No. 10-1011

IN THE
SUPREME COURT OF THE UNITED STATES

HECTOR ESCATON,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

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

P19,
Counsel for Respondent

UCLA Cyber Crimes Moot Court Competition
March 2019

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

QUESTIONS PRESENTED

I. Did the Fourteenth Circuit Court of Appeals comply with the Fourth Amendment when it upheld the denial of Hector Petitioner's Motion to Suppress Evidence of criminal ATM "skimming" found on his laptop during a border search absent reasonable suspicion?

A. ?

B. ?

II. Did the Fourteenth Circuit Court of Appeals comport with *Carpenter v. United States* when it upheld the government's narrowly tailored affidavit requests of cell-site location information?

A. Does the third-party doctrine apply to eliminate an individual's reasonable expectations of privacy when the government narrows its request of cell-site location information to very limited amounts?

B. Do cell-site location information requests constitute a Fourth Amendment search when the government narrowly tailors the requests to limited timeframes in which crimes occurred?

C. Do governmental requests for cell tower dumps constitute a Fourth Amendment search when the information only contains phone numbers and does not contain the content of communications or any intimate personal identifying information?

OPINION BELOW

The United States Court of Appeals for the Fourteenth Circuit issued its opinion on November 2, 2021. The opinion appears on pages 1-16 of the record. The opinion is reported in *Escaton v. United States*, 1001 F.3d 1341 (14th Cir. 2021).

CONSTITUTIONAL PROVISIONS AND RULES

This case involves the Fourth Amendment which 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

Advancing technology has undoubtedly afforded law enforcement novel tools to further their criminal investigations. These technological advancements have brought to the forefront an increasing need for courts to either extend general constitutional principles to these emerging technologies or to carve out new rules to complement these technologies.

In light of these emerging technologies, courts are concerned with ensuring a balance of privacy interests of individuals with government's interest in investigating serious crimes. However, despite concerns of how these emerging technologies can potentially have on an individual's privacy rights, the utility they provide law enforcement, if employed in a reasonable manner, remains invaluable as it can effectuate law enforcement's goal of ensuring public safety without infringing on important individual privacy rights.

Here, the present case implicates the Fourth Amendment through the government's use of technology to conduct forensic border searches and its requests for limited amounts of cell-site location information ("CSLI") of an individual.

Summary of the Argument

I. The first issue presented on appeal is whether the Border Search Exception to the Fourth Amendment should apply to forensic searches of digital devices. Searches and seizures are deemed reasonable when the legitimate governmental interests being pursued outweigh the privacy and dignity concerns of the individual. *See United States v. Flores-Montano*, 541 U.S. 149, 153 (2004). The Border Search Exception to the Fourth Amendment allows for searches and seizures of personal property absent particularized suspicion because the personal privacy and dignity interests of the individual only outweigh governmental security interests at the border in the case of intrusive body

searches. *United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985). Additionally, digital devices should not enjoy a different standard because the legitimate governmental interests effectuated by the Border Search Exception are even stronger in the context of digital devices, yet do not implicate the same privacy concerns as an intrusive body search.

In order for the Government to protect the nation's borders by combating increasingly covert smuggling, and the perpetration of crime, it must continue to employ the tools necessary to detect these crimes. If evidence of Petitioner Escaton's criminal ATM-skimming operation had been discovered in a binder, notebook, or other non-digital forms, CBP Agent Stubbs' discovery of this information would not be at issue. This Court should uphold long-settled precedent and affirm the Fourteenth Circuit Court of Appeals denial of Petitioner's Motion to Suppress because the forensic search of the Petitioner's digital devices was reasonable under the Fourth Amendment.

II. The second issue presented on appeal is whether the Government's request of various CSLI data complied with *Carpenter v. United States* or violated Petitioner's Fourth Amendment rights. CSLI data, amongst many emerging technologies, presents issues for this Court including whether to decide to implement bright-line rules or follow general constitutional principles that can continue along with each new technological invention. Despite the *Carpenter* Court not extending the third-party doctrine to CSLI data requests of seven days, this Court should apply the third-party here because the Government narrowly tailored its requests to be limited to the specific timeframes in which crimes occurred. *Smith* and *Miller* form the principal third-party doctrine cases and provide that the voluntary conveyance of information to a third-party entity defeats

an individual's reasonable expectation of privacy in that information. In sum, the total amount of data focused on a three specific days of CSLI in which evidence showed the crime had occurred.

Additionally, the Government limited its other historical CSLI data request to a set of weekdays and hours of operation of the bank that suffered criminal fraudulent acts involving their ATM machines. These limitations the Government placed on themselves exemplify that the Government narrowed its requests to the point that they could not piece together intimate details of Petitioner's life.

