Team P17

No. 4-422

IN THE

SUPREME COURT OF THE UNITED STATES

FALL TERM 2019

Jayne AUSTIN,
Petitioner,

V.

UNITED STATES OF AMERICA,
Respondent.

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

BRIEF FOR THE PETITIONER

October 6, 2019

COUNSEL FOR PETITIONER

TABLE OF CONTENTS

TABLE OF CONTENTS (CONT.)

TABLE OF AUTHORITIES

Page(s)

Cases

SUPREME COURT OF THE UNITED STATES

TABLE OF AUTHORITIES (CONT.)

TABLE OF AUTHORITIES (CONT.)

UNITED STATES COURTS OF APPEAL

Constitutional Provisions

Federal Statutes

TABLE OF AUTHORITIES (CONT.)

Page(s)

Other Authorities

ISSUES PRESENTED

I. Does an individual have standing to contest a warrantless search of a rental car when he or she is not listed on the rental agreement, but has implied permission from the authorized driver to use the car?

II. Does the Fourth Amendment require law enforcement to secure a warrant to obtain 92 days' worth of an individual's GPS tracking information from a mobile software application?

No. 4-422

IN THE

SUPREME COURT OF THE UNITED STATES

FALL TERM 2019

Jayne AUSTIN,
Petitioner,

V.

UNITED STATES OF AMERICA,
Respondent.

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

BRIEF FOR THE PETITIONER

STATEMENT OF FACTS

Petitioner Jayne Austin ("Ms. Austin") is an activist that spends her time investigating the financial crimes of the United States' banking industry. R. at 1. She is a minimalist that prides herself on her independent nomadic lifestyle. R. at 1. Ms. Austin prefers to live her life without reliance on any technology or other material things. R. at 18. For these reasons, Ms. Austin does not even have a permanent residence and, instead, lives in co-habitation facilities where she can

temporarily rent living spaces. R. at 1. Because of this desire to be "off the grid," Ms. Austin does not create online accounts for any software applications ("apps"). R. at 18. Rather, she uses the accounts of her on-and-off again partner, Ms. Martha Lloyd ("Ms. Lloyd"), with Ms. Lloyd's permission, including YOUBER and YOUBEREATS. R. at 2. Ms. Lloyd gave this permission by sharing her login information with Ms. Austin. R. at 18. Ms. Lloyd also made Ms. Austin an authorized user on her credit card and has yet to remove her or change any account passwords despite the status of their relationship. R. at 18-19.

On July 27, 2018, Ms. Lloyd created a YOUBER account. R. at 20. YOUBER is a popular mobile app similar to a standard rental car service with approximately 40 million users in the U.S. R. at 2 and 22. It allows a person to rent YOUBER-owned cars at a fixed hourly rate after a rental agreement is made in the app. R. at 2. Once a YOUBER user is done with a car, another user is free to rent the car on the same day. R. at 23. YOUBER cars are identifiable by a small, bright pink YOUBER logo. R. at 2. The YOUBER app connects individuals to cars through the Bluetooth and GPS technologies on their cellphones. R. at 2.

Using the user's cellphone location technology, YOUBER tracks their cars and the user's account throughout the entire rental period. R. at 3. The timestamped location of every YOUBER car is recorded every two minutes using the Smoogle's satellite mapping technology. R. at 4 and 22. Upon creating an account in the app, the YOUBER account creator must accept YOUBER's terms and conditions, including a clause permitting YOUBER to track the location of the rented car. R. at 3-4. The only time a YOUBER user is notified about the app's monitoring is when the user initially signs up for the account. R. at 23. YOUBER collects information about the user's devices used to access YOUBER services including the exact dates, times, duration, and specific links clicked. R. at 29. Only the account creator is aware that YOUBER provides any information

YOUBER collects to third-party service providers. R. at 29. If an individual uses someone else's YOUBER account, he or she is never notified of the data YOUBER collects. R. at 24.

A. Warrantless Search of the YOUBER Car Ms. Austin Rented.

Ms. Austin has relied on the YOUBER app as one of her primary means of transportation since Ms. Lloyd gave her permission to download the app on her phone using Ms. Lloyd's login information. R. at 2. Ms. Lloyd never specifically told or gave Ms. Austin any indication that Ms. Austin could no longer use her YOUBER account. R. at 20. Regardless of the status of their relationship, Ms. Austin continued to frequently use YOUBER to travel to work. R. at 2.

On January 3, 2019, Ms. Austin rented a car through the YOUBER app on her phone. R. at 2. Later that day, Officer Charles Kreuzberger ("Officer Kreuzberger") pulled Ms. Austin over for failure to stop at a stop sign. R. at 2. In an effort to show her lawful possession of the rental car, Ms. Austin voluntarily provided Officer Kreuzberger her license and the YOUBER app on her cellphone. R. at 2. Officer Kreuzberger told Ms. Austin that, because her name was not listed as the renter on the rental agreement in the YOUBER app, he did not need her consent to search the car. R. at 2. Without a warrant or Ms. Austin's consent, Officer Kreuzberger searched the trunk of the car, where any renter of the YOUBER car could keep their personal effects. R. at 3. Some of the items Officer Kreuzberger found in the YOUBER car included clothes, an inhaler, three pairs of shoes, a collection of signed Kendrick Lamar records, a cooler full of tofu, kale, and kombucha, a BB gun modeled after a handgun with the orange tip removed, a duffel bag full of money and blue dye packs, a maroon ski mask, bedding, and a pillow. R. at 3. Officer Kreuzberger noted that the car appeared to be "lived in," despite the fact that Ms. Austin had only rented the car earlier that same day. R. at 2-3.

