Team number – P20

No. 4-422

IN THE

Supreme Court of the United States

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 PETITIONER

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Other Authorities

STATEMENT OF ISSUES PRESENTED FOR REVIEW

I. Does an individual have standing to contest a search of a rental vehicle that the individual rented on another's account with that other person's permission?

II. 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)?

STATEMENT OF FACTS

On January 3, 2019, poet and activist Jayne Austin was arrested based on the fruits of a warrantless search of her rental vehicle. R. at 2:22–3:15. Two days later, Ms. Austin was implicated for five additional robberies based on the warrantless subpoena of historical location data from a car rental service she regularly used. R. at 4:8–14. Now, she asks this Court to suppress the information gathered from the two illegal searches that violated her fourth amendment rights.

On the day of the arrest, Ms. Austin rented a 2017 Black Toyota Prius from the YOUBER ride-share service through her on-again, off-again partner's account. R. at 2:22–23. Her partner, Martha Lloyd, gave Ms. Austin permission to use the account, did not retract that permission when they broke up, and knew that Ms. Austin habitually used Ms. Lloyd's account to stay off the grid. R. at 18:24–27, 19:6–12. Though the account was registered in Ms. Lloyd's name, Ms. Austin's payment went through a credit card authorized in her own name. R. at 20:3–4. Furthermore, YOUBER's does not limit account use to only one user. Chad David, a data and information specialist at YOUBER, testified that multiple users can use one account once the account is registered. R. at 24:2–4. Even YOUBER's company policy references "all users," not just one user. R. at 29. Still, when Officer Kreuzberger saw that the YOUBER rental agreement was not in Ms. Austin's name, he determined that he did not need her consent to search the vehicle. R. 2:26–3:2.

Nothing in Ms. Austin's car itself was illegal. R. at 3:2–9. Officer Kreuzberger discovered clothes, an inhaler, shoes, a duffle bag containing money, a collection of Kendrick Lamar records, a BB gun, blankets and a pillow, a ski mask, and a cooler of tofu, kale, and homemade kombucha. *Id*. It was not until after Officer Kruezberger began rifling through Ms.

Austin's personal effects that he received a call from dispatch informing him that a person driving a YOUBER rented 2017 Black Toyota Prius and wearing a ski mask had robbed a nearby Darcy and Bingley Credit Union. R. at 3:10–15. The first three digits of the car's license plate were recorded by the credit union's security camera and matched the car Ms. Austin was driving. *Id.* Pursuant to this discovery, Officer Kruezberger arrested Ms. Austin. *Id.*

Whenever one of its vehicles is in use, YOUBER uses GPS and Bluetooth signals to keep track of its whereabouts. R. at 3:24–26. Whether the vehicle is in use or not, its timestamped location is updated every two minutes in the YOUBER database. R. at 4:6–7. When rented, tracking commences automatically when the cell phone associated with a user's account is located within the vehicle. R. at 4:1–2. YOUBER routes this data through Smoogle's satellite mapping technology, which enables it to accurately track and record the movements of the vehicles registered to certain users. R. at 22:19–25. Two days after Ms. Austin's initial arrest, Detective Boober Hamm subpoenaed YOUBER for Ms. Lloyd's account's historical location data dating back three months prior to Ms. Austin's arrest. R. at 3:21–23. Using this data, the detective pinned five more bank robberies on Ms. Austin that all occurred prior to her arrest on January 3. R. at 4:9–12.

Prior to trial, Ms. Austin's counsel filed two motions to suppress: (1) to suppress the evidence obtained through the unreasonable search of Ms. Austin's rented vehicle, and (2) to suppress the location data provided by YOUBER. R. at 1:12–15. Both motions were denied in the trial court, and the Court of Appeals for the Thirteenth Circuit upheld the denial. R. at 1:15–16; 10:6–7.

SUMMARY OF THE ARGUMENT

The Fourth Amendment requires by principle and precedent that the warrantless search of Ms. Austin's YOUBER rental vehicle and the warrantless seizure of her YOUBER location data be suppressed. First, Ms. Austin was in lawful possession and control of the YOUBER rental vehicle when police searched her car, entitling her to a legitimate expectation of privacy in the rental vehicle. *Byrd v. United States*, 138 S. Ct. 1518, 1523–24 (2018). In 2018, the Court created a bright line rule protecting the legitimate expectation of privacy of unauthorized drivers of rental cars. *Id.* at 1527. The case at bar demonstrates a clear application of this rule. Alternatively, even if the Court finds that Ms. Austin was not in lawful control of the YOUBER rental car, the circumstances of the search demonstrate that she was entitled to Fourth Amendment protection in the vehicle because Ms. Austin had a possessory interest in the YOUBER vehicle, took normal precautions to protect her privacy in the vehicle, and had exclusive control over it. *Minnesota v. Olson*, 495 U.S. 91, 99–100 (1990); *Rakas*, 439 U.S. at 153 (Powell, J., concurring); *Byrd*, 138 S. Ct. at 1527.

Second, the police's collection of Ms. Austin's rental car location data was a search because she had a legitimate expectation of privacy in that data. This is exactly the type of invasion of privacy that the Court sought to protect in *Carpenter* in 2018. *United States v. Carpenter*, 138 S. Ct. 2206 (2018). Despite Ms. Austin agreeing to the YOUBER's term and conditions by using Ms. Lloyd's app to rent YOUBER vehicles, this is not sufficient to demonstrate voluntary exposure of her information, so that the government is free to acquire it via a subpoena. *United States v. Diggs*, 385 F. Supp. 3d 648, 650 (N.D. Ill. 2019). Based on the invasive extent of the data, the acquisition was unreasonable without a warrant. *Kentucky v. King*, 563 U.S. 452, 460 (2011).