Reasonableness has formed the basis of much of modern Fourth Amendment doctrine. Even if this Court holds that the third-party doctrine should not apply to the present case, the Government's actions in limiting the scope of their CSLI requests show they acted reasonably given the circumstances. They acted pursuant to the Stored Communications Act, a statute that requires judicial approval and sets a standard of "reasonable grounds." Additionally, the Government limited the scope of their requests to particular time frames in which the crimes may have occurred. Other Fourth Amendment cases have provided instances where a standard less than probable cause is sufficient despite intrusions into individual privacy rights.

Cell tower dump requests are limited and do not hold nearly the same privacy concerns that historical CSLI has. These requests only involve the government requesting and accessing records directly from cell-site towers rather than the individual and the individual's wireless carrier. Also, the requests only yield evidence of which phone numbers connected into the towers and provide minimal information on the locations of an individual compared to more expansive historical CSLI.

STATEMENT OF THE CASE

Procedural Posture

Hector Escaton ("Petitioner") appeals the United States Fourteenth Circuit Court of Appeals decision affirming the District Court's denial of a Motion to Suppress Evidence found during a search of his vehicle at the United States' southern border, and government affidavit requests of CSLI. (R. at 6). The District Court and the Fourteenth Circuit Court of Appeals held for Respondent ("Government") on both the evidence obtained at the border and the CSLI requests, denying Petitioner's Motion to Suppress Evidence. (R. at 2).

Statement of Facts

On September 25, 2019, Customs and Border Protection ("CBP") Agent Ashley Stubbs initiated a routine search of Petitioner's vehicle as Petitioner entered the United States from Mexico at a West Texas border checkpoint. (R. at 2). During the search, CBP Agent Stubbs discovered three large suitcases, an iPhone, a laptop, three external hard drives, and four USB storage devices. (R. at 2). Upon opening the laptop, CBP Agent Stubbs discovered a note that read, "Call Delores (201) 181-0981 $$$." (R. at 2). Before initiating a manual search of the items, CBP Agent Stubbs disabled their wireless communication abilities. (R. at 2). CBP Agent Stubbs then returned Petitioner's iPhone and kept the remaining items. (R. at 3). Although no passwords were needed to open the items, CBP Agent Stubbs discovered he could not access the contents of the USB devices, nor could he open folders on the laptop. (R. at 3).

CBP Agent Stubbs then brought the items to an Immigration and Customs Enforcement Senior Special Agent, Theresa Cullen, who scanned and copied the contents of the items. (R. at 3). After the contents were copied, a process that normally takes several hours, Agent Cullen erased the hard drive scans as they did not contain incriminating information. (R. at 3).

However, Agent Cullen found documents on the laptop listing individual bank accounts and pin numbers, in addition to malware on the USB device. (R. at 3).

The CBP notified the FBI of its findings through their forensic search of Petitioner's laptop and USB device. (R. at 3). As of October 2018, the Federal Bureau of Investigation (FBI) had been investigating pervasive instances of ATM skimming at Mariposa Bank ("Mariposa"), a nationally operated bank which owns several branches in the cities of Sweetwater and Escalante. (R. at 3). ATM skimming is a criminal activity involving the collection of customer bank accounts and pin numbers, and it costs banks hundreds of millions of dollars each year and affects thousands of customers. (R. at 3). Among various methods, criminals can commit ATM skimming by infecting ATM terminals with malware using a USB device. (R. at 3).

On October 13, 2018, a customer noticed differences between ATM machines at the Boswell Mariposa Bank branch. (R. at 3). The local branch manager called the engineer who had examined the ATM machines on October 11, just two days prior, to reexamine the ATM machines. (R. at 3). The engineer determined that an ATM machine had been infected with malware through its USB port, allowing the suspect to read information about customers who used the machine. (R. at 3).

Mariposa conducted an internal investigation that revealed ATM skimming at four additional Sweetwater ATMs and three total ATMs in the city of Escalante. (R. at 3). Because of a malfunction in storage, bank managers could only determine that ATM skimming occurred in early October 2018. (R. at 4). Mariposa investigators discovered additional Sweetwater ATMs with USB ports infected with malware, one of which contained sophisticated malware which allowed the suspect to take cash from the ATM. (R. at 4). Additionally, the investigators discovered hundreds of bank customers' identities had been stolen. (R. at 4). Mariposa estimated

$50,000 of losses in October 2018 from direct withdrawals and the creations of false bank accounts because of the ATM skimming. (R. at 4).

Mariposa reported the findings of its internal investigation to the FBI. (R. at 4). FBI Special Agent Catherine Hale, examining connections between evidence seized from the forensic border search and Mariposa's internal ATM skimming investigation, received surveillance photographs from Mariposa near three ATM machines which had malware. (R. at 4). ATM surveillance photographs captured images of a man wearing a black sweatshirt. (R. at 4).