During the stop, Officer Kreuzberger received a dispatch to look out for a 2017 Black Toyota Prius with a YOUBER logo driven by a suspect who allegedly robbed a *Darcy and Bingley Credit Union*. R. at 3. A surveillance camera caught a partial license plate number "R0L." R. at 3. The suspect was seen wearing a maroon ski mask and using a .45 caliber handgun. R. at 3. Based on the items found in the YOUBER car and the dispatch about the bank robbery, Officer Kreuzberger arrested Ms. Austin under suspicion of bank robbery. R. at 3.

B. Obtaining Ms. Austin's Cellphone Location Data from YOUBER Without a Warrant.

Following Ms. Austin's arrest, Detective Boober Hamm ("Detective Hamm") began investigating five other *Darcy and Bingley Credit Union* robberies in California and Nevada. R. at 1 and 3. Those five robberies occurred between October 15, 2018 and December 15, 2018. R. at 3. All six robberies Detective Hamm investigated used a car with a YOUBER logo. R. at 3. Five of the six robberies were associated with a 2017 Black Toyota Prius with the license plate "R0LL3M." R. at 4. The other with a 2016 Yellow Volkswagen Beetle with the license plate "FEEARLY." R. at 4. Detective Hamm checked Officer Kreuzberger's notes and saw that, when she was arrested, Ms. Austin had rented a 2017 Black Toyota Prius through YOUBER. R. at 3. Detective Hamm then served a subpoena duces tecum on YOUBER to obtain all the GPS and Bluetooth information from Ms. Lloyd's account that Ms. Austin also used between October 3, 2018 and January 3, 2019. R. at 3. Detective Hamm did not secure a warrant to obtain Ms. Austin's cellular location data from Ms. Lloyd's YOUBER account. R. at 10.

The 92 days' worth of data Detective Hamm subpoenaed from YOUBER indicated that Ms. Lloyd's account was used to rent cars near the locations and at the times of the six *Darcy and Bingley Credit Union* robberies. R. at 4. Based on this location data, Ms. Austin was charged with six counts of bank robbery under 18 U.S. Code § 2113, Bank Robbery and Incidental Crimes.

SUMMARY OF ARGUMENT

The Fourth Amendment protects individuals from unlawful searches and seizures by the government. First, Ms. Austin's Fourth Amendment rights were violated when Officer Kreuzberger conducted a warrantless search of the YOUBER rental car. Ms. Austin has standing to contest the warrantless search because she had both a property interest and a reasonable expectation of privacy in the car. Ms. Austin was legitimately present when the search occurred because she was in exclusive control of the car and had implied permission to use the car from the authorized renter. The Sixth Circuit's totality-of-the-circumstances test is the proper way to determine whether an unauthorized rental car driver has a reasonable expectation of privacy in the car because it balances both the government's interest in obtaining evidence and the individual's constitutional protections. Thus, the evidence unlawfully obtained during the warrantless and unreasonable search of the rental car should be barred pursuant to the exclusionary rule.

Second, Detective Hamm failed to secure a warrant for Ms. Austin's cellular location history. As technology advances, Fourth Amendment protections should advance with it, preventing the government from conducting warrantless searches on information society reasonably expects to be protected. Here, Ms. Austin had a reasonable expectation of privacy in the 92 days' worth of GPS information YOUBER gathered from her cellphone. Despite being disclosed to YOUBER, the Third-Party Doctrine does not apply because Ms. Austin did not voluntarily convey this information to YOUBER and was unaware that YOUBER was tracking her movements. Due to the duration and depth of these records, and the unreasonable exposure of Ms. Austin's privacy, law enforcement should have secured a warrant. Allowing the government to obtain these records without a warrant permits it to track any individual, anytime, anywhere.

Accordingly, this Court should REVERSE the decision of the Thirteenth Circuit.

STANDARD OF REVIEW

The standard of review for questions of law is de novo. *Bose Corp. v. Consumers Union of U.S., Inc.*, 466 U.S. 485, 499 (1984).

ARGUMENT

I. MS. AUSTIN HAS STANDING TO CONTEST THE SEARCH OF THE RENTAL CAR BECAUSE SHE WAS LEGITIMATELY PRESENT AND HAD A REASONABLE EXPECTATION OF PRIVACY IN THE CAR.

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. CONST. amend. IV. A search conducted without a warrant issued upon probable cause is per se unreasonable, subject only to a few narrow exceptions. *Schneckloth v. Bustamonte*, 412 U.S. 218, 219 (1973). The parties have stipulated that there are no exceptions to the warrant requirement for the warrantless search in the case at issue. R. at 31. In the face of a warrantless search, an individual must have standing to invoke a Fourth Amendment protection; meaning an individual must have a cognizable Fourth Amendment interest in the place searched. *Jones v. United States*, 362 U.S. 257, 261 (1960); *see also Byrd v. United States*, 138 S.Ct. 1518, 1530 (2018).

The Fourth Amendment protects both property rights and reasonable expectations of privacy. *Florida v. Jardines*, 569 U.S. 1, 5 (2012); *see also Katz v. United States*, 389 U.S. 347 (1967). These two concepts—property rights and expectations of privacy—are often intertwined. *Byrd*, 138 S.Ct. at 1527. In *Jones*, this Court held that a person does not need to have a recognized property interest where a search occurs to have standing to contest that search. 362 U.S. at 259. An individual can have standing if he or she is legitimately present on the premises. *Id*. at 267. However, legitimate presence on the premises alone is insufficient to accord a reasonable expectation of privacy because "it creates too broad a gauge for measurement of Fourth

Amendment Rights." *Byrd*, 138 S.Ct. at 1527 (citing *Rakas v. Illinois*, 439 U.S. 128, 142 (1978)). An expectation of privacy can be legitimate if it has a source outside of the Fourth Amendment, such as a reference to a property-based interest or an understanding that is permitted by society. *Id*. (citing to *Rakas*, 439 U.S. at 144, n. 12).

