R9

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 RESPONDENT

Counsel for Respondent

Oral Argument Requested

TABLE OF CONTENTS

TABLE OF AUTHORITIES

United States Supreme Court Cases:

United States Circuit Court Cases:

State Court Cases:

Constitutional and Statutory Provisions:

Other Authorities:

ISSUES PRESENTED

I. Whether an individual has standing to contest the search of a rental vehicle where she has neither authorization to rent the vehicle from the account owner.

II. Whether the acquisition of minimal location data of a rental vehicle constitutes a "search" within the meaning of the Fourth Amendment where the data was voluntarily conveyed to a third party, only tracked vehicular movements, and was limited in scope.

STATEMENT OF THE FACTS

A. Factual Background

Between October 2018 and January 2019, Petitioner Jayne Austin used her former partner's YOUBER account, without authorization, to rent cars which enabled her to rob six banks. R. at 10. Petitioner has a long-standing hatred for the banking industry, which she displayed through various blog and online poetry posts by calling for rebellion against a particular bank--Darcy and Bingley Credit Union--and advocating for its downfall. R. at 1. To further demonstrate her animosity, Petitioner robbed numerous branches of the bank. R. at 10.

Her actions came to light on January 3, 2019. R. at 2. On that day, Petitioner used Martha Lloyd's, Petitioner's "on-and-off again partner," YOUBER account to rent a Toyota Prius with the license plate number R0LL3M. R. at 2. Lloyd was not aware Petitioner was still using her account because she had switched to YOUBER's competitor, Bift. R. at 20. Lloyd also assumed Petitioner had ceased to use her account when she had asked Petitioner to give her space. R. at 20.

YOUBER is "a relatively new car rental software application ('app')" that can be downloaded onto cell phones. R. at 2. The app allows its 40 million users to find YOUBER rental cars and use them for up to 500 miles or one week. R. at 2, 23. Only YOUBER users are authorized to rent YOUBER-owned vehicles. R. at 2. YOUBER users can access the vehicles once their phone is detected inside a vehicle and the phone and vehicle connect via Bluetooth and GPS, which "ensure[s] that no one other than the registered renter operates" the vehicles. R. at 2-4. While signing up for the account, a pop-up message appears during the sign-up process warning the users "that YOUBER will track their information, and [users] must click a box to accept those terms." R. at 23. After the user accepts, YOUBER allows them to rent vehicles and, once they are renting the vehicle, begins tracking the vehicle's location through the user's account for security and

business purposes. R. at 4. YOUBER constantly tracks the vehicles, even when they are not being used, and filters the data through the search engine, SMOOGLE. R. at 4.

On January 3, 2019, Officer Charles Kreuzberger pulled Petitioner over for "failure to stop at a stop sign." R. at 2. Petitioner showed Officer Kreuzberger her license and the YOUBER app on her cell phone. R. at 2. Officer Kreuzberger realized Petitioner was not the authorized user of the YOUBER app and proceeded to search her car. R. at 3. Among some personal items, he found: "a BB gun modeled after a .45 caliber handgun with the orange tip removed, a maroon ski mask, and a duffel bag containing $50,000 and blue dye packs." R. at 3. At that time, the officer "received a dispatch to look out for a 2017 Black Toyota Prius with a YOUBER logo" because its driver robbed a local Darcy and Bingley Credit Union bank. R. at 3. The dispatch further noted that the surveillance had revealed a partial license plate of "R0L." R. at 3. The suspect was also "seen wearing a maroon ski mask and using a .45 caliber handgun." R. at 3. Based on the dispatch, the vehicle, the license plate, and the search, Officer Kreuzberger proceeded to arrest Petitioner "under suspicion for bank robbery." R. at 3.

On January 5, 2019, Detective Boober Hamm began to investigate Petitioner's case. R. at 3. While investigating, Hamm discovered five other open bank robbery cases, "occurring between October 15, 2018 and December 15, 2018 which matched the modus operandi of the robbery on January 3, 2019." R. at 3. Hamm "served a subpoena duces tecum (SDT) on YOUBER to obtain all GPS and Bluetooth information related to the account [Petitioner] allegedly used between October 3, 2018 through January 3, 2019." R. at 3. YOUBER complied, and its records allowed Hamm to deduce that Petitioner used rental cars "in the locations and at the times of each of the other five robberies." R. at 4. After reviewing the data and additional corroborative information--specifically, surveillance footage linking the rented YOUBER vehicles to the robberies--Hamm

recommended to the United States Attorney's Office that Petitioner be charged with "six counts of bank robbery under 18 U.S. Code § 2113, Bank Robbery and Incidental Crimes." R. at 4.

B. Procedural Background

Prior to trial, Petitioner filed two motions to suppress evidence. R. at 4. The first motion was to suppress the evidence obtained during Officer Kreuzberg's search of the rental car on January 3, 2019. R. at 4. The second motion was to suppress the location data YOUBER provided Detective Hamm. R. at 4. Both motions claimed that the searches were warrantless searches under the Fourth Amendment. R. at 4. The court denied both motions, holding that: (1) the Petitioner lacked Fourth Amendment standing to contest the search and (2) the data acquisition was not a search within the meaning of the Fourth Amendment. R. at 4. Petitioner was subsequently convicted of all six counts of bank robbery. R. at 10. Petitioner appealed the denial of the motions to the United States Court of Appeals for the Thirteenth Circuit. R. at 9-10.