Special Agent Hale, along with U.S. Attorney Elsie Hughes, used information provided by CBP from the forensic border search and information provided by Mariposa regarding its internal ATM skimming investigation to request three tower dumps from the cell-sites near three Sweetwater ATM machines. (R. at 4). U.S. Attorney Hughes and Special Agent Hale requested the tower dumps pursuant to the Stored Communications Act ("SCA"), which requires a standard below probable cause. (R. at 4). Mariposa estimated the times when the Sweetwater ATMs were tampered with through ATM maintenance records. (R. at 4). The requested tower dumps, comprising of only a list of all phone numbers connecting with a cell-site tower, were limited to 30 minute intervals before and after the surveillance photographs captured the man in the black sweatshirt at the three ATM machines. (R. at 4).

CBP Agent Stubbs relayed Petitioner's phone number and details on potential bank fraud and identity theft claims to the FBI. (R. at 5). Petitioner's phone number matched one of the phone numbers produced from the three cell tower dumps. (R. at 5). While not identical, the malware found on Petitioner's devices was similar to the malware found at the Sweetwater ATMs. (R. at 5). U.S. Attorney Hughes and Special Agent Hale sought a judicial order, pursuant

to the SCA, to obtain Petitioner's cell phone records using the information they gathered. (R. at 5).

A federal magistrate judge granted their request, issuing an order directing Delos Wireless ("Delos"), Petitioner's wireless cell phone carrier, to disclose CSLI between October 11, 2018 and October 13, 2018 (hereinafter "Three-day Records"). (R. at 5). ATM maintenance records indicated that the Boswell branch's ATM machine had been infected with malware during this stretch of time. (R. at 5). The Three-day Records located Petitioner's cell phone near the Sweetwater Boswell branch on October 12, 2018. (R. at 5).

These records, however, did not locate Petitioner's cell phone in the city of Escalante. (R. at 5). The Government then requested and received an additional order to disclose CSLI information, and determine the subscriber information, of the phone number listed on the note found on Petitioner's laptop which accompanied the name "Delores", suspecting the phone number could be of an accomplice. (R. at 5). The request and order also included CSLI for Petitioner's phone number. (R. at 5).

This order (hereinafter "Weekday Records") comprised of only 10 weekdays of CSLI limited to the bank's hours operations between 8 AM and 6 PM from October 1, 2018 through October 12, 2018. (R. at 5; aff. ¶ 17). The Weekday Records showed the unknown phone number to belong to Delores Abernathy and placed her phone with Petitioner's in Escalante in early October, even being recorded in the same cell-site tower. (R. at 5). Abernathy, previously convicted of ATM skimming, was subsequently indicted, and a search warrant of her home yielded cash and the same malware found on Petitioner's USB devices. (R. at 5). After arrest, Abernathy cooperated with the Government against Petitioner. (R. at 5-6).

The Government indicted Petitioner and a jury convicted him on all charges: Bank Fraud, Conspiracy to Commit Bank Fraud, and Aggravated Identity Theft. (R. at 6).

ARGUMENT

Standard of Review

"[D]eterminations of reasonable suspicion and probable cause should be reviewed *de novo* on appeal." *Ornelas v. United States*, 517 U.S. 690, 699 (1996). Additionally, courts should "review findings of historical fact only for clear error and to give weight to inferences drawn from those facts by resident judges and local law enforcement officers." *Id*.

I. THE FOURTEENTH CIRCUIT COURT OF APPEALS PROPERLY DENIED PETITIONER'S MOTION TO SUPPRESS BECAUSE THE FIRMLY ESTABLISHED BORDER SEARCH EXCEPTION ALLOWS CUSTOMS AGENTS TO SEARCH THE PERSONAL PROPERTY OF INDIVIDUALS CROSSING THE BORDER WITHOUT PARTICULARIZED SUSPICION

The Government has long recognized that reasonable searches at our nation's border will differ from reasonable searches on domestic soil because the "government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border." *United States v. Flores-Montano*, 541 U.S. 149, 153(2004). Due to the security concerns unique to the border, Congress and the Supreme Court have granted law enforcement, "plenary authority," to conduct searches and seizures in order to prevent contraband from crossing the border. *United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985).The Border Search Exception to the Fourth Amendment allows Customs and Border Patrols Agents to search personal property absent particularized suspicion. This honorable court held that "[b]order searches, then, from before the adoption of the Fourth Amendment, have been considered to be 'reasonable' by the single fact that the person or item in question [is at the border]." *United*

States v. Ramsey, 431 U.S. 606, 619 (1977) (Holding that a warrant was not required when a customs officer opened and searched international mail).

