held a different result. For example, it could have focused on the amount of data that was actually gathered by law enforcement (two days, as opposed to seven days), or it could have required a warrant for any request of historical CSLI. Instead, it narrowly held that seven days or more of CSLI would constitute a Fourth Amendment search. Where three days of records are not so encompassing as to invoke the same protections, the warrant requirement should not apply here, because the privacy interest does not overcome the weight of the interest of security. Thus, Respondent's acquisition of the Three-Day Records did not constitute a search and did not violate the Fourth Amendment.

D. The Acquisition of the Weekday Records of CSLI Did Not Constitute a Search Under the Fourth Amendment and Consequently Did Not Violate the Fourth Amendment.

Similarly, the request for 100 total hours within ten weekdays ("Weekday Records") did not constitute a search under the Fourth Amendment. These records were limited to what was necessary to monitor the time period when the Mariposa Bank ATMs were tampered with. In

Carpenter, the CSLI exhibited 168 hours of data, including all hours from weekdays and through the weekend, whereas here, only 100 hours of data were requested. A person's expectations of privacy for her movements between 8 AM and 6 PM on weekdays are diminished by the nature of what she has voluntarily conveyed to the public during that time period. The privacy interests referenced in *Jones* spoke to a comprehensive record that could detail a person's "religious and sexual associations;" 100 hours of CSLI data could not create such a precise record. The ATMs are likely made accessible during these times because Mariposa Bank knows this is when most persons are engaged in the public and would be free to use its services. Where the Weekday Records were the next necessary step in the investigation to prevent bank customers from any further loss, and the request was limited to the times necessary to determine the identities of the conspirators, this was not so invasive as to require a showing of probable cause, and thus did not violate the Fourth Amendment.

Petitioner may argue that collection of any historical CSLI requires a warrant, but it would be incorrect to apply *Carpenter* to all instances of historical CSLI where its use is vital to Respondent's ability to protect its residents. First, the number of cell towers placed in a community varies between regions and thus CSLI varies in its accuracy. For example, the cell sites in Escalante capture a cell phone within 1,000 feet of a cell site, so the CSLI gathered from these sites create a lessened intrusion on the person's privacy interest than where the towers have a shorter range, such as fifty feet.

Additionally, it would be incorrect to say that seven full-day records of CSLI is as intrusive as any lesser time period. Respondent seeks to halt crime to prevent harm and injury to its residents and, for that interest, is permitted some level of monitoring of suspected criminal activity. Certainly, as science advances, the Fourth Amendment must adapt, but it would be

unnecessary and unwise to require heightened protections simply because the technology is new or is utilized by many. By requiring a showing of reasonable suspicion to obtain records related to an ongoing investigation, the SCA sufficiently permits Respondent to satisfy its security interest without infringing on a person's reasonable expectation of privacy. This is particularly true when the search is conducted within the public sphere. To rule otherwise would hinder law enforcement from efficiently stopping crime, particularly when, as here, there was a glitch in the bank's surveillance and there was no other efficient way to identify the ATM skimmers. Where the amount of data requested comprised less than seven full days and did not create a record so comprehensive as to trespass against a person's reasonable expectation of privacy, it does not constitute a search under the Fourth Amendment.

This Court in *Carpenter* specified that its decision was "a narrow one," and the privacy expectation at issue here is distinctly less reasonable than what the Court identified in *Carpenter*, so the records did not constitute a search under the Fourth Amendment. If this Court were to categorize any acquisition of historical location information obtained from cell sites in the public as a Fourth Amendment search, confusion within law enforcement and the lower courts would ultimately result. As Justice Kennedy stated in his dissenting opinion,

> . . . the Government can acquire a record of every credit card purchase and phone call a person makes over months or years without upsetting a legitimate expectation of privacy. But, in the Court's view, the Government crosses a constitutional line when it obtains a court's approval to issue a subpoena for more than six days of cell-site records in order to determine whether a person was within several hundred city blocks of a crime science. That distinction is illogical and will frustrate principled application of the Fourth Amendment in many routine yet vital law enforcement operations.

Carpenter, 138 S. Ct. at 2224. Respondent may use technology to enhance investigations without a warrant when there is no reasonable expectation of privacy, so the acquisition of historical CSLI records which report no more than a seven-day period did not violate the Fourth

Amendment. Therefore, Respondent respectfully asks the Court to affirm the Fourteenth Circuit and hold that the tower dump records, the Three-Day Records, and the Weekday Records do not violate the Fourth Amendment.

CONCLUSION

The Fourteenth Circuit correctly decided both issues. First, the Fourth Amendment does not require reasonable suspicion for forensic searches at the border. Any privacy expectation that an individual crossing the border may have is far outweighed by the legitimate government interest in prohibiting contraband. Second, Respondent's acquisition of cell tower dumps and CSLI did not violate the Fourth Amendment following *Carpenter*. The holding in *Carpenter* was intentionally narrow and should be applied as such. The records acquired here were not so precise and comprehensive that a person would have a reasonable expectation of privacy. For the foregoing reasons, Respondent respectfully requests that this Court affirm the decision of the Fourteenth Circuit.

Respectfully submitted,
Attorneys for Respondent
Team 10