STANDARD OF REVIEW

Whether Ms. Austin had a reasonable expectation of privacy in either the YOUBER rental vehicle or the GPS location data is a question of law and thus reviewed de novo. *United States v. Williams*, 521 F.3d 902, 906 (8th Cir. 2008); *United States v. Jones*, 565 U.S. 400 (2012). Under this standard, the Court makes a non-deferential, independent evaluation of the legal issue. *Salve Regina Coll. v. Russell*, 499 U.S. 225, 238 (1991).

ARGUMENT

Ms. Austin had sufficient Fourth Amendment standing to contest the search of her rental vehicle.

The Fourth Amendment protects "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. The Amendment creates a rule that a warrantless search or seizure is presumed unreasonable, unless the government proves that an exception to the warrant requirement applies. *Katz v. United States*, 389 U.S. 347, 357 (1967). However, a defendant must first demonstrate that she was protected by the Fourth Amendment at the time a particular search or seizure occurred to argue that she is entitled to relief for a violation. *Rakas*, 439 U.S. at 143. Courts sometimes phrase this inquiry, whether the defendant was entitled to Fourth Amendment protection, as one of "standing." *Jones v. United States*, 362 U.S. 257 (1960).

I. Ms. Austin was in lawful possession and control of the YOUBER rental vehicle, demonstrating a reasonable expectation of privacy and protection under the Fourth Amendment.

A. A defendant can establish standing through one of two methods, which work together in exhibiting protection under the Fourth Amendment.

Fourth Amendment analyses begin with the question of "whether the challenged search or seizure violated the Fourth Amendment rights of a criminal defendant who seeks to exclude

the evidence obtained during it." *Rakas*, 439 U.S. at 140. Consequently, what has historically been considered a separate "standing" question is now integrated within the general analysis of every Fourth Amendment inquiry. *Id.* In other words, determining the issue of "standing" is simply the first step in establishing whether there was a Fourth Amendment violation that warrants some relief. *See Byrd*, 138 S. Ct. at 1526; *Florida v. Jardines*, 569 U.S. 1 (2013). From here, a court must decide whether the "disputed search or seizure has infringed an interest of the defendant which the Fourth Amendment was designed to protect." *Rakas*, 439 U.S. at 140.

A defendant can establish that she was protected by the Fourth Amendment when a search or seizure occurred in two ways. The first is through the legitimate expectation of privacy test, which creates a two-prong subjective and objective inquiry into the defendant's treatment of the area. *Katz*, 389 U.S. at 360–62 (Harlon, J., concurring). Since its introduction in *Katz*, this test has been adopted as the primary way to establish protection under the Fourth Amendment. *Rakas*, 439 U.S. at 143; *California v. Ciraolo*, 476 U.S. 207 (1986); *Bond v. United States*, 529 U.S. 334 (2000). In *Katz*, the Court considered whether the defendant had a constitutionally protected right to privacy in a public phone booth. *Katz*, 389 U.S. at 354. The Court held that he did, asserting that the Fourth Amendment protects "people, not places." *Id.* at 351. Justice Harlan further explained that there is a twofold requirement to establishing Fourth Amendment protection. *Id.* at 361 (Harlan, J., concurring). First, a person must have a subjective expectation of privacy. *Id.* Second, that expectation must "be one that society is prepared to recognize as 'reasonable,'" which the Court viewed as an objective standard. *Id.* Under this test, the Fourth Amendment can create "temporary private place[s]," where a person is entitled to protection despite the otherwise public nature of the space. *Id.* Temporary private places include homes in which someone is an overnight guest, dressing rooms, and bathroom stalls. *Olson*, 495 U.S. at

98; *State v. McDaniel*, 337 N.E.2d 173 (Ohio Ct. App. 1975); *Kroehler v. Scott*, 391 F. Supp. 1114 (E.D. Pa. 1975).

A defendant can also establish Fourth Amendment protection by showing that she had a proprietary interest in the area where the search or seizure occurred. Under the property rights test, there are certain constitutionally protected areas or things, which are most frequently defined as private property that a person owns. *Jardines*, 569 U.S. at 5–6. Examples include a person's own home and the area immediately surrounding it – called the "curtilage", a person's own car, the types of things a person typically keeps in their home, such as private documents, and a person's cell phone. *Jardines*, 569 U.S 1; *Jones*, 565 U.S. 400; *Olmstead v. United States*, 277 U.S. 438 (1928); *Riley v. California*, 134 S. Ct. 2473 (2014). The property rights doctrine has long been tied to common law trespass. *Jones*, 565 U.S. at 405. Under this approach, Fourth Amendment protection is guaranteed when a person occupies another's property without their consent. *Id.* However, the property rights protection does not extend to all private property. For example, it does not apply if a police officer could observe something while passing by private property while on a public road. *Ciraolo*, 476 U.S. at 213. Fourth Amendment protection for such property and the people occupying it starts when an officer "steps off those thoroughfares and enters the … protected areas." *Jardines*, 569 U.S. at 7.

This Court emphasizes the importance of considering the property rights approach separately from the legitimate expectation of privacy test. *Jones*, 565 U.S. at 404; *see also Jardines*, 569 U.S. at 5. Although property rights are no longer the sole baseline for Fourth Amendment protection, the addition of the *Katz* test does not eliminate the protections the Constitution provides when the government invades a protected area. *Jardines*, 569 U.S. at 5.