This tradition, "that searches at our borders without probable cause and without a warrant are nonetheless 'reasonable,' has a history as old as the Fourth Amendment itself." *Id.* Although the Supreme Court has recognized intrusive searches of the person implicate certain privacy and dignity concerns that require particularized suspicion, these concerns were not implicated by the forensic search of Petitioner Escaton's digital devices. Additionally, technological development provokes new questions regarding the balance of privacy and governmental interests involved in searches and seizures. In *Riley v. California*, this Court held that a warrant is required to search a cell phone during a search incident to arrest, but that ruling does not change our analysis because the search of Petitioner Escaton's digital devices protected weighty government interests in border security. *Riley*, 134 S. Ct. 2473, 2476 (2014). Because individuals expect that searches and seizures of their personal effects may occur at the border, to hold that the logic in *Riley* applies to Petitioner Escaton would be to notify criminals that their activity will be hidden as long as it is stored digitally. *Id.* The "impressive historical pedigree" of the government's power and interest in protecting our nation's borders should not be disregarded. *United States v. Villamonte Marquez*, 462 U.S. 579, 586 (1983) (Holding that particularized suspicion was not required for a customs officer to board a boat and search its contents).

A. Under the Well-Established Border Search Exception to the Fourth Amendment, Searches of Digital Devices at the Border do not Require Particularized Suspicion

The Fourth Amendment provides that, "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." *U.S. Const. amend. IV.* While the Fourth Amendment protects citizen's right to

privacy, the government has created certain exceptions to the requirement of a warrant, probable cause, or particularized suspicion to pursue important government interests.

Whether a search is reasonable will depend on the circumstances surrounding the search and the methods used, and this Court and Congress have determined that the circumstances at our international borders are unique. *See Montoya de Hernandez*, 473 U.S. at 537. These unique circumstances led to the creation of the Border Search Exception to the Fourth Amendment which allows law enforcement at the border to conduct searches and seizures of personal property absent particularized suspicion. *Id*. This was due to the holding that the legitimate governmental interests in protecting our border outweighed any intrusion upon individual privacy interests. *See Ramsey*, 431 U.S. at 619. Only intrusive searches of the individual's body require particularized suspicion because only then do individual privacy and dignity concerns outweigh the government's interest in maintaining safe borders. *Montoya de Hernandez*, 473 U.S. at 538.

The court held that particularized suspicion was not required for the search conducted in *United States v. Flores Montano* in which customs officials located thirty-seven kilograms of marijuana from inside the gas tank of the defendant's vehicle as he attempted to pass through a border checkpoint. *Flores Montano*, 541 U.S. at 153. The process entailed lifting the car, disconnecting internal hosing, dislodging what appeared to be, "bondo" with a hammer, and removing the gas tank, although the tank was re-assembled and the process did not damage the vehicle. *Flores-Montano*, 541 U.S. at 151. The court held that although officials had to perform mechanical work on the vehicle to remove its gas tank and inspect the contents, the search did not require particularized suspicion because the search did not implicate the dignity and privacy concerns involved in the intimate intrusions of the person. *Id*. at 152. The search was

constitutional by virtue of the fact that it occurred at the border and involved a search of the defendant's vehicle and personal effects. *Id*. Additionally, the Fourth Circuit Court of Appeals also held that particularized suspicion was not required for a search of the Defendant's laptop and seventy-five disks containing child pornography. *United States v. Ickes*, 393 F.3d 501, 502 (4th Cir. 2005). The court compared the digital devices to "cargo," and noted that "the expectation of privacy [at the border] is substantially lessened." *Id*. at 506.

CBP Agent Stubb's forensic search of Petitioner Escaton's laptop was constitutional absent particularized suspicion because personal property inside of one's car may be searched without particularized suspicion. Much like the car in *Flores-Montano* underwent extensive mechanical work to disassemble the gas tank and uncover the marijuana, Petitioner Escaton's devices underwent forensic scans and processes to uncover the malware present on the USB devices and documents containing individual private bank account information. *Flores-Montano*, 541 U.S. at 151; (R. at 3). Additionally, the different methods employed by Petitioner Escaton and the defendant in *Flores-Montano* illustrate the need for the court to allow for forensic searches of digital devices at the border absent particularized suspicion. *Id.* The ingenuity and skill involved in concealing kilos of marijuana within the gas tank of the car in *Flores-Montano* could be applied to concealing evidence in digital devices, which have infinite ways to hide information through encryption. *Flores-Montano* 541 U.S. at 151. The court held in *Flores-Montano* that the increasingly complex and adept smuggling methods developing at our borders necessitated allowing Customs Officers to employ correspondingly adept detection methods, and the increased storage capacity of digital devices supports this logic. *Id*.

CBP Agent Stubb's search of Petitioner Escaton's digital devices should fall within the power granted to CBP Agents under the Border Search Exception, which allows for searches of personal property absent particularized suspicion.