The Thirteenth Circuit affirmed the ruling of the trial court, holding that Petitioner lacked standing to contest the search of the rental vehicle and the data acquisition by Detective Hamm was constitutional. R. at 16. The court found that the Petitioner lacked standing because she had no reasonable expectation of privacy and did not have a property right to claim standing. R. at 12. The court further found that under the Third-Party Doctrine, Petitioner had willingly exposed her location data to third parties--YOUBER and SMOOGLE--and therefore she had no reasonable expectation of privacy. R. at 15.

This Court granted Petitioner's writ of certiorari and directed the parties to address two issues. The first issue is: "Does an individual have standing to contest a search of a rental vehicle that the individual rented on another's account without that other person's permission?" The

second issue is: "Is the acquisition of the location data of a rental vehicle a 'search' within the meaning of the Fourth Amendment and *Carpenter v. United States*, 138 S. Ct. 2206 (2018)?"

SUMMARY OF THE ARGUMENT

Privacy is a paradox when property is illegitimately used, and information is unabashedly shared. The Fourth Amendment simply does not protect Petitioner's illegitimate use of an app, nor the data it collected because she voluntarily agreed to share the movements of the app's vehicles. Therefore, this Court should affirm the decision of the Thirteenth Circuit.

First, Petitioner does not have standing to contest the search of the vehicle. To contest a search, the Fourth Amendment and this Court's jurisprudence require that Petitioner show that she either had a reasonable expectation of privacy in the vehicle or had a property interest in it. Petitioner cannot assert a privacy interest in the vehicle because she did not have authorization to rent the vehicle on Martha Lloyd's YOUBER account. Second, because it was not her account, Petitioner also cannot assert a property interest. Finally, Fourth Amendment policy also cautions against expanding Fourth Amendment standing to protect people who are unlawfully present in another person's vehicle.

Second, the acquisition of the YOUBER data was not a search within the meaning of the Fourth Amendment. The holding of *Carpenter v. United States*, 138 S. Ct. 2206 (2018) is narrow and distinguishable from the present case. The Third-Party Doctrine is applicable because YOUBER requires its users to give affirmative and voluntary consent before it begins recording the movement data and Petitioner shared the application with Martha Lloyd. Additionally, the expectation of privacy is diminished because the movements took place in public spaces and inside vehicles. Finally, the reach and use of the YOUBER app is far more limited and narrower than cell phones. For these reasons, the collection of the YOUBER data is not a search within the meaning

of the Fourth Amendment. Accordingly, the judgment of the Thirteenth Circuit Court of Appeals should be affirmed on both grounds.

STANDARD OF REVIEW

The standard of review on writ of certiorari for a Fourth Amendment search and standing question is de novo. *United States v. Williams*, 521 F.3d 902, 906 (8th Cir. 2008); *United States v. Shryock*, 342 F.3d 948, 977 (9th Cir. 2003).

ARGUMENT

I. PETITIONER LACKS STANDING TO CONTEST THE SEARCH OF A VEHICLE SHE WAS UNAUTHORIZED TO USE BECAUSE SHE HAD NEITHER A PRIVACY INTEREST NOR PROPERTY INTEREST IN THE VEHICLE

The decision of the Thirteenth Circuit should be affirmed because Petitioner did not have standing as she did not have a privacy or property interest in the car. Fourth Amendment standing is "shorthand for capturing the idea that a person must have a cognizable Fourth Amendment interest in the place searched before seeking relief for an unconstitutional search." *Byrd v. United States*, 138 S. Ct. 1518, 1530 (2018). A defendant asserting a Fourth Amendment violation must demonstrate "the disputed search and seizure has infringed an interest of the defendant which the Fourth Amendment was designed to protect." *Rakas v. Illinois*, 439 U.S. 128, 140 (1978). Fourth Amendment standing only permits "defendants whose Fourth Amendment rights have been violated to benefit from" the exclusionary rule. *Id.* at 134. The Court has traditionally recognized two forms of cognizable Fourth Amendment interests that create standing: (1) privacy interests and (2) property interests. *Rawling v. Kentucky*, 448 U.S. 98, 106 (1980); *United States v. Jones*, 565 U.S. 400, 405 (2012). These two interests tend to merge as "any legitimate expectation of privacy" held by a defendant. *Rawling*, 448 U.S. at 106.

In this case, Petitioner can assert neither interest in the rental vehicle. Thus, this Court should affirm the decision of the Thirteenth Circuit Court of Appeals for three reasons. First, Petitioner does not have standing to protest the search of the rental vehicle when she did not have a reasonable expectation of privacy in the vehicle because she did not lawfully possess the vehicle. Second, Petitioner does not have standing to protect the search of the rental vehicle when she did not have a property interest in the rental vehicle because she rented it without the account user's permission and knowledge. Third, the policy of Fourth Amendment standing was created to allow petitioners to protest their own Fourth Amendment rights, not the rights of others.

A. Petitioner Does Not Have Fourth Amendment Standing Because She Did Not Have a Reasonable Expectation of Privacy in a Vehicle That She Was Unauthorized to Rent from Another Person's Account

Petitioner does not have Fourth Amendment standing to contest the search of the rental vehicle because she did not have a reasonable expectation of privacy in the vehicle that she was unauthorized to rent. A defendant has a reasonable expectation of privacy under the Fourth Amendment if (1) "the person [has] exhibited an actual expectation of privacy," and (2) "the expectation [is] one that society is prepared to recognize as 'reasonable.'" *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); Thomas K. Clancy, The Fourth Amendment: Its History and Interpretation 60 (2008) (arguing that Harlan's reasonable expectation of privacy test is the "predominant measure for the scope of the Fourth Amendment's protections").

