

IN THE SUPREME COURT OF OHIO
CASE NOS. 2024-1083

STATE OF OHIO,)	
Plaintiff-Appellee,)	
)	
)	On Appeal from Franklin
vs.)	County Court of Appeals
)	Tenth Appellate District
MAMADOU DIAW,)	
Defendant-Appellant.)	C.A. Case Nos. 21AP-614
)	

**AMICUS BRIEF OF OHIO PROSECUTING ATTORNEY'S ASSOCIATION IN SUPPORT OF
APPELLEE-STATE OF OHIO**

MICHAEL C. O'MALLEY (#0059592)
Cuyahoga County Prosecutor

DANIEL T. VAN (#0084614)
KRISTEN L. HATCHER (#0093864)
Assistant Prosecuting Attorneys
The Justice Center, 8th Floor
1200 Ontario Street
Cleveland, Ohio 44113
216-443-7800
dvan@prosecutor.cuyahogacounty.us

Counsel for Amicus Curiae
Ohio Prosecuting Attorney's Association

SHAYLA FAVOR (#90418)
Franklin County Prosecutor

SETH L. GILBERT (#0072929)
Chief Counsel, Appeals Unit
373 South High Street, 13th Floor
Columbus, Ohio 43215
614-525-3555
sgilbert@franklincountyohio.gov

Counsel for Appellee, State of Ohio

ADAM G. BURKE (#0083184)
625 City Park Avenue
Columbus, Ohio 43206
614-280-9122
burke142@gmail.com

Counsel for Appellant – Mamadou Diaw

DAVE YOST (#0056290)
Ohio Attorney General

T. ELLIOT GAISER (#0096145)
Solicitor General
ZACHARY P. KELLER (#0086930)
Deputy Solicitor General
30 East Broad Street, 17th Floor
Columbus, Ohio 43215
614-466-8980

Counsel for Amicus Curiae,
Ohio Attorney General

TABLE OF CONTENTS

Table of Authorities.....	i
Introduction and Statement of Amicus Interest	1
Statement of the Case and Facts.....	2
Law and Argument.....	4
PROPOSITION OF LAW (ACCEPTED FOR REVIEW): THE UNITED STATES SUPREME COURT’S HOLDING IN <i>CARPENTER</i> AND RELATED CASES HOLD THAT INDIVIDUALS MAINTAIN A PRIVACY INTEREST AND ATTENDANT FOURTH AMENDMENT PROTECTIONS IN THE WHOLE OF THEIR MOVEMENTS, INCLUDING THEIR PHYSICAL LOCATION.....	4
Conclusion.....	20
Certificate of Service	21

Table of Authorities

CASES

<i>Athens v. Wolf</i> , 38 Ohio St.2d 237 (1974).....	6
<i>Cardwell v. Lewis</i> , 417 U.S. 583 (1974).....	10
<i>Carpenter v. United States</i> , 585 U.S. 296 (2018).....	<i>passim</i>
<i>Carroll v. United States</i> , 267 U. S. 132 (1925).....	9
<i>Commonwealth v. Almonor</i> , 482 Mass. 35 (2019)	13
<i>Commonwealth v. Mora</i> , 485 Mass. 360 (2020).....	14, 15
<i>Donovan v. Lone Steer, Inc.</i> , 464 U.S. 408 (1984).....	6
<i>Katz v. United States</i> , 389 U.S. 347 (1967).....	17
<i>People v. Tafoya</i> , 494 P.3d 613 (Colo. 2021)	14
<i>Sanchez v. Los Angeles Dept. of Transp.</i> , 39 F.4th 548 (9th Cir.2022)	18, 19
<i>See v. City of Seattle</i> , 387 U.S. 541 (1967).....	6
<i>Smith v. Maryland</i> , 442 U.S. 735 (1979).....	16
<i>State v. Banks-Harvey</i> , 2018-Ohio-201	5
<i>State v. Brown</i> , 2003-Ohio-3931	5