Therefore, the legitimate expectation test and the property rights test work together in establishing Fourth Amendment protection, or "standing". *Id.*

It is important to respect and adhere to the dual approach to establishing "standing" because the two tests allow for both protection as it was understood at the time the Amendment was written and as it evolves with the progress of technology. *Jones*, 565 U.S. at 411. The property rights approach permits protection against unreasonable searches and seizures to the degree afforded when the Fourth Amendment was adopted. *Id.* The legitimate expectation of privacy test encompasses any alleged violation beyond such a clear invasion of property. *Id.* Further, preserving the property rights approach to Fourth Amendment protection allows for swifter and simpler resolutions of cases when a constitutionally protected area is involved. *Id.* at 404–05. These cases risk becoming unnecessarily complicated if a court were to employ only the *Katz* test. *Id.* at 412. Therefore, although the legitimate expectation of privacy test is the primary mode of establishing Fourth Amendment protection, the property rights approach remains crucial when analyzing Fourth Amendment challenges.

B. The Fourth Amendment absolutely protects a driver's reasonable expectation of privacy in a rental vehicle.

In Fourth Amendment jurisprudence, there are bright line rules that establish areas in which people are absolutely protected from warrantless searches and seizures. Through these rules, the Court recognizes not only that a person has a subjective expectation of privacy in a particular area, but also that the area is one in which society believes that person's expectation will *always* be reasonable. *See Katz*, 389 U.S. at 361. The most common example of this is the rule that a person is always protected from government invasion while in their own home. *Payton v. New York*, 445 U.S. 573 (1980); *see also Kyllo v. United States*, 533 U.S. 27 (2001).

Recently, the Court created such a bright line rule for drivers of rental cars who are not listed as an authorized driver on the rental agreement. *Byrd*, 138 S. Ct. at 1523–24. In *Byrd*, the petitioner's friend rented a car and signed the rental agreement, which indicated that permitting an unauthorized driver to operate the vehicle was a violation of that agreement. *Id.* at 1524. However, after signing the agreement and receiving the keys to the car, petitioner's friend gave him the keys, permitting him to drive it. *Id.* While petitioner was driving the rental vehicle, he was pulled over for a traffic violation. *Id.* After the police officers realized that he was not listed as an authorized driver on the rental agreement, they determined that he did not have a reasonable expectation of privacy and searched the car without his consent. *Id.* at 1525.

The Court determined that someone in "lawful possession and control" of a rental vehicle generally has a reasonable expectation of privacy in it even if the rental agreement does not list her as an authorized driver. *Id.* at 1531. Because of the unauthorized driver's right to exclude another from the car, the Fourth Amendment's protection applied. *Id.* at 1527; *Rakas*, 439 U.S. at 144, n.12 ("one who … lawfully possesses or controls property will in all likelihood have a legitimate expectation of privacy by virtue of the right to exclude.")

The Court also stated that violating a rental agreement's provisions does not automatically result in eliminating a defendant's reasonable expectation of privacy because rental agreements contain long lists of restrictions that people violate frequently. *Byrd*, 138 S. Ct. at 1529. YOUBER's rental policy parallels these standard rental agreements, with restrictions on how a driver must return a YOUBER vehicle, including the specific charge or gas level it must have, where a user can drive the vehicle, and how the driver can use the vehicle. R. at 23:9–28. The Court in *Byrd* maintained, "few would contend that violating provisions like these has anything to do with a driver's reasonable expectation of privacy." *Byrd*, 138 S. Ct. at 1529

(referring to standard prohibitions against driving on unpaved roads and using a cell phone in rental car agreements). Further, there should not be a distinction between these types of standard restrictions and a provision in a rental agreement impeding an unauthorized driver from operating the vehicle. *Id.* In fact, the Court pointed out that there may be reasons why it is important for authorized drivers to allow an unauthorized driver to get behind the wheel of her rental car. *Id.* For example, if the authorized driver was "drowsy or inebriated" and did not feel it was safe for her to drive the car, we should encourage her to ask a friend to drive instead. *Id.* We would not want her to feel constricted in asking for assistance simply because a provision on her rental agreement, or her YOUBER driver authorization form, says she should not. *Id.*

C. Ms. Austin is precisely the type of driver the Court intended to protect through its rule in Byrd.

Byrd's bright line rule that an unauthorized driver of a rental vehicle has a reasonable expectation of privacy in it applies to Ms. Austin because she was in lawful possession and control of the YOUBER rental vehicle at the time the police stopped and searched the car. Although Ms. Austin's name was not listed on the rental agreement, she had permission from the YOUBER account holder, Ms. Lloyd, to rent vehicles in her name through the YOUBER app.

Both the district and appellate courts erred in focusing on the nature of the relationship between Ms. Austin and Ms. Lloyd in their analyses. The Supreme Court never stated in *Byrd* that the authorized and unauthorized drivers of the rental vehicle have to be in a certain type of relationship with one another. In fact, the lower courts' evaluating of Ms. Austin and Ms. Lloyd's relationship is exactly the kind of intrusion of privacy the Fourth Amendment intends to protect. *See Carpenter*, 138 S. Ct. 2206. The basic purpose of the Amendment is to "safeguard the privacy and security of individuals against arbitrary invasions by government officials." *Id.* (quoting *Camara v. Mun. Court of S.F.*, 387 U.S. 523 (1967)). Through this protection, a

significant focus is placed on the things in a person's life she keeps most private. *Id.* at 2214. The intimate aspects of a person's relationship with another encompasses just the type of information a person intends to keep to herself, or between herself and her partner. *See Id.* at 2216. The lower courts invaded exactly the kind of private information the Fourth Amendment protects when it assessed the nature of Ms. Austin's relationship with Ms. Lloyd.