While this Court has applied Harlan's test on a case by case basis, this Court has consistently found that subjective and objective expectations of privacy are largely based on "lawful possession and control" of the property. *Byrd*, 138 S. Ct. at 1528; *Rawling*, 448 U.S. at 105; *Jones v. United States*, 362 U.S. 257, 259 (1960), *overruled by United States v. Salvucci*, 448 U.S. 83, 85 (1980) (rejecting automatic standing); *Rakas*, 439 U.S. at 134; Thomas K. Clancy, The

Fourth Amendment: Its History and Interpretation 65 (2008) (arguing that the Court uses a "chameleon-like and case-specific approach" in its reasonable expectation of privacy determinations). In *Rawling*, this Court held that the defendant did not have a reasonable expectation of privacy in the contents of his friend's purse, where he had hastily stowed illegal controlled substances before a police search. *Rawling*, 448 U.S. at 105. This Court found the defendant did not have the right to exclude others from the purse because he did not "take normal precautions to maintain his privacy," and he did not have any "real subjective expectation that the [purse] would remain free of government intrusion." *Id.* at 104-05.

In rental car cases, this Court has only found a reasonable expectation of privacy when the defendant has lawful possession of the car because of the "diminished expectation of privacy in automobiles." *Byrd*, 138 S. Ct. at 1526-28. In *Byrd*, this Court found that possession itself, which renders the right to exclude, is not enough to create a reasonable expectation of privacy. *Id.* This is because while a carjacker could exclude others from the car, a "car thief would not have a reasonable expectation of privacy in a stolen car." *Id.* at 1529. In fact, the Seventh Circuit Court of Appeals has held that Fourth Amendment standing to contest the search of a car or rental car is based on the "permission of the owner." *United States v. Walton*, 763 F.3d 655, 664 (7th Cir. 2014) (quoting *Johnson v. United States*, 604 F.3d 1016, 1020 (7th Cir. 2010)).

Further, a person who has disavowed ownership of a vehicle cannot turn around and assert a reasonable expectation of privacy. *United States v. Boruff*, 909 F.2d 111, 116 (5th Cir. 1990). Following *Katz*, the Fifth Circuit found that a defendant who had bought a truck but then "completely disassociated himself from the truck both legally and factually" could not assert a reasonable expectation of privacy in it. *Id.* (citing *Katz*, 389 U.S. at 361) Further, defendant could not assert a reasonable expectation of privacy in a rental car he drove, when he knew the terms of

the rental agreement did not permit him to drive the rental car, and he did not rent the car himself. *Id.* at 117.

In Petitioner's case, there is no reasonable expectation of privacy in the YOUBER rental car that would give her standing to exclude evidence obtained through the search of the rental vehicle since she did not lawfully possess the rental vehicle. YOUBER requires, contractually, for any user of its app and services to "agree to YOUBER's privacy policies." R. at 30. Petitioner does not have a YOUBER account but uses the account of "her on-and-off-partner, Martha Lloyd." R. at 2. Only Lloyd agreed to the terms of the account. R. at 2. Petitioner has not. R. at 2. Yet, Petitioner uses the account on her own personal cellphone. R. at 2. Petitioner, therefore, is an unauthorized user, according to YOUBER's policies. R. at 30. Further, Petitioner did not attain Lloyd's permission to use her YOUBER account on the day of the search. R. at 2, 19. In fact, Lloyd had written Petitioner a letter asking Petitioner to let Lloyd "distance herself from [Petitioner]." R. at 20. Like the defendant in *Walton*, since Petitioner did not have permission to use the rental car or the rental car app, Petitioner cannot have Fourth Amendment standing to protest the search. *Walton*, 763 F.3d 655.

Additionally, like the defendant in *Rawling*, Petitioner does not have a reasonable expectation of privacy in a rental car she was unauthorized to use. In *Rawling*, the defendant had at least asked permission to stow the illegal narcotics in the friend's purse. *Rawling*, 448 U.S. at 105. Here, Lloyd did not even know Petitioner was still using her account at all. R. at 20. Petitioner, like the defendant in *Rawling*, also took no reasonable precaution to protect her privacy by openly using a rental vehicle that she failed to secure in her own name. R. at 3. Petitioner, consequently, could not have a reasonable expectation of privacy in the unauthorized use of the rental car.

Lastly, Petitioner could not have a reasonable expectation of privacy when she disavowed all property interests and proactively attempted to "stay off the grid." R. at 26, 18. In her blog poems, Petitioner explicitly stated that "I claim no property" and that "Ownership is nothing." R. at 26-27. She also actively attempted to remain undetected by using Lloyd's information to prevent her name from being on any account. R. at 18. This included the YOUBER app. R. at 18. Like the defendant in *Boruf*, when a defendant takes active steps to dissociate himself from a property and ownership interest to avoid detection, he cannot later claim to have a privacy interest in the property to gain Fourth Amendment standing and exclusion remedies. *Boruff*, 909 F.2d at 116. The same concept applies to Petitioner and prevents her from contesting a search.

Consequently, Petitioner did not have a reasonable expectation of privacy that would give her standing to exclude the search of the unauthorized car rental.

B. Petitioner Did Not Have a Legitimate Property Interest Protected by the Fourth Amendment Because She Was Unlawfully Present in the Car

Petitioner did not have a legitimate property interest protected by the Fourth Amendment because she was unlawfully present in the rental car. The Fourth Amendment protects "persons, houses, papers, and effects." U.S. Const. amend. IV; *Olmstead v. United States*, 277 U.S. 438 (1928) (holding that a wiretap was not a search and seizure under the Fourth Amendment because the government did not physically intrude on the defendant's home to obtain the recorded evidence). To assert a Fourth Amendment claim, nonetheless, "the legitimation of expectation of privacy by law must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property or to understandings that are cognized and permitted by society." *Byrd*, 138 S. Ct. at 1527. A reference to real property occurs when "the government physically occup[ies] physical property for the purpose of obtaining information." *Jones*, 565 U.S.

at 404. Vehicles are protected by the Fourth Amendment. *Id.* Therefore, when the government trespasses upon a vehicle, it may be considered a search under the Fourth Amendment. *Id.* at 406.