A. Ms. Austin has a Property Interest in the Rental Car because she was Legitimately Present at the Time of the Search.

An individual can have a *legitimate expectation of privacy* in premises that he or she does not own because he or she is lawfully present on the premises, and therefore has standing to claim Fourth Amendment protection. *Rakas*, 439 U.S. at 142-43 (emphasis added). For example, in *Jones* the defendant was staying at a friend's apartment when police observed him placing narcotics outside a window. 362 U.S. at 259. Police searched the apartment and arrested the defendant. *Id*. at 258. Prior to trial, the defendant moved to suppress the evidence seized by the police during the search of the apartment. *Id*. at 259. The government argued that the defendant did not have standing to challenge the legality of the search because he did not have a property or possessory interest in the friend's apartment or in the evidence seized. *Id*. This Court rejected the government's argument and held that the defendant did have standing to assert his Fourth Amendment rights and challenge the legality of the warrantless search because the defendant was legitimately on the premises. *Id*. at 267. This Court reasoned that the defendant's presence in the friend's apartment was legitimate because he had a key, was an overnight guest, and was present during the search. *Id*. at 259. Thus, the defendant did not need to own the premises searched or have a substantial possessory interest in the property seized to have standing. *Id*. at 261.

Similar to *Jones*, Ms. Austin does not need to have ownership of the car searched or have a substantial possessory interest in the property seized to have standing. Instead, Ms. Austin must simply show that she was legitimately present in the car. Her presence was legitimate because she

was given the proverbial "keys" when Ms. Lloyd allowed her to use the YOUBER account, she was an authorized user on the credit card that was on the account, and she was present at the time of the search. R. at 18-19. The government argues that Ms. Austin was not legitimately present in the car because she did not have explicit permission from Ms. Lloyd to rent the car through YOUBER on January 3, 2019. However, Ms. Lloyd admits that Ms. Austin had permission to use Ms. Lloyd's login information to her online accounts, including YOUBER. R. at 18-19. Ms. Lloyd never rescinded her permission or changed her login and password information to prevent Ms. Austin from using the YOUBER app. R. at 19. Ms. Lloyd had the opportunity to change the password of her YOUBER account or forbid Ms. Austin from using the account but took no such action. R. at 19. Thus, Ms. Austin was legitimately present in the rental car she lawfully possessed and has standing to contest the warrantless search of the car.

B. Ms. Austin Had a Reasonable Expectation of Privacy in the Rental Car Even Though She was Not Listed on the Rental Agreement.

The mere fact that drivers in lawful possession or control of rental cars are not listed on the rental agreements does not diminish their otherwise reasonable expectation of privacy. *Byrd,* 138 S.Ct. at 1530. To determine whether an individual has a legitimate expectation of privacy under the Fourth Amendment, the individual must have exhibited a subjective expectation of privacy that society readily recognizes as reasonable. *Katz,* 389 U.S. at 361 (Harlan, J., concurring). A reasonable expectation of privacy exists in the closed compartment of an individual's car, such as the trunk or glove compartment. *Cal. v. Acevedo,* 500 U.S. 565, 573 (1991).

In *Byrd,* the defendant was not an authorized driver of a rental car. 138 S.Ct. at 1523. He was given the keys by his friend, who was the authorized driver on the rental agreement. *Id*. at 1524. The rental agreement explicitly stated that permitting an unauthorized driver to drive the car would violate the agreement. *Id*. Later, the defendant was stopped by State Troopers for a

traffic infraction. *Byrd*, 138 S.Ct. at 1524. When the Troopers learned that the defendant was not listed as the authorized driver of the rental agreement, they proceeded to conduct a warrantless search of the car. *Id*. at 1525. The defendant was arrested when the Troopers found body armor and bricks of heroin in the car as a result of the search. *Id*. At trial, the defendant moved to suppress the evidence arguing it was obtained in violation of his Fourth Amendment rights. *Id*. The trial court concluded, and the Third Circuit agreed, that the defendant did not have a reasonable expectation of privacy because he was not listed on the rental agreement. *Id*.

However, this Court reversed the decisions below in *Byrd* because the bright line rule created—that drivers not listed on rental agreements always lack an expectation of privacy—was too restrictive of a view of the Fourth Amendment.[1] *Id*. at 1527 and 1531. This Court reasoned that, for Fourth Amendment purposes, there is no difference between a driver who is authorized to drive a rental car and one that is not authorized that would eliminate the expectation of privacy.[2] *Id*. at 1529. This Court promulgated several innocuous reasons as to why an unauthorized driver might drive a rental car. *Id*. For example, the authorized driver may consent to their friend borrowing his or her rental car to go shopping. The fact that the friend is an unauthorized driver would have no bearing on whether the friend has less of an expectation of privacy in the car. *Id*. The proper analysis to determine an expectation of privacy looks to *Katz*. *Id*. at 1527.

Ms. Austin's privacy is of utmost importance to her which is why she lives a minimalist lifestyle off the grid. R. at 1 and 18. Ms. Austin exhibited a subjective expectation of privacy in

[1] This Court's ruling in *Byrd* abrogated the bright line rule created by the Third, Fourth, Fifth, and Tenth Circuits that unauthorized drivers of rental cars had no expectation of privacy. 138 S.Ct. at 1531. *See United States v. Kennedy*, 638 F.3d 159 (3rd Cir. 2011); *United States. v. Seeley*, 331 F.3d 471 (5th Cir. 2003); *United States v. Wellons*, 32 F.3d 117 (4th Cir. 1994); and *United States v. Roper*, 918 F.2d 885 (10th Cir. 1990).