<i>State v. Burnside</i> , 2003-Ohio-5372	5
<i>State v. Diaw</i> , 2024-Ohio-2237 (10th Dist).....	<i>passim</i>
<i>State v. Fanning</i> , 1 Ohio St.3d 19 (1982)	5
<i>State v. Gause</i> , 2022-Ohio-2168 (2d Dist.)	12, 13
<i>State v. LaRosa</i> , 2021-Ohio-4060	6
<i>State v. Robinette</i> , 80 Ohio St.3d 234 (1997).....	5
<i>State v. Snowden</i> , 2019-Ohio-3006 (2d Dist.)	12
<i>United States v. Contreras</i> , 905 F.3d 853 (5th Cir.2018)	18
<i>United States v. Dennis</i> , 41 F.4th 732 (5th Cir. 2022)	14
<i>United States v. Di Re</i> , 332 U. S. 581 (1948).....	9
<i>United States v. Gregory</i> , __ F.4th __, 2025 U.S. App. LEXIS 3431 (Feb. 13, 2025)	14
<i>United States v. Hay</i> , 95 F.4th 1304 (10th Cir.2024)	14
<i>United States v. Jones</i> , 565 U.S. 400 (2012).....	11, 17
<i>United States v. Knotts</i> , 460 U.S. 276 (1983).....	10, 12
<i>United States v. Miller</i> , 425 U.S. 435 (1976).....	16, 17

STATE RULES

Ohio Criminal Procedure Rule 17	6
---------------------------------------	---

OTHER AUTHORITIES

Android (on managing permissions) https://perma.cc/UAF3-K7K6	9
Apple (on location services) https://perma.cc/YK3A-KU6E	9
Offerup and letgo Combine Marketplaces, https://perma.cc/S9NZ-T5NW	7
OfferUp Privacy Policy, https://perma.cc/KU4H-9BBL	8

INTRODUCTION AND STATEMENT OF AMICUS INTEREST

The Ohio Prosecuting Attorneys Association (OPAA) is a private, non-profit trade organization that supports Ohio's 88 elected prosecutors. Its mission includes assisting prosecuting attorneys in pursuit of truth and justice and advocating for public interest policies that promote public safety and help secure justice for victims.

Given these considerations, OPAA urges this Court to reject the proposition of law advanced by Diaw. A modern cellular phone can collect data about its user. Applications on a phone also store data about its user – often with the user's consent. One such application, Offer Up, was used in this case to facilitate the crime. Prosecutors across Ohio have a strong interest in a rule of law that correctly applies Fourth Amendment concerns.

This case is about an agreement that the victim made with "John Malick" to purchase an Apple MacBook laptop. "Malick" never intended to sell the victim a laptop. Instead, this was a scheme by Mamadou Diaw, facilitated through an internet service to rob the victim. The Court should affirm the judgment below because Diaw did not have an expectation of privacy in the single location data point that was collected as part of the customer records stored at Offer Up. *Carpenter v. United States*, 585 U.S. 296 (2018) does not extend to the location point here and because the third-party doctrine diminishes Diaw's expectation of privacy. In addition to the location point, other records revealed Diaw's identity which was confirmed through a photo array. The judgment below should be affirmed.

STATEMENT OF THE CASE AND FACTS

In February 2020, Kareem Wafa agreed to meet “John Malick” to buy a MacBook laptop. K.W. agreed to meet Malick in the Kroger’s parking lot on Groveport Road. The defendant Mamadou Diaw used the online marketplace Letgo to ultimately arrange the sham transaction and to lure Wafa to a Kroger parking lot, where he robbed them of an iPhone and \$360 cash. After assaulting the victim by punching them in the head and face, Diaw fled the scene.

The investigation began with only limited information: a description of the suspects, a red Honda Accord with tinted windows, partial license plate numbers, the username “John Malick” from Letgo, and a telephone number. Tr. 13-15. Law enforcement databases returned information on the Honda, and it was determined that the telephone number was serviced by Boost Mobile. Tr. 16-17.

Using an investigative subpoena, police obtained customer records from Letgo. The company produced records showing a single location point where “John Malick” identified as the “last_latitude.ios” and “last_longitude.ios.” This coordinate corresponded to a McDonald’s on East Broad Street - a public location. Tr. 21-26, State’s Ex. A-1.

Other investigative subpoenas were sent. The cell phone company indicated the subscriber was “John Malick” with an address in Colorado, but the detective determined that was a fake name. Tr. 26-27, State’s Ex. A-2. A subpoena was also sent to Google because the electronic mail associated with the Letgo account was a Gmail account. Tr. 31, State’s Ex. A-3. The subscriber of the Gmail account was Mamadou Diaw. *Id.* And the name “Mamadou Diaw” matched to a person in Ohio. Obtaining Diaw’s photograph, a photo array was prepared. Tr. 32. Wafa identified Diaw in the array. Tr. 32-33. An address associated with

Diaw was associated with an address behind the location point identified in the Letgo record. Tr. 26, 68. Additional investigative subpoenas were issued based on a “John Malick” positing additional items on separate platform at the time – OfferUp. Tr. 34, State’s Ex. A-6. The investigation followed this lead with additional subpoenas. State’s Ex. A-4, A-7.