However, unless a Petitioner can demonstrate that a rental vehicle is capable of invasion through "physical intrusion" the court will not find a recognized property right protected by the Fourth Amendment. *Florida v. Jardines*, 569 U.S. 1, 5 (2013). The remnants of common law trespass as a method of obtaining Fourth Amendment standing had, until recently, been abrogated throughout the decades, but not overruled. *Rakas*, 439 U.S. at 142 (holding, *Jones*, 362 U.S. at 263, only stands "for the unremarkable proposition that a person can have a legally sufficient interest in a place other than his own home so that the Fourth Amendment protects him from unreasonable governmental intrusion in that place"). In 2012, however, this Court revitalized the common-law trespass method of determining standing. *Jones*, 565 U.S. at 405. To meet the common law trespass requirement, this Court has acknowledged that "one who owns or lawfully possess, or controls property will in all likelihood have a legitimate expectation of privacy by virtue of [the] right to exclude." *Byrd*, 138 S. Ct. at 1527. In *Byrd*, this Court held that person who "lawfully possessed and control[ed]" a rental car, despite the rental agreement prohibiting use by any other than the renter themselves, could have Fourth Amendment standing. *Id.* at 1528. In contrast, "one wrongfully on the premises could not move to suppress evidence obtained as a result" of a search. *Rakas*, 439 U.S. at 141. "A person present in a stolen automobile at the time of the search may [not] object to the lawfulness of the search of the automobile." *Id.* at 141 & n. 9.

Notably, property used for "commercial purposes is treated differently for Fourth Amendment purposes." *Minnesota v. Carter*, 525 U.S. 83, 90 (1998). In *Carter*, this Court held that the defendants did not have Fourth Amendment standing to challenge the search of an apartment after a police officer saw the defendants bagging cocaine through window blinds. *Id*. at

85. This Court found that even though the defendants were in a home when they were bagging cocaine, the "home" was not functioning as such at the time. *Id.* at 91. Further, the "purely commercial nature of the transaction engaged in" and "the relatively short period of time on the premises" prevented the creation of a Fourth Amendment protected property interest. *Id.*

In Petitioner's case, she was not legitimately present in the rental car and the commercial nature of the YOUBER app diminished her property interest and, consequently, her Fourth Amendment rights in the property. Petitioner did not have a legitimate property interest in the YOUBER rental car. She was not registered to use the YOUBER app, which would have allowed her to rent cars from YOUBER. R. at 18. She did not have authorization from YOUBER to rent a car on the day of the stop, per its terms and conditions. R. at 19. The app registeree did not give Petitioner authorization to use a car rented from the app. R. at 19. Unlike *Byrd*, Petitioner was not authorized and lawfully in control of the car when the stop by the police officer occurred because the account user had cut off contact with Petitioner. R. at 20. Petitioner did not ask to use the YOUBER account on the day of the search and did not receive permission to use the account. R. at 20. Therefore, Petitioner's presence in the car did not cause a Fourth Amendment right to arise and Petitioner does not have standing to exclude the search of the rental vehicle.

Additionally, the transactional nature of the use of the YOUBER app lowers Petitioner's expectation of privacy and legitimate presence on the property even further. YOUBER is a modern car rental agency that allows car rentals at hourly rates. R. at 2. A YOUBER car rental period can extend up to a week or 500 miles. R. at 2. Like in *Carter*, Petitioner lacked a property interest that created a privacy interest in the car protected by the Fourth Amendment because the YOUBER car rentals are for extremely short periods of time and the nature of the relationship between the parties was purely transactional.

Consequently, Petitioner lacked any legitimate property interest in the YOUBER rental due to her lack of lawful possession and control over the rental car.

C. Fourth Amendment Standing Policy Protects Individuals, Not Others, and Does Not Protect an Illegitimate and Unlawful Presence in a Vehicle

In determining Fourth Amendment standing and the exclusionary rule, Justice White asserted that suppression "can be successfully urged only by those whose rights were violated by the search itself, not by those who are aggrieved solely by the introduction of damaging evidence." *Alderman v. United States*, 394 U.S. 165, 171-72 (1969) (citing U.S. Const. amend IV). In this case, Petitioner seeks to suppress evidence that is damaging to her, but where she does not have Fourth Amendment rights to protect. This Court should continue to preclude such assertion of rights. In *Rakas*, this Court acknowledged its disdain for criminals asserting privacy rights in property not legitimately in their possession. *Rakas*, 439 U.S. at 143 n. 12. This Court compared one defendant to a "car thief" when he "intentionally used a third party to precure a rental car by a fraudulent scheme for the purpose of committing a crime." *Byrd*, 138 S. Ct. at 1531.

Further, to give standing to a defendant who used and rented property without the authorization of the owner goes against the policies of suppression. The exclusionary rule was designed to preserve judicial integrity and to deter police misconduct. *Mapp v. Ohio*, 367 U.S. 643, 656, 660 (1961); *Weeks v. United States*, 232 U.S. 383 (1914). Judicial integrity is not served by allowing a defendant to use rental services to escape criminal detection and police misconduct is not deterred by preventing police officers from searching a rental vehicle where there is no trace of the user lawfully renting it. In fact, unauthorized use of a rental vehicle, where the driver's name is not connected to the rental at all, has the potential to put public safety at risk. Amy Winter, *Identity Theft and Car Rental*, Auto Rental News (Sept. 11, 2013), https://www.autorentalnews.com/153089/identity-theft-and-car-rental. If police cannot ascertain the lawful driver of the rental

vehicle, car thieves and agents of fraud will be able to steal rental vehicles and use rental vehicles for crime with impunity.