[2] An unauthorized driver's expectation of privacy may diminish if the driver is not in lawful possession or control of the rental car. *Id*. at 1529 (citing to *Rakas*, 439 U.S. at 141, n. 9).

the rental car because the search was conducted in the closed compartments of the car. R. at 3. Here, Ms. Austin does not lose her subjective expectation of privacy simply because she was not listed on the YOUBER rental agreement. She was in lawful control and exclusive dominion of the YOUBER car. The next step of the *Katz* inquiry is to determine whether this subjective expectation of privacy is reasonable. Circuit courts are split as to whether unauthorized rental car drivers have standing to claim Fourth Amendment protections. *See United States v. Smith*, 263 F.3d 571 (6th Cir. 2001) (adopting a totality-of-the-circumstances framework to determine whether an unauthorized rental car driver has standing); *see also United States v. Thomas*, 447 F.3d 1191 (9th Cir. 2006) (holding that an unauthorized driver may have standing to challenge a search if he or she has received permission to use the car); and *United States v. Muhammad*, 58 F.3d 353 (8th Cir. 1995) (holding that an unauthorized rental car driver must provide sufficient evidence that he or she had permission to use the rental car to have standing).

1. This Court should adopt the Sixth Circuit's totality-of-the-circumstances test to determine that Ms. Austin had a subjective and reasonable expectation of privacy in the rental car.

To determine whether Ms. Austin's subjective expectation of privacy is reasonable, this Court must consider the totality of the circumstances. A totality-of-the-circumstances analysis is the proper way to determine whether there is a reasonable expectation of privacy that demands Fourth Amendment protection. *See Ohio v. Robinette*, 519 U.S. 33, 34 (1996) ("The [Fourth] Amendment's touchstone is reasonableness, which is measured in objective terms by examining the totality of the circumstances"); *see also Rakas*, 439 U.S. at 152 (Powell, J., concurring) ("The ultimate question is 'whether one's claim to privacy from government intrusion is reasonable in light of all the surrounding circumstances,' rather than reasonable within an arbitrary bright line test"). In *Robinette*, this court emphasized the importance of measuring reasonableness by

examining the totality of the circumstances. 519 U.S. at 39. Similarly, here, this Court should adopt a framework that emphasizes the fact-specific nature of whether an expectation of privacy is reasonable instead of adopting arbitrary rigid rules. *Id*.

In *Smith*, the Sixth Circuit considered a range of factors surrounding an unauthorized driver's use of a rental car to determine whether he had standing to raise Fourth Amendment protections. 263 F.3d at 586. The factors used were: (1) whether the defendant had a valid driver's license at the time of the search; (2) whether the defendant was able to provide law enforcement with the rental agreement and sufficient information about the car; (3) whether there was any relationship between the defendant and the authorized driver listed on the rental agreement that was not an "unrelated third party"; (4) whether the defendant had received permission to use the rental car from the authorized driver; and (5) whether the defendant had established a business relationship with the rental car company. *Id*.

Applying the first factor of the totality-of-the-circumstances test, Ms. Austin had a valid driver's license which she presented to Officer Kreuzberger when she cooperated during the traffic stop. R. at 2. Second, Ms. Austin showed Officer Kreuzberger the YOUBER app on her cellphone to demonstrate she was legitimately in possession of the 2017 Black Toyota Prius. R. at 2. Third, Ms. Austin had a romantic relationship with Ms. Lloyd that lasted several years. R. at 18. Even though Ms. Austin and Ms. Lloyd were not involved at the time of the car's search, they have remained updated on each other's lives, evidenced by their correspondence with each other. R. at 19. Ms. Austin and Ms. Lloyd are not "unrelated third parties" as they are both deeply involved in each other's lives, so much so that Ms. Lloyd gave Ms. Austin access to her personal information and Ms. Austin is currently an authorized user on her credit card. R. at 18-19. Fourth, Ms. Lloyd gave Ms. Austin permission to use her YOUBER account by voluntarily providing her with the

account's login information. R. at 18-19. Ms. Lloyd has never rescinded her permission for Ms. Austin to use her YOUBER account to rent cars. R. at 19. Further, she has never changed the passwords to her YOUBER account, nor explicitly denied Ms. Austin use of her account. R. at 19. Fifth, there is a strong business relationship between Ms. Austin and YOUBER because Ms. Austin has been frequently renting cars through YOUBER and depends on it as a primary mode of transportation. R. at 2. Moreover, Ms. Austin has been paying for YOUBER's services with her authorized credit card. R. at 20. In light of the totality of the circumstances surrounding Ms. Austin's use of the car, Ms. Austin has a reasonable expectation of privacy giving her standing to contest the warrantless search.

2. Alternatively, this Court should adopt the Eighth and Ninth Circuits' permission-based test to determine that Ms. Austin had joint authority of the car.

If this Court chooses not to adopt the Sixth Circuit's totality-of-the-circumstances test, this Court should adopt the Eighth and Ninth Circuit's permission-based test. The test adopted by those courts grants an unauthorized driver of a rental car standing at the time of the search if he or she received permission to use the car. *See Thomas*, 447 F.3d 1191; *see also United States v. Best*, 135 F.3d 1223 (8th Cir. 1998); and *Muhammad*, 58 F.3d 353. A permission-based test allows this Court to determine whether an unauthorized driver of a rental car "has joint authority over the car [and] may challenge the search to the same extent as the authorized renter." *Thomas*, 447 F.3d at 1199 (stating that "[t]his approach is in accord with precedent holding that indicia of ownership-including the right to exclude others-coupled with possession and the permission of the rightful owner, are sufficient grounds upon which to find standing" (citing to *Jones*, 362 U.S. at 266)).