B. The Only Border Searches that Require Particularized Suspicion are those that Physically Intrude Upon the Person and Digital Devices Do Not Require a Separate Standard from Other Forms of Property

CBP Agent Stubbs did not need particularized suspicion to initiate the forensic search of Petitioner Escaton's digital devices, because personal property, including digital devices, does not enjoy the special protection afforded to an individual's person. When examining searches at the border the balance is "struck more favorably to the government," due to the government's interest in preventing crime and smuggling. *Id*. at 539. This honorable court has held that two situations are so highly intrusive of "personal privacy and dignity," so as to require particularized suspicion, and those are intrusive searches of the person's physical body, *Id*. at 537, as well as searches that are destructive to individual property, *Flores-Montano*, 541 U.S. at 151.

In *United States v. Montoya de Hernandez* this Court held that detaining a woman suspected of alimentary canal smuggling for at least sixteen hours until evidence of the smuggling could be obtained did violate the Fourth Amendment absent particularized suspicion. *Montoya de Hernandez*, 473 U.S. at 537. The search was deemed particularly offensive since border officials chose to wait for her to pass the drug-filled balloons being smuggled, which generated both discomfort and embarrassment for the defendant. *Id*. The court held that although searches at the border generally did not require particularized suspicion, "highly intrusive searches of the person," did. *Id*.

The court added to this standard in *Flores Montano* by specifying that some searches may be so destructive to personal property so as to require particularized suspicion in order to be

justified under the Fourth Amendment. *Id*. Although the disassembling of the gas tank in *Flores-Montano* did not damage the vehicle at issue, the court foresaw that if similar searches did cause damage, those searches would violate the Fourth Amendment absent particularized suspicion. *Id*. By contrast, the Eleventh Circuit Court of Appeals held in *United States v. Touset* that when a computer or other digital device was implicated in a border search, particularized suspicion was not necessary. *Touset*, 890 F.3d 1227, 1233 (11th Cir. 2018). In *Touset*, a man arriving from an international flight was stopped by customs agents due to his recent trips and money transfers to the Philippines, an area known for sex tourism, and a forensic search of his laptop uncovered child pornography. *Id*. The court noted that the Supreme Court drew a clear line in *Montoya De Hernandez*, and in keeping with longstanding precedent prior to that decision, held that searches of property "however non-routine and intrusive," do not require particularized suspicion. Id. Although the court did discuss technology's increasing ability to house vast amounts of information, it held that this fact supported searches absent particularized suspicion as the court posited that increased digital storage capacity would make detection of criminal activity more difficult. *Id*. at 1235.

CBP Agent Stubbs' search of Petitioner Escaton's digital devices was constitutional because a forensic search of digital devices does not implicate the same privacy and dignity concerns involved in a search of one's person, nor was it destructive of Petitioner Escaton's personal property. The search in *Montoya De Hernandez* involved not only a strip search, but also a body cavity search, which is highly vastly more intrusive than the forensic search of Petitioner Escaton's digital devices because it did not involve exposure or touching of his body. *Montoya de Hernandez*, 473 U.S. at 537; (R. at 3). Searches of the person evoke significant dignity and privacy concerns, but because Petitioner Escaton's personal property was searched

rather than his person, the privacy interests that outweighed governmental interests in *Flores-Montano* are not present here. Touset's case was more similar to Petitioner Escaton's because both cases involved forensic searches of laptops that uncovered incriminating materials. *Touset*, 890 F.3d at 1233. That the incriminating information found would not have been uncovered without forensic technological intervention, R. at 3, also presents support for points made by the court in *Touset*, *Touset*, 890 F.3d at 1233. The Court asserted that increased technological capability meant officers must retain the ability to initiate searches absent particularized suspicion. *Id.*

CBP Agent Stubbs' forensic search of Petitioner Escaton's digital devices was constitutional because the same privacy and dignity interests involved in searches of an individual's person are not implicated by forensic searches of digital devices. Additionally, CBP Agent Stubbs' search of Petitioner Escaton's digital devices should be held constitutional regardless of the Court's decision in *Riley* because the governmental interests furthered by forensic searches of digital devices far outweigh the governmental interests furthered by digital searches incident to an arrest.

In *Riley*, the Supreme Court held that police officers must obtain a warrant to manually search the digital contents of a cell phone even within the context of a search incident to arrest. *Riley*, 134 S. Ct. at 2476. This bears on the Border Search Exception because searches incident to an arrest are another one of the narrow exceptions to Fourth Amendment protection granted in order to further governmental interests. *Id.* The court held that the search of the cell phone's digital contents did not further either of the two purposes of the exception: (1) to protect evidence from destruction by the defendant, or; (2) to protect officers from weapons hidden on defendant's person. *Id.* at 2487. The Court in *Riley* explained that it "generally determines

whether to exempt a given type of search from the warrant requirement by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." *Id*. The court explained that the purpose of the exception would not be furthered by searches of the digital contents of the cell phone. *Id*. at 2486. On balance, it was determined that the privacy interests involved in a search of the digital contents of a cell phone outweighed the governmental interests in that arena. *Id*. at 2487.