In Petitioner's case, no policy of standing or the exclusionary rule would be advanced by allowing Petitioner to protest the search of her rental vehicle. Privacy is a paradox when property is illegitimately used. Petitioner used the rental app to avoid detection to commit crime. R. at 4. She purposefully used the app of Lloyd to keep herself "off the grid." R. at 18. In this case, Petitioner is no better than a car thief.

Further, judicial integrity would be harmed by granting Petitioner's standing argument. This Court has been vigilant in preventing Fourth Amendment standing from "serv[ing] only to afford a windfall to defendants whose Fourth Amendment rights have not been violated." *Salvucci*, 448 U.S. at 95. Petitioner is simply attempting to dupe the judicial system by acting as an innocent party when in fact she took every effort to prevent detection and traceable property interests to conduct her crimes. R. at 2, 18.

Police misconduct is not an issue when a police officer can determine whether a party is the rightful user of a car rental through an app--especially in apps, like YOUBER, that only permit its contractually bound users to rent cars. R. at 29. The only reason the police were able to impede Petitioner from her elusive bank robbery spree was because officers realized she was an unauthorized user of the YOUBER app. R. at 3. The police realized that Petitioner was no better than a car thief. Therefore, the police officers acted within the bounds of the Fourth Amendment and public safety was protected.

Conclusively, to protect the integrity of the Fourth Amendment standing doctrine, Petitioner should be denied standing.

II. THE ACQUISITION OF DATA FROM A THIRD-PARTY IS NOT A FOURTH AMENDMENT SEARCH WHEN THE DATA IS CONVEYED VOLUNTARILY AND IS LIMITED TO VEHICULAR MOVEMENTS

The decision of the lower court should also be affirmed for a second reason: this Court's Fourth Amendment precedent, including *Carpenter v. United States*, 138 S. Ct. 2206 (2018), allows for the acquisition of data conveyed to a third party or to the public, where the data does not reveal intimate details about a person. As discussed previously, the Fourth Amendment guarantees: "[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. To challenge a search, defendants traditionally needed to show that there was a physical trespass of their property by a government agent. *Olmstead v. United States*, 277 U.S. 438, 463-64 (1928). However, this Court recognized that a search may also implicate privacy interests without a physical intrusion. *Katz v. United States*, 389 U.S. 347, 351 (1967).

The expectation of privacy in the digital age was scrutinized last year by this Court, when it considered whether location data collected by a cell phone company and then revealed to law enforcement agents was a search within the meaning of the Fourth Amendment. *Carpenter*, 138 S. Ct. at 2217. This Court analyzed several factors before holding that a search did occur when officers requested a log of the defendant's cell phone location data from a cell phone company. *Id.* These factors included: (1) the extent to which the conveyance of the data to the cell phone company was voluntary; (2) the relative public or private nature of the movements, in light of other movement tracking cases; and (3) the pervasive and essential role that cell phones have in modern society. *Id.* at 2215-18. In its holding, this Court cautioned that "the decision is narrow." *Id.* at 2210. Chief Justice Roberts specifically acknowledged its limitations by stating that the Court "do[es] not begin to claim all the answers today," in light of "the manifold situations that may be

presented by this new technology." *Id.* at 2220 n. 4. This Court's own emphasis on the limitation of its decision in *Carpenter* is instructive.

Considering this Court's warning, the decision of the Thirteenth Circuit should be affirmed for three reasons. First, Petitioner voluntarily revealed the data to several third parties, including YOUBER and Lloyd; therefore, she assumed the risk of the data being revealed. Second, because Petitioner's data only reflected her public, vehicular movements, she already had a diminished expectation of privacy. Third, as a matter of policy, this Court's analysis of the "depth, breadth, and comprehensive reach" of CSLI and cell phones does not ubiquitously apply to all apps. *Id.* at 2220.

A. Petitioner Has No Reasonable Expectation of Privacy in Information She Shared Voluntarily with YOUBER and Martha Lloyd

Petitioner's Fourth Amendment rights were not violated because she voluntarily revealed the data to several third parties. A search occurs when "the government violates a subjective expectation of privacy that society recognizes as reasonable." *Kyllo v. United States*, 533 U.S. 27, 33 (2001). The subjective expectation of privacy standard involves determining whether a person has "exhibited an actual… expectation of privacy," such as when a person limits the information exposed to outsiders. *Katz*, 389 U.S. at 361 (Harlan, J., concurring) (illustrating that closing a door to a phone booth is an expression of a subjective expectation of privacy because it essentially transforms a public space into a private one). The objective prong of the standard is not satisfied unless society is prepared to recognize an expectation of privacy as reasonable or legitimate. *Id.*

A person's expectation of privacy may be diminished when a person voluntarily and knowingly reveals information to another; this is otherwise referred to as the Third-Party Doctrine. *United States v. Miller*, 425 U.S. 435, 442 (1976). This is because "[he] takes the risk… that the information will be conveyed by that person to the Government." *Id.* After all, the Constitution,

protects "privacy, and once privacy has been shared, the shared information, documents, or places remain private only at the discretion of the confidant." *Georgia v. Randolph*, 547 U.S. 103, 131 (2006). Even information shared with a trusted friend necessarily implicates the Third-Party Doctrine. *Id.* For example, "[i]f two roommates share a computer and one keeps pirated software on a shared drive, he might assume that his roommate will not inform the government. But that person has given up his privacy with respect to his roommate by saving the software on their shared computer." *Id.*

This concept has often pertained to situations where a customer voluntarily shares information with a business, knowing that it intends to store the information in its records. *Miller*, 425 U.S. at 444. For example, this Court has held that a defendant does not have a legitimate expectation of privacy in his bank records. *Id.* The records only contained information that was "voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business." *Id.* The defendant, therefore, could "assert neither ownership nor possession" of the records because they were "business records of the banks." *Id*. at 440.