In *Muhammad*, in connection with a drug investigation, police officers stopped the defendant while driving. 58 F.3d at 354. The car was leased to another individual and the

defendant was not an authorized driver of the car under the lease agreement. *Muhammad*, 58 F.3d at 354. After searching the car, police officers discovered cocaine in the trunk and arrested the defendant. *Id*. at 355. The defendant moved to suppress the evidence found during the search because it violated his reasonable expectation of privacy under the Fourth Amendment. *Id*. The government argued that the defendant lacked standing to challenge the warrantless search because the defendant did not provide any evidence indicating he had permission to use the car. *Id*. The Eighth Circuit stated that had the defendant provided "at least some evidence of consent or permission from the lawful owner/renter [of the car] to give rise to an objectively reasonable expectation of privacy," the defendant would have established standing. *Id*.

While the defendant in *Muhammad* failed to bring forth any evidence that he had permission to use the rental car, in the present case, Ms. Austin has presented several pieces of evidence that give rise to her objectively reasonable expectation of privacy in the YOUBER car. When Ms. Lloyd gave Ms. Austin her YOUBER login information, this was equivalent to Ms. Lloyd handing Ms. Austin her keys to the rental car, giving Ms. Austin joint authority over the car. R. at 18-19. While YOUBER may operate like a typical rental car service, the mobile platform is what sets it apart. R. at 2 and 23. There are no physical keys hand over, only login information. Further, Ms. Lloyd had ample opportunity to change her login information for YOUBER or disable her account entirely if she wished to "take back the keys" to the rental car but she did not. The permission-based test does not explicitly require that Ms. Lloyd give Ms. Austin permission *every time* she used a YOUBER car. To have consent to drive the car, the test only requires that the unauthorized driver provide sufficient evidence of permission to use the rental car. The fact that Ms. Austin properly had the "keys" to the YOUBER car, had the rental agreement on her cellphone, and willingly provided this information to Officer Kreuzberger at the time of the stop,

is sufficient evidence to demonstrate she had permission from Ms. Lloyd to use the car and had joint authority over the car.

The problem with the Eighth and Ninth Circuits' permission-based test is that the courts do not make clear what permission is sufficient to show joint authority over the car. Therefore, the totality-of-the-circumstances test is a better analysis of whether an unauthorized driver has a reasonable expectation of privacy in the car. The totality-of-the-circumstances test incorporates permission as part of its analysis and also looks to several other factors—such as the relationship between the authorized and unauthorized driver—that would provide this Court with a better understanding of whether a reasonable exception of privacy exists.

C. The Exclusionary Rule Bars the Use of any Evidence Obtained by the Unreasonable and Warrantless Search of the Rental Car.

All evidence obtained by unconstitutional searches and seizures is inadmissible in court under the exclusionary rule. *Mapp v. Ohio*, 367 U.S. 643, 654 (1961). The purpose of the exclusionary rule is to create a judicial remedy "designed to safeguard Fourth Amendment rights generally through its deterrent effect." *United States v. Calandra*, 414 U.S. 338, 347 (1974). One of these safeguards is the requirement that law enforcement obtain a judicially sanctioned warrant prior to conducting intrusive searches. U.S. CONST. amend IV. Warrants must be rooted in probable cause. U.S. CONST. amend IV. There are some instances where the time delay in obtaining a warrant justifies a warrantless search. *See, e.g.*, *Missouri v. McNeely*, 569 U.S. 141 (2013) (where this Court recognized that, based on the totality of the circumstances, there may be some instances that make obtaining a warrant impractical that would justify a warrantless search). However, the present case presents no such instance.

Here, the evidence obtained by Officer Kreuzberger was the result of an unconstitutional search. If Officer Kreuzberger suspected that Ms. Austin was not in lawful possession of the rental

car, or that the rental car had been used in criminal activity, Officer Kreuzberger had ample opportunity to request a warrant to search her car. There would have been no delay or potential destruction of evidence if Officer Kreuzberger had requested a telephonic warrant. Moreover, Officer Kreuzberger did not have any probable cause to search Ms. Austin's car. He had not received a dispatch to look out for a 2017 Black Toyota Prius with a YOUBER logo until after he had already searched the trunk of the car. R. at 3. Even if Officer Kreuzberger suspected Ms. Austin to have used the car in a crime, that suspicion alone did not justify a warrantless search. This Court has held that a person merely present in a car suspected to be used in a crime, does not lose immunities from search of his or her person to which he or she would otherwise be entitled. *United States v. Di Re*, 332 U.S. 581, 587 (1948). Ms. Austin's car was unlawfully searched; thus, the results of that search should be barred.

II. MS. AUSTIN'S CELL SITE LOCATION INFORMATION ("CSLI") FROM YOUBER WAS UNLAWFULLY SEARCHED BECAUSE THE GOVERNMENT FAILED TO OBTAIN THE WARRANT REQUIRED BY THE FOURTH AMENDEMENT UNDER *CARPENTER.*

The Fourth Amendment protects individuals from unreasonable searches and seizures by the government. U.S. CONST. amend. IV. The basic purpose of the Fourth Amendment is to "safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." *Camara v. Mun. Ct. of City and Cty. of S.F.*, 387 U.S. 523, 528 (1967). While the measure of the constitutionality of a search is reasonableness, warrantless searches are typically unreasonable where law enforcement utilize searches to discover evidence of a crime. *Carpenter v. United States*, 138 S.Ct. 2206, 2221 (2018) (citing to *Veronica School Dist. 47J v. Acton*, 515 U.S. 646, 652-53 (1995)). Even if there is probable cause of a crime, unreasonable warrantless searches remain unconstitutional. *Agnello v. United States*, 269 U.S. 20, 33 (1925).