Instead of a court, without adequate fact-finding, delving into the complex dynamics of an intimate relationship, the sole question, based on both previous rulings by this Court and the general spirit of the Fourth Amendment, is whether Ms. Lloyd gave Ms. Austin permission to rent the cars through her account. This alone establishes whether Ms. Austin was in legal possession of the YOUBER rental vehicle. Three key facts already established in the record indicate that Ms. Lloyd did give Ms. Austin such permission—there is no room nor need in the Fourth Amendment analysis to make unwarranted assumptions regarding the stability of personal relationships.

First, Ms. Lloyd explicitly granted Ms. Austin permission to use her YOUBER app to rent vehicles while the two were living together. R. at 19:1. As two people that had been in a relationship for several years, living together for a significant amount of that time, Ms. Lloyd knew Ms. Austin was without a permanent home or a car of her own. R. at 18: 24–27. Therefore, Ms. Lloyd knew that Ms. Austin would have to continue to use ride-sharing and rental services, like YOUBER, to get from place to place.

Second, Ms. Lloyd knew the types of activities that Ms. Austin was involved in. Even after the relationship ended, Ms. Austin would frequently send Ms. Lloyd letters telling her "what she was doing and where she was." R. at 19:21–22. Ms. Lloyd even took the time to respond to one of those letters, telling Ms. Austin that she still "loved her" and leaving open the

potential that the two would someday get back together. R. at 19:26–27. Knowing what Ms. Austin was involved in, Ms. Lloyd had notice that she needed transportation, likely through YOUBER, to continue that involvement.

Finally, despite knowing all of this information about Ms. Austin, including her involvement in protesting activities and potential bank robberies, Ms. Lloyd continued to let Ms. Austin use her YOUBER account for rental car services. She did not delete the account or change the password, despite starting to use a new app, BIFT, for all of her ridesharing needs. R. at 19:11, 20:2–4. She did not remove Ms. Austin as an authorized user of her credit card, which she was using to pay for YOUBER's services. R. at 19:2–3. She did not check the account to see whether Ms. Austin had been renting cars in her name. R. at 20:1. She did not give Ms. Austin any clear indication that she was rescinding her permission to use the YOUBER account. R. at 20:12–14.

Together, these facts indicate that Ms. Lloyd knew Ms. Austin was using her YOUBER app and renting vehicles in her name. Even though Ms. Austin was not specifically listed on the rental agreement as an authorized driver, she was in lawful possession and control of the rental vehicle at the time law enforcement stopped and searched her car. Therefore, under *Byrd*'s bright line rule, Ms. Austin had a reasonable expectation of privacy in the YOUBER rental vehicle and was entitled to protection under the Fourth Amendment.

II. If the Court finds that Ms. Austin was not in lawful control of the YOUBER rental vehicle, the facts and circumstances still demonstrate she possessed Fourth Amendment protection.

If the Court holds that Ms. Austin's case falls within a question left open in *Byrd*, or that she intentionally used "a third party to procure a rental car by a fraudulent scheme for the purpose of committing a crime," there would be an absence of a clear rule or precedent to follow.

Byrd, 138 S. Ct. at 1531. In Fourth Amendment cases, when there is no precedent to adopt, courts turn to the individual facts and circumstances of the case to determine whether the defendant had a legitimate expectation of privacy. *Opperman*, 428 U.S. at 375.

Three factors help demonstrate a legitimate expectation of privacy in the absence of a bright line rule. First is whether a person had a possessory interest in the area. *Olson*, 495 U.S. at 99–100. A possessory interest is distinct from the proprietary interest discussed above in that a person does not have to own property to have a possessory interest in it. *See id.* (reasoning that an overnight houseguest had a legitimate expectation of privacy in the apartment they were staying in). A defendant can demonstrate that even temporary possession of an area or effect is sufficient to establish Fourth Amendment protection. *Id.* The second factor is whether the person took normal precautions to protect her privacy in the area. *Rakas*, 439 U.S. at 152 (Powell, J., concurring). Normal precautions are those "customarily taken by those seeking privacy." *Id.* A common example is keeping personal effects inside a locked or closed compartment. *United States v. Chadwick*, 433 U.S. 1, 11 (1977).

The third factor which, as already mentioned is crucial in Fourth Amendment standing cases, is whether the person had exclusive control over the area in which the search or seizure occurred. *Byrd,* 138 S. Ct. at 1527. Exclusive control is most frequently analyzed with respect to the person's ability to exclude others from the premises. *Olson*, 495 U.S. at 99. In cases that focused on a defendant's expectation of privacy in a car, the Court has considered whether she had control over the keys to the car and, therefore, any of the locked compartments within the vehicle. *Rakas*, 439 U.S. at 154 (Powell, J., concurring). The Court has further considered whether she had the doors to the car locked and the windows rolled up in an effort to protect both her own privacy and any valuables stored within the car. *Opperman*, 428 U.S at 379 (Powell, J.,

concurring). These factors are not intended to be determinative in establishing protection under the Fourth Amendment, as "[t]he range of variables in the fact situations of search and seizure is almost infinite." *Rakas*, 439 U.S. at 156 (Powell, J., concurring). Instead, the Court should weigh the importance of each factor with reference to the case before it. *See id.*