Three years later, this Court applied the same standard to a record of dialed numbers by a telephone company—even though the phone records were collected by automatic switching equipment and not employees. *Smith v. Maryland*, 442 U.S. 735, 745 (1979). "Telephone users... typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes." *Id.* at 743. Therefore, any subjective expectation of privacy is not objectively reasonable by societal standards. *Id.* Consequently, a government's subsequent acquisition of those business records is not a Fourth Amendment search. *Id.* at 746.

Last year, this Court reexamined the Third-Party Doctrine's workability in the digital age. *Carpenter,* 138 S. Ct. at 2219. While investigating a series of bank robberies, investigators subpoenaed two cell phone companies for the defendant's cell-site location information (CSLI). *Id.* at 2212. CSLI reveals a time-stamped record of a person's location based on the cell phone's connection to a radio antenna, called a cell-site. *Id.* at 2211. After requesting the defendant's CSLI, the investigators received a record of his movements over the course of 127 days, which the State introduced as evidence in trial. *Id.* This Court held that the acquisition was a search under the Fourth Amendment because a cell phone owner does not "voluntarily 'assume the risk' of turning over a comprehensive dossier of his physical movements." *Id.* People cannot opt out of sharing CSLI with the companies because the collection is "inescapable and automatic." *Id.* at 2223. In fact, "a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up." *Id.* at 2210. The connection to the cell-site occurs even if the user[1] is not actively using one of the features of the phone. *Id.* at 2212. This Court, however, limited the scope of this analysis to CSLI and left the Third-Party Doctrine untouched in cases involving voluntarily conveyed information. *Id.* at 2220.

In the Petitioner's case, the information was voluntarily conveyed to several third parties, which distinguishes its collection from that in *Carpenter*. Before making an account, users must agree to share their location data with YOUBER. R. at 4. Upon signing-up, "[a] message pops up that says that YOUBER will track [the user's location] information." R. at 23. Users must then affirmatively assent to the data collection before they can create an account. R. at 23. YOUBER's

[1] Lower courts have even suggested that it is "unlikely that cell phone customers are aware that their cell phone providers collect and store historical location information." *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304, 317 (3d Cir. 2010).

privacy policy also warns users of the fact that another third party, SMOOGLE, has access to the data for satellite mapping purposes. R. at 29. Because of the active sign-up process, all account holders are aware of the collection. Applying the rationale used in *Smith*, all users know that their location information is being conveyed to the company and that the company intends to keep a record of it because of the pop-up message. Since all users are aware of the collection, there is no reasonable expectation of privacy in the data and Petitioner's desire to keep her locational data private is unreasonable.

The collection is also not "inescapable;" if a user does not want to share the locational data, the user may opt out of using the app or delete it entirely. *Carpenter,* 138 S. Ct. at 2223. Like the records in *Miller* and *Smith*, the YOUBER data is stored in the ordinary course of business for security and maintenance purposes. R. at 2, 4. This is exemplified by YOUBER's continuous monitoring of their vehicles, even when no one is renting them. R. at 4. YOUBER cannot monitor its property effectively if it does not keep a record of the vehicle's location. Additionally, YOUBER and similar service-providing apps rely on users voluntarily conveying locational data so that the companies can monitor where its customers are requesting the service and allocate their resources accordingly. *See* R. at 4; *Ride*, Uber (last visited Oct. 1, 2019), https://www.uber.com/ride. Therefore, like the records in *Smith*, the government's subsequent acquisition of the YOUBER records is not a Fourth Amendment search. *Smith*, 442 U.S. at 746.

Petitioner's use of Martha Lloyd's account also indicates that she had no subjective expectation of privacy. Lloyd—to whom the YOUBER account is registered—could have realized that Petitioner was still using her account, if she had checked YOUBER. R. at 21. Like the shared computer described in *Randolph*, once Petitioner and Lloyd agreed to share the app, the expectation of privacy as to the contents and data contained within the app became "frustrated."

Randolph, 547 U.S. at 131. Further undercutting any claim of an expectation of privacy is that Petitioner did not take "normal precautions to maintain [her] privacy." *Rawling v. Kentucky*, 448 U.S. 98, 105 (1980). Most smartphones have a location privacy setting that can be enabled to prevent all apps—such as YOUBER—from accessing the phone's location. *See iPhone User Guide: Location Services*, Apple (2017), https://help.apple.com/iphone/10/#/iph3dd5f9be. Users that want to be "off the grid" may simply turn off their location sharing. R. at 18. This makes the location tracking 'escapable' because users can limit the data shared with services without limiting the functionality of their entire phone. Here, there is no indication that Petitioner ever attempted to turn off her location sharing.

Because of these factors, Petitioner exhibited neither a subjective nor an objective expectation of privacy. Privacy is a paradox when information is unabashedly shared with another. Thus, the government's acquisition of the YOUBER records is not a Fourth Amendment Search.