The Ninth Circuit Court of Appeals attempted to apply the same logic to a Border Search in *United States v. Cotterman*, in which the defendant's laptop was taken at the border and driven 170 miles away for a five-day forensic examination, during which deleted files containing child pornography were recovered. *Cotterman*, 709 F.3d 952, 959 (9th Cir. 2013). Noting that the Court "has never defined the precise dimensions of a reasonable border search, instead pointing to the necessity of a case-by-case analysis," the Ninth Circuit held that the private information held on the computer combined with the "exhaustive," search that "took days to turn up contraband," struck the balance in favor of the Defendant's privacy interests. *Id*. at 966. By contrast, just years earlier in *United States v. Arnold*, the Ninth Circuit Court of Appeals also held that a several-hour-long search of the Defendant's laptop, which uncovered child pornography, was reasonable. *Arnold*, 533 F.3d 1003, 1006 (9th Cir. 2008). The court explained that the search was not offensive to the defendant because it was logically no different from a search of luggage that could occur at the border. *Id*. at 1010.

CBP Agent Stubbs' forensic search of Petitioner Escaton's digital devices was reasonable not only because it took place at the border but also because the method used was reasonable given the circumstances. When the Officer in *Riley* discovered evidence of the defendant's gang

affiliation, the evidence did not help him disarm the defendant or prevent the destruction of evidence, the two legitimate governmental interests that could outweigh intrusions into privacy. *Riley*, 134 S. Ct. at 2485. When CBP Agent Stubbs forensically examined Petitioner Escaton's digital devices, she uncovered evidence of criminal activity and malware within hours, much like the officer in *Arnold*, and fulfilled her duty to prevent crime at the border. (R. at 3); *Arnold*, 533 F.3d at 1006. Therefore, because the search pursued the legitimate governmental interests for which the exception was created, and those interests outweighed the Petitioner's privacy interests, particularized suspicion was not required. If the Ninth Circuit's analysis in *Cotterman* was persuasive, even given its disruption of well-established precedent, the search of Petitioner Escaton's digital devices was still distinguishable from the forensic search in *Cotterman*.

The forensic search conducted on Petitioner Escaton's devices "typically took several hours," (R. at 3), and by contrast, the search of Cotterman's devices spanned five days, entailed displacing the digital devices 170 miles away from their owner, and even included recovering deleted files, *Cotterman*, 709 F.3d at 959. The forensic search of Petitioner Escaton's digital devices simply entailed using the technology to gain entry to locked files, and to detect of traces of malware on a USB device, all within several hours and at the same location Petitioner Escaton was held. (R. at 3). The proximity of the search to the Petitioner enabled the defendant to protest or monitor the search of his devices if he wished, and the short duration of the search did not allow the government to conduct the same exhaustive search conducted in *Cotterman*. *Cotterman*, 709 F.3d at 959.

This court should uphold CBP Agent Stubb's forensic search of Petitioner Escaton's laptop because the governmental interests of uncovering contraband and preventing smuggling are better served by allowing forensic digital searches absent reasonable suspicion.

II. NARROWLY TAILORED REQUESTS FOR CELL SITE LOCATION INFORMATION DO NOT CONSTITUTE A FOURTH AMENDMENT SEARCH BECAUSE INDIVIDUALS DO NOT HOLD A REASONABLE EXPECTATION OF PRIVACY IN LIMITED AMOUNTS OF LOCATION INFORMATION

"We have long held that the 'touchstone of the Fourth Amendment is reasonableness.'" *Ohio v. Robinette*, 519 U.S. 33, 39 (1996) (Citing *Florida v. Jimeno*, 500 U. S. 248, 250 (1991)).

A. The Fourteenth Circuit Correctly Upheld the District Court's Denial of Petitioner's Motion to Suppress Evidence Because Petitioner Voluntarily Conveyed the Information to a Third-Party Wireless Carrier and Thus Lacks a Reasonable Expectation of Privacy in the Information

This Court, in *Carpenter*, did not extend the third-party doctrine, which would defeat an individual's reasonable expectation of privacy, to seven days of historical CSLI. However, here, the present case involves two different historical CSLI data requests, each much more limited than the seven days requested by the Government in the *Carpenter* case. The Government narrowly curtailed the scope of its various requests to the Three Days Records, and the Weekday Records, which was narrowed only to the times of the Mariposa banks hours of operation. (R. at 5; aff. ¶ 17).

"Our decision today is a narrow one. . . . We do not disturb the application of *Smith* and *Miller*." *Carpenter v. United States*, ____ (2018). "This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith v. Maryland*, 442 U.S. 735, 743-744.