Applying the above the factors to the case at the bar, Ms. Austin had a reasonable expectation of privacy in the YOUBER rental vehicle. First, Ms. Austin can establish a temporary possessory interest in the YOUBER vehicle. She kept many personal effects, such as her clothes, shoes, her inhaler, food, bedding, and a pillow in the car. R. at 3:4–8. The arresting officer even admitted that the car appeared to have been "lived in" at the time he searched the vehicle. R. at 3:6. For the period of time that she rented the car, Ms. Austin treated it as her own, establishing a temporary possessory interest. Second, Ms. Austin took normal precautions to protect her privacy in the car by keeping her items in the trunk and out of the plain view. R. at 3:2–5. Finally, Ms. Austin had the ability to exclude other people from the car. She had the keys to the car and therefore, had the ability to lock both the car and any compartments in it. R. at 23:10–11. While she had the YOUBER vehicle rented through Ms. Lloyd's account, no other YOUBER users had the ability to rent that vehicle. R. at 2:13–14. If anyone else tried to rent the car, Ms. Austin would have been entitled to exclude them from it.

These factors demonstrate that, even if the Court holds that Ms. Austin does not fall within *Byrd*'s bright line rule, she still had a legitimate expectation of privacy in her YOUBER rental vehicle at the time the search occurred. Therefore, she was entitled to the protection of the Fourth Amendment. The police were not permitted to search the vehicle without either her consent or a warrant.

The warrantless acquisition of Ms. Austin's rental car location data was a search within the meaning of the Fourth Amendment.

I. Law enforcement's collection of Ms. Austin's rental car location data was a search because Ms. Austin had a reasonable expectation of privacy in her movements.

Collecting an individual's location data is a search of her physical locations and movements throughout a period of time. *See Carpenter* 138 S. Ct. at 2215. A search occurs when the government intrudes on a person's reasonable expectation of privacy. *Katz,* 389 U.S. 347. An expectation of privacy is reasonable when an individual "seeks to preserve something as private," and that expectation is "one that society is prepared to recognize as reasonable." *See Katz*, 389 U.S. at 361 (Harlan, J., concurring), *Smith v. Maryland*, 442 U.S. 735, 739 (1979).

Technological advancements cannot overwhelm Fourth Amendment protections. Historically, the Fourth Amendment was tied heavily to trespass law, and required a physical intrusion for violation. *Carpenter*, 138 S. Ct. 2213. *Katz* was a response to the changing technological landscape. Sensitive conversations no longer happened in a person's home—they happened through wires. *Katz*, 389 U.S. at 347. Technological advances are not loopholes in Fourth Amendment protection. The areas of a person's private life that are protected by the Fourth Amendment has always been informed by what the founders considered an unreasonable intrusion when the Amendment was adopted. *Carpenter*, 138 S. Ct. at 2214 (citing *Carroll v. United States*, 267 U.S. 132, 149 (1925)). If a search was unreasonable or impossible for the founders, it remains so today. *Id.*

This Court has already explained that a person has a reasonable expectation that a cell phone company will not divulge her location data to law enforcement without a warrant, (*Carpenter*, 138 S. Ct. at 2217) and that warrantless vehicle tracking raises similar concerns (*Carpenter*, 138 S. Ct. at 2215 (explaining that in *Jones*, 565 U.S. 400, five justices agree that serious privacy concerns are raised when considering warrantless vehicle GPS tracking). The

issue in this case is simply whether an individual has a reasonable expectation that her location data will not be searched by law enforcement when the data is automatically collected by the rental car company, not a cell phone company. This distinction is irrelevant—it would amount to amount to defining Fourth Amendment protections based on what entity collected data, not the data that was collected, or the intrusion of privacy that resulted. If Ms. Austin had a reasonable expectation that her location data would remain private, its collection constitutes a search.

A. Ms. Austin did not voluntarily divulge her location information, and therefore has a reasonable expectation in its privacy.

A person has no reasonable expectation of privacy in information or areas that are voluntarily exposed to the public. *E.g.*, *United States v. Knotts*, 460 U.S. 276 (1983); *Katz*, 389 U.S. 400. Being in public does not expose all an individual's secrets that are otherwise unexposed to the wandering eye or ear. *Katz*, 389 U.S. at 352. In *Katz*, although defendant was visible to passersby, by shutting the door to a phone booth, he was "entitled to assume that the words he utters into the [phone] will not be broadcast to the world." *Id.* It follows that in *Knotts*, where the information sought by the police was where defendant drove, this court held that defendant risked exposure of this path by driving on public roads. *Knotts*, 460 U.S. 276 (citing *Cardwell v. Lewis*, 417 U.S. 583, 590 (1974) and *Rakas v. Illinois*, 439 U.S. 128, 153-154 (Powell,, J., concurring)). The use of a beeper to track this path revealed nothing otherwise unknowable through traditional surveillance. *Id.* As such, its use did not violate defendant's reasonable expectation of privacy. *Id.*

A person can also lose her reasonable expectation of privacy by voluntarily exposing her information to a third party. *Smith*, 442 U.S. at 744; *United States v. Miller*, 425 U.S. 435, 441-43 (1976); *United States v. Hood*, 920 F.3d 87 (1st Cir. 2019). For instance, in *Smith*, defendant voluntarily dialed numbers into a telephone, thereby exposing the numbers to his telephone

company. *Smith*, 442 U.S. at 744. Similarly, in *Miller*, defendant voluntarily deposited checks into a bank account, thereby exposing the information on the check to the bank. *Miller*, 425 U.S. 441-43. This is no different for digital data. *Carpenter*, 138 S. Ct. 2206; *Hood*, 920 F.3d 87. In *Hood*, defendant voluntarily logged into a website, thereby exposing his login information and internet protocol (IP) address. *Hood*, 920 F.3d at 92. However, in *Carpenter*, where defendant's cell site location information (CSLI) was frequently created by other people calling or texting, or apps independently updating, the release of CSLI required no affirmative act of the user. *Carpenter*, 138 S. Ct. at 2220. Thus, in all cases but *Carpenter*, the Court found the exposure of information to cause a diminished expectation of privacy.