Over time, the Fourth Amendment has expanded to protect expectations of privacy. *Katz*, 389 U.S. at 347. "What [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Id*. at 351. This Court reasoned that "it would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology." *Kyllo v. United States*, 533 U.S. 27, 33–34 (2001). For example, cellphones today are based on technology that was inconceivable a few decades ago. *Riley v. California*, 573 U.S. 373, 385 (2014). Modern cellphones contain "the privacies of life" in a person's hand that is equally worthy of protection under which the Founders created the Fourth Amendment. *Id*. at 403. As such, this Court applied this historic intention to modern day technology by requiring law enforcement to secure a warrant before probing a cellphone seized during a search incident to arrest. *Id*. With the advancements of technology, the government may have the ability to conduct twenty-four-hour surveillance of any individual; however, that does not permit the government to forego constitutional protections. *Carpenter*, 138 S.Ct. at 2215 (citing to *United States v. Knotts*, 460 U.S. 276, 283 (1983)).

General protections of privacy under the Fourth Amendment only extend so far. *United States v. Miller*, 425 U.S. 435, 442 (1976). An exception is created under the "Third-Party Doctrine" when a person knowingly exposes information to the public. *Id*. at 442. However, in this digital age, "the fact that information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection." *Carpenter*, 138 S.Ct. at 2216. Long term GPS monitoring of a car by the government impinges on expectations of privacy, even if those movements were disclosed to the public at large. *Id*. at 2215 (quoting *United States v. Jones*, 565 U.S. 400, 404-05 (2012)). Cellphones have the ability to record an individual's every movement, making their technology akin to that of a car's GPS monitoring. *Id*. at 2216. Without a warrant,

the extended duration of monitoring of an individual's location through his or her CSLI records is an unreasonable search under the Fourth Amendment. *Carpenter*, 138 S.Ct. at 2215.

Given the unique nature of cell site location information ("CSLI"), an individual holds a legitimate expectation of privacy in his or her physical movements recorded through CSLI. *Id*. at 2217. CSLI is generated by a cellphone continuously scanning the environment looking for the best signal. *Id*. at 2211. Most smartphones tap into the wireless network several times a minute, even if the owner is not using the device. *Id*. Every time the device connects, it generates a time-stamped record. *Id*. "In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection." *Id*. at 2223.

A. Ms. Austin Had a Reasonable Expectation of Privacy in her 92 Days of CSLI Complied by YOUBER.

The Fourth Amendment protects individual privacy interests that society recognizes as justifiably reasonable. *Smith v. Maryland*, 442 U.S. 735, 740 (1979). Intrusions by law enforcement into these expectations of privacy are searches that require a warrant. *Id*. A reasonable search under the Fourth Amendment depends on the context within which a search takes place. *New Jersey v. T.L.O.*, 469 U.S. 325, 337 (1985). The reasonableness of a search is determined by balancing the need to conduct the search against the invasion of an individual's legitimate expectation of privacy. *Id*.

To establish if an expectation of privacy is reasonable, courts look to the Framers' original intention of the Fourth Amendment. *Oliver v. United States*, 466 U.S. 170, 178 (1984). A central aim of the Framers was to limit over intrusive police surveillance. *Di Re*, 332 U.S. at 595. Additionally, courts consider society's expectations about what information deserves the most

protection from government invasion. *Oliver,* 466 U.S. at 178. Society often finds that an individual maintains a reasonable expectation of privacy in information that is not shared with the public eye. *Katz,* 389 U.S. at 357. Cellphone location information is not shared with the public eye in the traditional sense. *Carpenter,* 138 S.Ct. at 2210. An item such as a cellphone is practically an extension of the human body that follows its owner through public and private movements. *Id*. at 2218. Due to a cellphone's ability to achieve "near perfect surveillance," there is a heightened expectation of privacy when sharing such data. *Id.*

In *Carpenter*, this Court held that the government's warrantless acquisition of CSLI records constitutes a search under the Fourth Amendment because a right to privacy exists. *Id*. at 2217 and 2223. There, the trial court convicted the defendant of armed robbery when the government used the defendant's CSLI records as evidence of the crime. *Id*. at 2212. The records contained 127 days of location data. *Id*. at 2218. The government used this data to place the defendant in the areas of six armed robberies. *Id*. at 2213. The defendant made a motion to suppress the CSLI records provided by the wireless carriers because the government obtained the data without a warrant, violating the defendant's Fourth Amendment rights. *Id*. at 2212. This Court acknowledged that "although [CSLI] records are generated for commercial purposes, that distinction does not negate [the defendant's] anticipation of privacy in his physical location." *Id.* at 2217. The mapping of the defendant's cellphone's location over 127 days provided an all-encompassing record of his whereabouts. *Id*. This Court reasoned that the time-stamped data "provide[d] an intimate window into a person's life," revealing his personal associations beyond his physical movements and making the context of the search unreasonable. *Id.*

While a car's movements and final destination are voluntarily conveyed to onlookers, the data recorded from a cellphone going from public to private locations is not. *Id*. at 2215. "In fact,

historical cell-site records present even greater privacy concerns than the GPS monitoring of a car." *Carpenter*, 138 S.Ct. at 2218. Due to the progression of CSLI acquisition rapidly approaching GPS-level precision, this Court recognized that the government is required to obtain a warrant for CSLI records because it invaded the defendant's reasonable expectation of privacy in his physical movements. *Id*. at 2219. The depth and duration of this digital record allows the government to achieve near perfect surveillance of an individual. *Id*. at 2218. This Court took into consideration the heightened privacy concerns associated with more sophisticated systems and technological advancements in finding that law enforcement violated the defendant's Fourth Amendment rights. *Id*.; *see also Kyllo*, 533 U.S. 27 (holding that the use of thermal imaging devices to surveil a home was presumptively unreasonable without a warrant due to the intrusive nature of the sophisticated technology).