Reasonably limited and minimal amounts of CSLI data voluntarily conveyed to a third-party entity falls within the third-party doctrine and defeats an individual's reasonable expectation of privacy. In *Smith v. Maryland*, this Court held that the government's installation and recording of contents from a pen register did not constitute a Fourth Amendment search because individuals convey the phone numbers they dial to their phone company, and whether

they subjectively knew this, it was objectively reasonable that they had this knowledge. 442 U.S. 735, 742, 745-746. The pen register was a device that could be installed onto a telephone to only reveal the phone numbers called by the attached phone device. *Id*. at 741. Additionally, in *United States v. Miller*, 425 U.S. 435, 446, this Court utilized the third-party doctrine to reject an individual's argument that he held a reasonable expectation of privacy into the bank records he voluntarily conveyed to the bank.

Petitioner holds no reasonable expectation of privacy into the narrowly curtailed CSLI data requests made by the Government because the request was reasonably limited and contained insufficient amounts of information to infringe on Petitioner's reasonable expectation of privacy. Here, Petitioner conveyed CSLI to his wireless carrier, a third-party entity. Now, this Court has grappled with the issue of whether or not CSLI is "voluntarily" conveyed by individuals to third-party entities. We concede, like many answers to difficult legal questions involving novel technologies, that this question is not straightforward nor is it easy to draw lines for all Circuit Courts to adopt. Individuals surely know, at least in a general sense, that on a constant basis, they offer various data to the wireless carriers they contract with, whether it be from or general knowledge.

The Fourteenth Circuit correctly upheld the denial of Petitioner's Motion to Suppress Evidence because the third-party doctrine should extend to such limited amounts of CSLI data that the Government cannot aggregate to paint intimate details of an individual's life.

B. Even if the Court Holds That the Third-Party Doctrine Not Extend to Narrowly Curtailed Requests for Cell-Site Location Information, the Government's Reasonable Requests of Petitioner's information Do Not Infringe on His Expectation of Privacy

An overarching concern of the Court during its recent forays into cases intersecting the Fourth Amendment and emerging technologies lies in the aggregation of data accrued from

technology that can conceivably be pieced together to form intimate details about individuals, such as the activities they may partake in or any affiliations they may hold. *See U.S. v. Jones*, 132 S. Ct. 945 (2012); *Riley v. California*, 134 S. Ct. 2473 (2014); *Carpenter v. US*, 138 S. Ct. 2206 (2018). Here, the Government limited its request for CSLI to focus exclusively on timeframes in which the crimes it was investigating likely occurred, and the sum of the information did not rise to the level where the Government could piece such intimate details of Petitioner.

"We have long held that the 'touchstone of the Fourth Amendment is reasonableness.'" *Ohio v. Robinette*, 519 U.S. 33, 39 (1996) (Citing *Florida v. Jimeno*, 500 U. S. 248, 250 (1991)). In *U.S. v. Jones*, 132 S. Ct. 945, 962-964 (2012) (Alito, J., concurrence), Justice Alito illustrated a key concern with governmental aggregation of technological data, as large amounts of it can be used together to paint intimate details of the private and intimate lives of individuals.

Notwithstanding whether the Court extends the third-party doctrine to narrowly curtailed requests for historical CSLI, the government's limited requests for an individual's CSLI in a reasonable manner focused on investigation of criminal activity. Fourth Amendment doctrine has allowed many exceptions to the warrant requirement, but it additionally has provided instances where a standard of less than probable cause be met before privacy interests of an individual are impeded. *Terry v. Ohio*, 392 U.S. 1 1968 (holding a standard a reasonable suspicion be required without any judicial order to initiate a stop of an individual an officer suspects may be in the process of committing a crime).

The Government internally limited the scope of its request and had to meet the SCA's standard, requiring "reasonable grounds to believe that . . . the records or other information sought are relevant and material to an ongoing criminal investigation" to access the CSLI data.

Coupled with the requirement that an affidavit be submitted and the request granted by a magistrate judge, the SCA's statutory scheme provides a limit on the government to not overreach and violate Petitioner's privacy rights.

The concerns that Justice Alito asserted in *Jones* about aggregation of data are not present here. The Government limited its requests for CSLI to specific, narrow points in which crimes had occurred. The Weekday Records are narrowed to specific timelines in which Mariposa was open for business, and the requests involved 10 weekdays at 8am-6pm local time. This timeline, common to be the typical workweek, would likely implicate only the location of an individual at their place of business. The Three Day Records, narrowly tailored to evidence indicating that crimes had occurred on those days, especially when compared to the *Carpenter* seven days, does not implicate Justice Alito's concerns of aggregation. The amount of information is so minimal as to not offend those principles.

Should the Court hold that the third-party doctrine not extend to narrow requests for CSLI, the Government's actions here were still reasonable and did not infringe Petitioner's reasonable expectation of privacy.