A privacy policy disclosure that does not inform its users of the extent of tracking or location data recording cannot show voluntary exposure. *Diggs*, 385 F.Supp.3d at 650. In the age of technologically-stored information, many companies require private individuals to disclose their personal information to them in order to use the company's services. In *Diggs*, when defendant's wife purchased a vehicle on credit from a car company, her contract said "if your vehicle has an electronic tracking device, you agree that we may use this device to find the vehicle." *Id.* at 650. However, the Court explained that this was not sufficient for true voluntary exposure of information; the contract did not alert the defendant that the vehicle would be tracked continuously, its location would be updated every five minutes, or that historical data would be recorded. *Id.* at 660-61. The Court held that without full knowledge of the extent of data tracking, defendant could not voluntarily consent, and did not lose any Fourth Amendment protection. *Id.*

Finally, in addition to voluntariness, this court also considers the content of information exposed to a third party in determining whether that information is entitled to a reasonable

expectation of privacy. *Carpenter*, 138 S. Ct. at 2218; *Smith*, 442 U.S. 741; *Miller*, 425 U.S. 443; *Hood*, 920 F.3d 87. If the privacy interest in exposed information is too great, it may not lose Fourth Amendment protection. *Carpenter*, 138 S.Ct. 2218. The privacy interests in phone numbers, deposit slips, or IP addresses could not compare to the privacy interests in CSLI. On the other hand, location data is far more concerning. In her concurrence in *United States v. Jones*, Justice Sotomayor stated

> Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may "alter the relationship between citizen and government in a way that is inimical to democratic society."

United States v. Jones, 565 U.S. 400, 416 (Sotomayor, J., concurring) (quoting *United States v. Cuevas-Perez*, 640 F.3d 272, 285 (C.A.7 2011)).

Here, even though Ms. Austin drove on public roads, she did not expose her historical location information to the public. Unlike in *Knotts*, Ms. Austin's movements could not be readily obtained by traditional mechanisms, like visual surveillance. While the beeper in *Knotts* tracked defendant for only a several hour drive, Ms. Austin's location information on the YOUBER app tracked her for months. While a person understands she can be surveilled when she is on public roads, she cannot expect that law enforcement would be able to warrantlessly access the entirety of her rental car location history simply because she drove on public roads. Like in *Katz*, she has effectively kept the door shut as to her history, even though her current physical location may be revealed.

It follows that Ms. Austin did not expose her location information simply by sharing it with YOUBER. YOUBER GPS location signals are sent from rental vehicles to the YOUBER

mainframe every two minutes—whether or not a vehicle is rented. R. at 29. Although the YOUBER mainframe is also signaled whenever a person gets in or out of her rental vehicle, this has no effect on whether the GPS signals are sent, it is just more data that is collected. R. at 22:21–27, 29. Unlike dialing phone numbers, depositing checks, and logging into an online account, no truly voluntary action on the part of the YOUBER user occurs that gives away a person's location. The third-party doctrine relies on the idea that an individual assumes the risk that her information will be conveyed to law enforcement by *voluntarily* exposing it to a third party. If no voluntary exposure existed, no risk was assumed.

Neither does the existence of a privacy policy show that Ms. Austin's data was voluntarily given. YOUBER's specifically does not limit the number of users on an account, but only notifies the user who created the account of its tracking policies. R. at 24:2–11. Any other user could not possibly be aware that her data is being tracked, recorded, and updated every two minutes. Like in *Diggs*, any secondary user would not know about such an expansive privacy policy. A user could not reasonably expect a large company to keep such close tabs on them and their use without having first been notified.

Furthermore, the records collected by YOUBER are location records, which have far fewer limitations than phone numbers, deposit slips, or IP addresses. Like in *Carpenter*, YOUBER data location records are collected automatically, stored automatically, and can reveal a great amount of information about a person—effectively creating a map of who a person is based on where she goes. As such, location records must be entitled to greater Fourth Amendment protection.

It is clear that Ms. Austin had a reasonable expectation of privacy in the location data collected by YOUBER. Ms. Austin did not disclose her location by being in public or through

automatic location updates. She did not know about, consent to, or expect that her data could be tracked to the extent that it was. For that reason, law enforcement's warrantless acquisition of her data was a search within the meaning of the Fourth Amendment.

II. Law enforcement's search of Ms. Austin's location data was unreasonable and required a warrant.

Reasonableness presumes that a warrant is required wherever law enforcement officers conduct a search for evidence of criminal wrongdoing. *Riley*, 573 U.S. at 382 (2014) (citing *Vernonia School Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995)); *Carpenter*, 138 S. Ct. at 2221. While there are exceptions to the warrant requirement, the parties in this case have stipulated that no existing exception to applies here. *King*, 563 U.S. at 460; R. 31, ¶1. Therefore, unless this Court creates a new exception to the warrant requirement for seizures and searches of rental car location data obtained two days post-arrest, this Court must rule law enforcement's actions unconstitutional.