B. YOUBER's Data Reflects Petitioner's Public and Vehicular Movements, and Therefore Petitioner Has a Diminished Expectation of Privacy

Petitioner has a diminished expectation of privacy because the YOUBER app only recorded movements which were no longer private because she drove on public roads. The goal of the Fourth Amendment is to protect the "privacies of life" from arbitrary government intrusion. *Boyd v. United States*, 116 U.S. 616, 630 (1886); *Kyllo*, 533 U.S. at 37 (holding the use of thermal imaging to monitor a home is a search because it may reveal "intimate details" about the people inside). A person's home is the place where an individual has the most privacy. *United States v. United States District Court*, 407 U.S. 297, 313 (1972) (noting "physical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed"). The curtilage, or area surrounding the home, is protected because of similar, heightened privacy concerns. *Collins v. Virginia*, 138 S. Ct. 1663, 1670 (2018); *California v. Ciraolo*, 476 U.S. 207, 212-13 (1986).

In contrast, this Court has held time and again that observation of outdoor activities does not constitute a search within the meaning of the Fourth Amendment. *Hester v. United States*, 265 U.S. 57 (1924) (observing a person in an open field is not a search); *Oliver v. United States*, 466 U.S. 170, 178 (1984) (emphasizing, "an individual may not legitimately demand privacy for activities conducted out of doors in fields, except in the area immediately surrounding the home."). The logic behind the distinction is that "the police cannot reasonably be expected to avert their eyes from evidence of criminal activity that could have been observed by any member of the public." *California v. Greenwood*, 486 U.S. 35, 41 (1988).

In search cases, the line between private and public spaces is determinative. For example, in *United States v. Knotts*, 460 U.S. 276, 277 (1983) officers accessed a vehicle's movements via a beeper, a type of radio transmitter. The beeper was first placed within a container of chloroform and then into the defendant's vehicle by law enforcement agents. *Id.* When it reviewed the constitutionality of the tracking, this Court explained, "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another" because the movements were already voluntarily revealed to the public. *Id.* at 281. Therefore, it held that the use of a beeper was permissible. *Id.* Just one year later, however, this Court held that the validity of a beeper search was unconstitutional, particularly because the beeper intruded upon private property. *United States v. Karo*, 468 U.S. 705 (1984) (noting that the beeper was moved inside of a home and storage unit).

When this Court revisited the topic of vehicle movements in *Jones*, it did not place a lot of emphasis on the reasonable expectation of privacy standard; instead it focused on the defendant's property interest in the vehicle. *United States v. Jones*, 565 U.S. 400, 412 (2012). In that case, officers monitored a defendant's location after attaching a GPS device to his vehicle. *Id.* at 402.

This was a search within the meaning of the Fourth Amendment because there was a physical invasion of the defendant's property by the government. *Id.* at 407. In its holding, this Court specifically declined to rule on the issue of whether officers may monitor the location of a vehicle when there is no physical trespass. *Id.* at 412.

Picking up where *Jones* left off, the holding of *Carpenter* weighed in on the issue of whether there is a reasonable expectation of privacy in one's movements. *Carpenter*, 138 S. Ct. at 2223. This Court acknowledged the questions left unanswered in *Jones*, by stating that CSLI has "even greater privacy concerns than the GPS monitoring of a vehicle." *Id.* at 2218. It stated:

> Unlike the bugged container in *Knotts* or the car in *Jones*, a cell phone—almost a feature of human anatomy—tracks nearly exactly the movements of its owner. While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time. A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales.

Id. (internal citations omitted). It even compared a cell phone to an ankle monitor because "nearly three-quarters of smart phone users report being within five feet of their phones most of the time." *Id.* (quoting *Riley v. California*, 573 U.S. 373, 395 (2014)). Vehicles have "little capacity for escaping public scrutiny" because their movements are limited to public roads. *Id.* (quoting *Cardwell v. Lewis*, 417 U.S. 583, 590 (1974)). CSLI, in stark contrast, is "absolute," "near perfect," "deeply revealing," and a "comprehensive" record of a person's location. *Id.* at 2218-23.

In Petitioner's case, the scope of the YOUBER data is much less intrusive and comprehensive than CSLI. R. at 29, 30. The physical trespass protections of the Fourth Amendment are unimplicated because the method used to acquire the data is significantly less intrusive than the GPS device in *Jones*. Here, there was no physical invasion of the vehicle, or Petitioner's phone, by the government.

Next, the inquiry shifts to the nature of the data that was collected. The fundamental difference between *Knotts* and *Karo* was where the monitoring took place. The monitoring was acceptable in *Knotts* because it was already accessible to the public; in *Karo*, it was unacceptable because it invaded private spaces. *Knotts*, 460 U.S. at 281; *Karo*, 468 U.S. at 715. YOUBER only collects location data from its customers when they are actually renting the vehicle and their phones are physically within it. R. at 3, 4, 22. This makes the data limited to public movements. Vehicles tend to stay on streets and in parking lots; cell phones go wherever their owners go. This means that cell phones can track an individual inside the curtilage of their private property; vehicles cannot, except in a garage or driveway. Cell phones are carried to places that reveal intimate facts about a person—like doctor's offices, religious buildings, or to political events and concerts. *Carpenter*, 138 S. Ct. at 2218. Vehicles usually stay in a parking lot and are not the only form of transportation. Because of this limitation, the company merely recorded movements that Petitioner already voluntarily conveyed to the public, such as: "the fact that [s]he was traveling over particular roads in a particular direction, the fact of whatever stops [s]he made, and the fact of [her] final destination when [s]he exited from public roads onto private property." *Knotts*, 460 U.S. at 282.