Just as the defendant in *Carpenter*, Ms. Austin maintains a reasonable expectation of privacy in her GPS information that Detective Hamm obtained from YOUBER. Ms. Austin's cellphone is an extension of her body. It follows her through both the public and private moments of her life. As such, the location data obtained from her cellphone is protected under society's understanding that there is a reasonable expectation of privacy in information from a cellphone. The records Detective Hamm obtained contained a vast amount of time-stamped data that depicted the intimate whereabouts of Ms. Austin's life any time she used a YOUBER car over 92 days. R. at 3 and 22. The duration of this comprehensive record raised concerns in *Carpenter* that should be echoed here as well. The immense amount of private data in Ms. Austin's CSLI records is protected by her reasonable expectation of privacy. Thus, the records are protected under the Fourth Amendment and require a warrant.

B. The Third-Party Doctrine Does Not Apply Because Ms. Austin Did Not Voluntarily Convey her CSLI to YOUBER.

The Third-Party Doctrine holds that a person does not maintain a reasonable expectation of privacy in information he or she voluntarily exposes to the public. *Miller*, 425 U.S. at 442. One of the main purposes of the Third-Party Doctrine is to correct the substitution effect of third parties acting on behalf of or at the direction of savvy criminal actors by allowing those individuals to substitute a hidden third-party exchange for a previously public act. Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 561 (2009). Simply because a person has a "diminished expectation of privacy does not mean that the Fourth Amendment falls out of the picture entirely." *Carpenter*, 138 S.Ct. at 2219 (citing to *Riley*, 573 U.S. at 392). This Court's holding in *Carpenter* demonstrated a crucial shift towards a more privacy conscious Fourth Amendment analysis in the face of technological advancements. Michael Price, Carpenter v. United States *and the Future Fourth Amendment*, 24 CHAMPION 48, 48 (2018). Many legal scholars viewed this holding as a significant departure from the Third-Party Doctrine established by *Katz*, *Miller*, and *Smith*. *Id*.

This Court applied the Third-Party Doctrine in *Miller* when law enforcement subpoenaed a bank for the defendant's account statements during a tax fraud investigation. 425 U.S. at 442. The defendant had a limited expectation of privacy in his account statements because the information was exposed to bank employees in the ordinary course of business. *Id*. Society would not reasonably expect the defendant's bank statements to have protected privacy interests because, in providing the transactions to the bank, the defendant risked having the documents turned over to law enforcement. *Id*. This Court held that the defendant did not have any Fourth Amendment protections over his account statements because the documents pertained to a business transaction between the defendant and the bank. *Id*. at 441. Additionally, because the defendant *voluntarily*

conveyed this information to the bank and the defendant did not own or possess the records, there was no justifiably reasonable expectation of privacy. *Miller*, 425 U.S. at 441 (emphasis added). Even if a defendant revealed the information under the assumption that it would only be used for a limited purpose by the trusted third party, the Fourth Amendment does not prohibit law enforcement from obtaining this information. *Id*. at 443.

Similarly, in *Smith v. Maryland*, this Court held that the Third-Party Doctrine applies to phone numbers a person dials because an individual does not have a reasonable expectation of privacy when he or she *conveys* phone numbers to the telephone company. 442 U.S. at 736 (emphasis added). This Court concluded that law enforcement did not need a warrant to obtain the information from a pen register—a device that recorded the outgoing phone numbers on a landline telephone. *Id*. A pen register differed significantly from the listening device on a public telephone booth used in *Katz* because the pen register did not acquire the *contents* of the communications, just the phone numbers. *Id*. at 741 (emphasis added).

Despite the fact that the Third-Party Doctrine stems from a reduced expectation of privacy in information knowingly shared with the public, CSLI warrants an exemption due to the unique privacy concerns implicated by its collection. *Carpenter*, 138 S.Ct. at 2219. This Court has acknowledged that certain types of data, such as CSLI, are simply incompatible with the Third-Party Doctrine. *Id*. at 2209. There are significant differences between the limited types of numerical information collected from the defendants in *Smith* and *Miller* and the meticulous historical record of personal location information collected by cellphone service providers. *Id*. at 2210. Cellphone location information is not gathered or shared in the way a person normally applies the terms in the Third-Party Doctrine analysis. *Id*. at 2220. Similar to GPS tracking of a car, cellphone location information provides law enforcement with a "detailed, encyclopedic, and

effortlessly complied" window into the private life of an individual. *Carpenter*, 138 S.Ct. at 2216-18. However, it is not the origin of the device recording the information that is most troubling, but the extent and depth of the information gathered. *Data Mining, Dog Sniffs, And The Fourth Amendment*, 128 HARVARD L. REV. 691, 700 (2014). In this digital age, this Court has questioned the viability of the Third-Party Doctrine because people reveal a substantial amount of personal information to third parties while completing everyday tasks. *Carpenter*, 138 S.Ct. at 2216 (citing to *City of Ontario, Cal. v. Quon*, 560 U.S. 746 (2010)).