To determine the reasonableness of a warrantless search, the Court applies a balancing test. *Riley*, 573 U.S. at 385-86 (citing *Wyoming v. Houghton*, 526 U.S. 295 (1999)). The Court weighs any legitimate interest the government has in not obtaining a warrant against the invasion of privacy suffered by an individual who is searched without a warrant. The exceptions to the warrant that exist today largely arise from "the exigencies of the situation,", such as the desire to preserve evidence, or from the legitimate government interest in protecting the safety of law enforcement officers and the greater public. *Id.* at 383; *King*, 563 U.S. at 460 (citing *Mincey v. Arizona*, 437 U.S. 385, 394 (1978)). Where no legitimate interest exists, no exception can be created.

Waiting for a warrant to search digitally stored information presents neither a threat of physical harm to officers nor destruction of evidence. *Riley*, 573 U.S. at 387-88. In *Riley*, the Court declined to create an exception to a search of digital information stored on an arrestee's cell phone for two reasons. *Id.* at 386. First, evidence on a phone could not be destroyed when the phone is confiscated from the arrestee and disconnected from its network to prevent remote data wiping—eliminating any destruction of evidence justification for a warrantless search. *Id.* at 387. Second, information data stored on a phone plainly could not harm police officers—eliminating any safety justification for a warrantless search. *Id.* As such, the burden of obtaining a warrant prior to searching a cell phone was low and did not create an unreasonable hurdle for law enforcement. *Id.*

Even if a legitimate interest exists, this interest must be balanced against a person's interest in preserving her privacy. *Id.* at 383. In this balancing, the Court is compelled to consider the expansive nature of information warrantlessly accessed, as well as the number of individuals whose Fourth Amendment rights would be impacted by a warrantless search. *Id.*, *see also Carpenter*, 138 S. Ct. at 2218, 2220.

First, the expansive nature of data stored in cellular phones implicates a massive privacy interest. *Riley*, 573 U.S. at 383; *Carpenter*, 138 S. Ct. at 2220. In *Riley*, the court found that private information digitally stored in cell phones could reveal a massive assortment of personal information that never before would have been accessible incident to an arrest. *Riley*, 573 U.S.at 393-95. Should a phone be searched without a warrant, the government would have intimate knowledge of all a person's privacies such private photos, emails, texts, google search history, passwords to accounts, calendars, and contacts. *Id.* at 394. Importantly, the *Riley* Court notes location data and information stored on apps as types of data to which law enforcement should

not have access without a more specific warrant. *Id.* at 396. Furthermore, even if the government could obtain each of these things separately, the information "reveal[s] much more in combination than an isolated record." *Id.* The entirety of an individual's private life is now stored on a phone that is carried wherever she goes.

The Court in *Carpenter* focused specifically on location information retrieved from cell phones. Cell-site location information (CSLI) creates a "detailed, encyclopedic, and effortlessly complied" log of a person's exact movements throughout her day for years and reveals much more than just her location. *Carpenter*, 138 S. Ct. 2216-17 (citing *Jones*, 565 U.S. 416 (Sotomayor, J., concurring)).

Location data retrieved from a vehicle is just as revealing. Although *United States v. Jones* was decided on trespassory fourth Amendment issues, Justices Sotomayor, Alito, Ginsburg, Breyer and Kagan all found that continuous GPS tracking of a vehicle can implicate the Fourth Amendment. *Jones* 565 U.S. at 413, 418 (Sotomayor, J., concurring and Alito, J., concurring). The justices reasoned that location tracking reveals more than movements—it can reveal a person's "familial, political, professional and sexual associations." *Id.* at 415. Police should only have access to such intimate and private information through the use of a warrant.

Furthermore, access to digital location data gives law enforcement the opportunity to essentially "travel back in time to retrace a person's whereabouts" to see what a person is doing before she was ever under any suspicion of criminal wrongdoing, potentially years into the past with perfect recollection. *Carpenter*, 138 S. Ct. at 2218. In *Carpenter*, the Court was very concerned by retrospective data because it is otherwise unknowable. *Id.* Fourth Amendment protections are informed by founding-era understandings of the types of searches that were possible for police to execute. *Kyllo*, 533 U.S. at 40; *Carroll v. United States*, 267 U.S. 132, 149

(1925). Never before "could police have decided today to track [an individual] 24 hours a day, seven days a week, five months ago." Transcript of oral argument at 27, *Carpenter v. United States,* 138 U.S. 2206 (2018) (No. 16-402). A warrantless search of the past is an unreasonable search.

Significantly, both *Riley* and *Carpenter* considered the number of individuals impacted by warrantless searches of cell phones and their accompanying CSLI records.. *Riley,* 573 U.S. at 385. In *Riley*, the Court understood that cell phones are now such an "insistent part of daily life" that they were nearly a "feature of human anatomy." *Id.* Accordingly, warrantless CSLI tracking could quickly lead to omnipresent police surveillance, to which only those few without phones would be immune. *Carpenter,* 138 S. Ct. at 2218. It follows that to keep any expectation of privacy in one's physical location or digital information, one would have to give up using a cell phone. In today's society, where an individual's job, school, relationships, transportation, appointments, and communication rely on access to a cell phone, such a request is unreasonable.