The nature of the information revealed in the YOUBER data is far from a "detailed log" of Petitioner's life. *Carpenter*, 138 S. Ct. at 2218. It is, at most, a snapshot of her life when she is in a rental vehicle, which already has "little capacity for escaping public scrutiny." *Cardwell*, 417 U.S. at 590. Because the YOUBER data is already conveyed to the public and there was no physical trespass of Petitioner's property, the acquisition of the data is not a Fourth Amendment search.

C. As a Matter of Policy, This Court's Analysis of the "Depth, Breadth, and Comprehensive Reach" of CSLI Does Not Ubiquitously Apply to All Apps

The holding of *Carpenter* is "narrow." *Carpenter*, 138 S. Ct. at 2210. It should not be categorically applied to all apps. To maintain a just balance between the expectation of privacy of individuals and the expanding technological capabilities of the digital age, this Court should continue to balance a variety of factors—like the voluntariness of the data exposure and the "depth, breadth, and comprehensive reach" of the data acquisition. *Id.* at 2220. In the present case, the depth and breadth of the YOUBER data is more limited and narrower than CSLI. Also, society's use of the YOUBER app is not so pervasive that is has a comprehensive reach.

When this Court reviewed the "depth" and "breadth" of a person's movements collected through CSLI, it referred to "the whole of a person's movements," or the level of thoroughness of the movement record. *Carpenter*, 138 S. Ct. at 2219. The data's "comprehensive reach" was measured by how many people were being tracked. *Id.* at 2218 (noting, "[o]nly the few without cell phones could escape this tireless and absolute surveillance"). CSLI offers "an intimate window into a person's life." *Id.* at 2220. A cell phone can track where a person is, "not only around town but also within a particular building." *Riley*, 573 U.S. at 396. CSLI does not just reveal a person's location at a specific time, but it creates a "chronicle of a person's physical presence compiled every day, every moment, over several years." *Carpenter*, 138 S. Ct. at 2220.

In Petitioner's case, the YOUBER data is drastically less revealing than CSLI due to its limited "depth" and "breadth." *Id.* at 2219. The YOUBER data reflects Petitioner's use of its vehicles over the course of three months. R. at 5. The data is recorded in increments of up to 500 miles or seven days, the maximum rental period. R. at 2. It is entirely likely that Petitioner did not rent the vehicles continuously for the entirety of the three-month period. Even if she did rent the vehicles constantly, the amount of YOUBER data would still be less than the amount of CSLI; a

recent study found that Americans are in their vehicles for less than an hour each day. B. C. Tefft, *American Driving Survey, 2015-2016*, AAA Foundation for Traffic Safety 2 (2018). Meanwhile, a person almost always has their phone with them and "a cell phone logs a cell-site record by dint of its operation" and during "virtually any activity on the phone." *Carpenter*, 138 S. Ct. at 2220. The usage disparity indicates that the data for CSLI is far more extensive than data of when a person is within a vehicle, and the latter is less likely to give officers "an intimate window into a person's life." *Id.* at 2217.

To analogize to the relationship between CSLI and the YOUBER data, accessing someone's entire phone provides a comprehensive account of who the person is because of the content on it. *Riley*, 573 U.S. at 396; *State v. Granville*, 423 S.W.3d 399, 415-17 (Tex. Crim. App. 2014) (emphasizing, "searching a person's cell phone is like searching his home desk, computer, bank vault, and medicine cabinet all at once"). Smaller subsets of data on a phone can be contained in apps, which reveal intimate details about a person, including their political affiliation, relationship status, religion, and hobbies. *Riley*, 573 U.S. at 396. "The average smart phone user has installed 33 apps, which *together* can form a revealing montage of the user's life." *Id.* (emphasis added). Individually, however, apps can only offer a small glimpse about a person. To reveal a "montage of a user's life," an app on someone's phone needs to be viewed in context with the other apps. *Id.* For instance, knowing that a person has the Starbucks app reveals fairly little about them; knowing that a person has an app for every coffee shop within a five-mile radius may reveal that a person is a coffee addict—or a student in law school.

Likewise, YOUBER's data on its own does not reveal "intimate" details of its users. *Carpenter*, 138 S. Ct. at 2217. Whereas CSLI, reveals a comprehensive log of a person's movements, YOUBER only records a minor subset of those movements. Therefore, the reach of

YOUBER's data is more limited than CSLI. Further, YOUBER's presence in society is incomparable to that of cell phones. "[M]odern cell phones... are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Riley*, 573 U.S. at 385. In fact, "[t]here are 396 million cell phone service accounts in the United States—for a Nation of 326 million people." *Carpenter*, 138 S. Ct. at 2211. Cell phones are "so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification." *City of Ontario v. Quon*, 560 U.S. 746, 760 (2010). In contrast, YOUBER is also a relatively new app. R. at 2. Out of all cell phone users in America, only about 10% have the YOUBER app installed on their phones. R. at 22. YOUBER's reach can hardly be considered "comprehensive" or analogous to a technology akin to "an important feature of human anatomy." *Riley*, 573 U.S. at 385. Thus, this Court's balancing of the "depth, breadth, and comprehensive reach" of cell phones and CSLI does not automatically extend to all apps. *Carpenter*, 138 S. Ct. at 2220.

This Court should not apply the proscription of data acquisition where users voluntarily provide information--after an affirmative consent--to a third party or to the public and that information is limited in its scope. Under this Court's jurisprudence, the acquisition of the data collected by YOUBER does not constitute a search within the meaning of the Fourth Amendment.

CONCLUSION

WHEREFORE, for the reasons set forth above, Respondent, the United States of America, asks this Court to affirm the decision of the Thirteenth Circuit.

Respectfully submitted,

_____

Counsel for Respondent