Unlike *Miller* and *Smith*, here, the Third-Party Doctrine does not apply because Ms. Austin did not voluntarily convey her CSLI to YOUBER. The only time a user is notified of the YOUBER data collection policy is when the user creates the account. R. at 24. Ms. Lloyd created the account and gave Ms. Austin permission to use it. R. at 19-20. Nothing prohibited Ms. Austin from using Ms. Lloyd's account because Ms. Lloyd gave her the login information. R. at 19 and 24. When Ms. Lloyd granted permission for Ms. Austin to access her YOUBER account, Ms. Austin was never notified that YOUBER collects data information. R. at 24. While YOUBER is a business, and in *Carpenter* this Court elected not to address business records that may incidentally reveal a customer's location information, the Third-Party Doctrine looks to the voluntary conduct of sharing information. *Carpenter*, 138 S.Ct. at 2220. Ms. Austin never had the opportunity to learn about YOUBER's data collection policy and was unaware her private location information was being collected by the app, let alone would be shared with the government. Based on this Court's analysis that CSLI is not "shared" in the usual way and Ms. Austin's lack of voluntarily conveying this information, the Third-Party Doctrine does not apply. As in *Carpenter*, Ms. Austin's CSLI warrants an exemption because the exhaustive 92-day record collected by YOUBER detailed her intimate physical movements and was extremely comprehensive. Due to the duration and depth

of personal data in Ms. Austin's CSLI records, a reasonable expectation of privacy exists that is not subject to the warrantless disclosure of the Third-Party Doctrine.

C. The Warrantless Search of Ms. Austin's CSLI is Not Admissible Because Law Enforcement Abused Sophisticated Surveillance Techniques to Violate her Reasonable Expectation of Privacy.

Rooted in the Fourth Amendment is the protection against infringement of privacy by overreaching police surveillance. *Di Re*, 332 U.S. at 595. Since the government has access to subtle and far-reaching methods to invade individuals' privacy, a balance must be struck between the fruits of a search and unreasonable invasions of privacy. *T.L.O.*, 469 U.S. at 337; *see also Olmstead v. United States*, 277 U.S. 438, 473 (1928). Almost a century ago, this Court knew that the "progress of science" would provide the government with means of espionage beyond their current devices and insisted that these technological advancements not erode Fourth Amendment protections. *Olmstead*, 277 U.S. at 474.

"There are 396 million cellphone service accounts in the United States—for a Nation of 326 million people." *Carpenter*, 138 S.Ct. at 2211. Cellphone tracking is remarkably simple. *Id*. at 2217-18. It is cheap, efficient, and comprehensive. *Id*. With just a click of a button, the government can obtain a person's complete record of historical location information at almost no cost. *Id*. In *Carpenter*, this Court likened the government's tracking of a cellphone location to attaching an ankle monitor to the cellphone holder due to the information's near perfect surveillance of the individual. *Id*. at 2218. There are deep privacy concerns regarding the unique nature of CSLI in the hands of law enforcement. *Id*. CSLI gives police retroactive access to information that would otherwise be unknowable, even before the police are interested in such information. *Id*. These advancements mean that "the [g]overnment can now travel back in time to retrace a person's whereabouts, subject only to the retention policies of wireless carriers." *Id*.

This infringement of privacy not only presents risks to those under investigation, but to every single cellphone holder. *Carpenter*, 138 S.Ct. at 2218. Unlike previous police investigation tools such as a GPS device attached to a car, CSLI records do not require police to know in advance whether they want to follow a person, or even when. *Id*. The collecting of otherwise hard-to-obtain data changes the privacy interests that are implicated by disclosure because the data is not made available to the public. *U.S. Dep't of Justice v. Reporters Comm. For Freedom of the Press*, 489 U.S. 749, 764 (1989). There is a significant difference between the information uncovered from a diligent search of public files and the one-click access to a comprehensive digital record of a person's every movement. *Id*. As such, a subpoena is never a sufficient means of obtaining records from a third party that the suspect reasonably expects to be private. *Carpenter*, 138 S.Ct. at 2221. Thus, infringing upon these legitimate privacy rights requires a warrant. *Id*. at 2222.

Due to the overwhelming popular use of cellphones in the U.S. and the extremely intimate information these devices hold, there is a desperate need to protect everyone's justifiably reasonable expectation of privacy. A cellphone is essentially an extension of the body because every user has a compulsive tendency to carry their device wherever they go without hesitation. *Id*. at 2218. A cellphone "faithfully follows its owner" everywhere, providing an intimate window into the owner's personal life and private associations. *Id*. Under the Fourth Amendment, individuals should not fear that their every movement is trackable by the government. As such, there is a societal understanding that a justifiably reasonable expectation to privacy exists in the information obtained from a cellphone. Allowing law enforcement to circumvent this privacy interest by subpoenaing smartphone apps and cell service providers leaves individuals severely unprotected from government abuse. Detective Hamm violated Ms. Austin's Fourth Amendment rights when he failed to secure a warrant and neglected Ms. Austin's legitimate privacy interest in

her CSLI. This Court requires a warrant to obtain this highly sensitive information from third parties, making Detective Hamm's subpoena insufficient and unconstitutional. As technology advances, the law should not remain stagnant. In alliance with *Carpenter*, this Court should continue to recognize Fourth Amendment protections against new sophisticated systems that threaten the privacy of individuals everywhere.

CONCLUSION

This Court should REVERSE the Thirteenth Circuit's ruling that an unauthorized driver who has implied permission to drive a rental car does not have standing to contest a warrantless search of that car. Under the Fourth Amendment, an unauthorized driver has standing once he or she has demonstrated a legitimate property interest and reasonable expectation of privacy in the place searched. This Court should also REVERSE the Thirteenth Circuit's ruling that the Fourth Amendment permits warrantless searches of CSLI gathered by a third party. Such a holding undermines the safeguards implemented by *Carpenter* and ignores Ms. Austin's reasonable expectation of privacy.

Dated: October 6, 2019

Respectfully Submitted,

Team P17

Counsel for Petitioner.