Here, the Court is again asked to balance the burden of a warrant with the prospect of living in Bentham's panopticon.[1] As in *Riley,* neither officer safety nor destruction of evidence is threatened by requiring a warrant for the seizure of YOUBER location data records. Arguably, location data records pose even less of a threat to these governmental concerns than cell phones. Unlike personal records kept on an individual's cell phone, YOUBER location data records are kept by the company. Even if the individual wished to destroy evidence of her travels, she would

[1] Jeremy Bentham, a utilitarian philosopher, initially devised the idea of a panopticon as an efficient method for controlling the behavior of those who would otherwise wish to act out. The panopticon is generally thought of as a prison operated by a single guard in which all the prisoners are in individual cells that all face a guard's tower. The guard in the tower can see into the cells, but the prisoners cannot see into the guard tower, and do not know when they are being watched, which compels them to behave at all times. This concept has been critiqued not only as the breeding ground of total oppression and social control, but as a direct metaphor for modern surveillance technology. Michel Foucault, *Discipline and Punish: The Birth of the Prison* 200 (Alan Sheridan trans., Vintage Books 2d ed. 1995) (1977).

not be able to. Thus, the government bears no added burden in its familiar obligation to get a warrant.

Conversely, warrantless searches of data come at a great cost to the individual. Like most cell phone companies, YOUBER systematically tracks and catalogues an individual's vehicle usage history including everywhere she has taken a car. R. at 29. If the government is able to access this information without a warrant, it will have unfettered and unsupervised access to intimate details in our lives that we do not wish to disclose. Without the requirement of a warrant, no record of our movements would be protected by the Fourth Amendment. *Carpenter*, 138 S. Ct. at 2222.

The *Carpenter* doctrine must extend to more than CSLI. If the Court distinguishes *Carpenter* from this case simply because the tracking mechanism was a car, not a phone, it will define Fourth Amendment protections based on whether a person is on foot or driving in a vehicle. Such a ruling would ignore that both CSLI and YOUBER's location records rely on automatically connected location information. The release of any location information will have the same impact the Court sought to prevent in *Carpenter*. Suddenly, using a rental car becomes risking exposure of one's attendance of a Pride Parade, a mosque, a synagogue, or a Black Lives Matter rally. Renting a car would mean telling law enforcement about one's frequent patronage of a gay bar, a liquor store, or having gone to a women's shelter, an abortion clinic, or a therapist. Even more chilling, it could mean not doing one of these things for fear of someone else learning that information about you. Additionally, retrospective data allows law enforcement can examine these records to see where a person *used* to go, where they *used* to live, and how they have changed. This is a massive invasion into a person's private life that cannot continue without probable cause and judicial supervision.

Should the Court hold that warrantless collection of location data from YOUBER is constitutional, its decision will affect the privacy interests of millions. Alone, YOUBER is used by 40 million Americans. R. at 22:12-15. Warrantless access to the location data of millions of people is the exact type of expansion of law enforcement power that was ruled unconstitutional in *Carpenter*.

Moreover, this Court must consider the impact its ruling will have on future cases. The impact of vehicle location tracking does not end with app-based ride-hailing and rental services. More and more frequently, private cars are embedded with tracking devices by manufacturers. Peter Holley, *Big Brother On Wheels: Why your Car Company knows more About you than your Spouse*, WASH. TIMES, Jan. 15, 2018, https://www.washingtonpost.com/news/innovations/wp/2018/01/15/big-brother-on-wheels-why-your-car-company-may-know-more-about-you-than-your-spouse/. Holley explains,

> By monitoring his everyday movements, an automaker can vacuum up a massive amount of personal information about someone like Dunn, everything from how fast he drives and how hard he brakes to how much fuel his car uses and the entertainment he prefers. The company can determine where he shops, the weather on his street, how often he wears his seat belt, what he was doing moments before a wreck — even where he likes to eat and how much he weighs.

Id. At present, law enforcement can subpoena a car company and acquire any of this information without probable cause, judicial oversight, or even a good reason. This is wrong. This silences associational and expressive freedoms for fear that the government is always watching. This directly contradicts the intention of the Fourth Amendment to prevent unreasonable invasions into the private spheres of a person's life. Here, nothing about the government's actions was reasonable, and for that reason, a warrant was required.

Without relying on CSLI, law enforcement can still paint an extensive and accurate picture of a person's life with data collected by other apps. *Riley*, 573 U.S. at 396. Today, many

apps running in the background of a person's phone and continuously updating are recording a person's location. *Carpenter*, 138 S. Ct. at 2222. As such, the holding in today's case can extend not only to automatically collected information from a vehicle, but to all automatically collected location information from other third parties. This decision will impact how Americans live their lives in modern society.

If law enforcement's infiltration into the private lives of American citizens are justified, it is only by precedents made by courts that could not imagine the technologies of today. As technology advances, so must the law. If Fourth Amendment rights are not to be smothered by advancing technology, this Court must be prepared and also actively rule that an individual's automatically collected data, even if stored by a third party, is subject to a reasonable expectation of privacy, and is out of reach of government officials absent a valid warrant.

CONCLUSION

For the aforementioned reasons, the Court should first find that Ms. Austin was protected by the Fourth Amendment when law enforcement initially stopped and searched her YOUBER rental vehicle. Second, the Court should hold that the acquisition of the GPS location data from the YOUBER app was a search under the Fourth Amendment. Accordingly, the Court should reverse the circuit court's denial of Ms. Austin's motions to suppress and remand her claim for further proceedings consistent with its opinion.