1. *Public safety would be at risk if law enforcement could not access even limited amounts of historical cell-site location information without a warrant*

Law enforcement, especially in dealing with complex criminal activities involving multiple criminal actors and crimes, often must take a reactionary role in its investigations. Historical CSLI affords law enforcement the ability to retroactively determine locations of an individual. While this technology raises obvious concerns allowing law enforcement knowledge of an individual's movements they could not otherwise have accrued, technology providing law enforcement a snapshot of retroactive actions is neither a temporary issue to grapple with nor is this issue a novel one for courts. Various courts have confronted issues such as on the topic of

bank records or other records that provide intimate personal information. *United States v. Miller*, 425 U.S. 435 (1976).

While individuals maintain tremendous privacy rights and concerns about its rights in relation to emerging technology, law enforcement's interests in providing safety to the general public, and doing so efficiently, must be taken into account. *See United States v. Knotts*, 460 U.S. 276 (1983).

The Government's requests of Petitioner's historical CSLI was vital for law enforcement to determine whether Petitioner was implicated in an ongoing ATM skimming scheme. Without it, law enforcement likely would have struggled to make progress on its investigation into the ATM skimming considering the dearth of information it had. Mariposa's internal investigation had yielded ranges in time in which the crimes were likely to have occurred and provided the Government three surveillance photos of the likely culprit, but they lacked any substantial evidence and the criminal actors had already committed at least seven different criminal acts and caused $50,000 in financial injury. (R. at 3-4).

Because of the immense value of historical CSLI data as a tool for law enforcement to investigate serious crimes, especially in light of a potential diminishing of the third-party doctrine, the Government's interest in employing tools to provide the public safety from criminal actions should be heavily weighed.

C. The Government's Narrowed Requests of Cell Tower Dump Information Do Not Constitute a Fourth Amendment Search Because They Do Not Contain Personal Identifying Information or the Content of Communications

Cell tower dump information requests, often made in exceptionally short intervals, only contain a list of each phone number connecting to particular cell towers in a given interval. (R. at 4). They do not reveal the content of communications nor do they reveal who a person may have

communicated with. (R. at 4). As cell tower dumps are limited to short timeframes, the government is unable to piece together intimate details about the private details of an individual's life. Here, the Government limited its tower dump requests to such a limited timeframe of 30 minute intervals immediately before and after the ATM skimming crimes occurred (R. at 4), and it could provide the ability to narrow potential suspects at the start of investigations. Requiring a warrant issued on probable cause for the government to receive tower dump information would seriously impede law enforcement's ability to investigate crimes, especially serious conspiratorial ones.

"We do not express a view on matters not before us" such as "'tower dumps' (a download of information on all the devices that connected to a particular cell site during a particular interval)." *Carpenter*, 138 S. Ct. 2206, 2220 (2018).

Narrow government requests for information, even location information, bearing little to no personal identifying information or content of communications do not infringe on an individual's reasonable expectation of privacy if the requests are so temporally limited as to not implicate the concerns of providing the government intimate details of the individual. *See Jones*, 132 S. Ct. 945 (2012). In *Carpenter*, this Court had before them the issue of historical CSLI and not tower dumps. 138 S. Ct. 2206, 2220 (2018). However, this Court's concerns with historical CSLI revolved around the magnitude of the information and the potential aggregation of information that can be used to reveal intimate details about an individual's life. *Id*. at 2215.

The Government's narrow request of tower dump information did not constitute a Fourth Amendment search because the information does not contain any personal identifying information or content of communications and was so temporally limited that it does not offend the privacy interests of Petitioner. Governmental requests for tower dump information do not

focus on an individual but rather pinpoint specific cell-site towers to provide them the list of each phone number connecting with that particular cell tower in a limited timespan. This differs from requests for historical CSLI information, which involve seeking a judicial order to obtain, from a wireless cell phone carrier, an individual's cell-site records. (R. at 4-5). Here, the tower dump requests were narrowed to 30 minute intervals before and after the surveillance photos identified the suspect who skimmed the three ATM machines. (R. at 4). Additionally, the Government limited these tower dump requests to narrow the scope of who could be the man in the black sweatshirt in the surveillance photographs. (R. at 4). Accordingly, the concerns of the *Carpenter* Court do not apply to tower dumps because of the limited nature of data requested as well as the minimal invasion into Petitioner's privacy.

The Fourteenth Circuit correctly upheld the Government's requests of cell tower dump information because the requests did not infringe Petitioner's reasonable expectation of privacy and thus do not constitute a Fourth Amendment search as they contained no personal information and were narrowly tailored to the precise times before and after a crime occurred.

CONCLUSION

For the foregoing reasons, Respondent respectfully requests this Court affirm the Fourteenth Circuit Court of Appeals decision affirming the District Court's denial of Petitioner's Motion to Suppress Evidence.

Dated: February 10, 2019

Respectfully Submitted,

Attorneys for
Respondent