Unlike the comprehensive cell phone tracking at issue in *Carpenter* which captured thousands of location points over months, here law enforcement obtained just one historical coordinate from Letgo. The defendant voluntarily disclosed this location data by choosing to use the Letgo platform - a completely optional service that is not an “inescapable” part of modern life like carrying a cell phone. He took no steps to prevent location tracking while using Letgo such as denying the service from accessing his location information.

The coordinate revealed only Diaw’s presence at a public fast-food restaurant. The Letgo record provided an email address which is not challenged here. There is also an IP address which is not challenged here. Another subpoena relating to the IP address provided a customer address corresponding with an apartment by the McDonald’s location. The trial court suppressed the evidence associated with the investigative subpoenas. and the State appealed resulting in reversal by the Tenth District in *State v. Diaw*, 2024-Ohio-2237(10th Dist).

The Court accepted the following proposition of law for review:

The United States Supreme Court’s holding in *Carpenter* and related cases holds that individuals maintain a privacy interest and attendant Fourth Amendment protections in the whole of their movements, including their physical location.

Amicus Curiae urges the Court to affirm the judgment below.

LAW AND ARGUMENT

PROPOSITION OF LAW (ACCEPTED FOR REVIEW): THE UNITED STATES SUPREME COURT'S HOLDING IN *CARPENTER* AND RELATED CASES HOLD THAT INDIVIDUALS MAINTAIN A PRIVACY INTEREST AND ATTENDANT FOURTH AMENDMENT PROTECTIONS IN THE WHOLE OF THEIR MOVEMENTS, INCLUDING THEIR PHYSICAL LOCATION.

Because the Court is constrained to decide the proposition of law accepted for review, the Court cannot and should not revisit the Tenth District's opinion as to non-location subscriber information associated with the investigative subpoenas issued in this case. This would include among other things, the electronic Gmail address associated with the Letgo records, see State's Ex. A-1 and the name associated with the Gmail address, see State's Ex. A-3 among other things. As to the proposition of law, this Court should distinguish between the type of location data collected in *Carpenter* and distinguish it from the single location point that was provided in the Letgo record. See State's Ex. A-1. Based upon the third-party doctrine, the Court should hold that *Carpenter* does not apply here. But because this case only implicates the single location point contained in the Letgo record, see State's Ex. A-1, no matter how the Court decides the proposition of law, the trial court's decision must be reversed given that the trial court was reversed as to other records that had been erroneously suppressed. And a remand to the trial court is appropriate under any circumstance.

I. The Ohio and United States Constitution

Normally, on appellate review a motion to suppress presents a mixed question of law and fact. While the determinations of fact must be supported if they are supported by competent, credible evidence, the appellate court must decide the legal questions without

deference to the trial court's decision. *State v. Banks-Harvey*, 2018-Ohio-201, ¶14 citing *State v. Burnside*, 2003-Ohio-5372, ¶8 and *State v. Fanning*, 1 Ohio St.3d 19, 20 (1982).

This case involves investigative subpoenas and through the proposition of law accepted review, whether Diaw has an expectation of privacy in the single location point under the Fourth Amendment of the United States Constitution. The Fourth Amendment to the United States Constitution states:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the places to be searched, and the persons to be seized.

Ohio's counterpart, Section 14, Article I of the Ohio Constitution has been treated as providing co-extensive protections as that provided under Fourth Amendment analysis. *See State v. Robinette*, 80 Ohio St.3d 234, 245 (1997). And for good reason. The text of Ohio's Constitution tracks the language of the Fourth Amendment.

The right of the people to be secure in their persons, houses, papers, and possessions, against unreasonable searches and seizures shall not be violated; and no warrant shall issue, but upon probable cause, supported by oath or affirmation, particularly describing the place to be searched and the person and things to be seized.

While the Ohio Constitution is a document of independent force, Diaw has advanced no textual or historical analysis to conclude that Ohio's Constitution is not co-extensive with the Fourth Amendment. Amicus recognizes that a limited exception as to minor misdemeanors was found by the Court in *State v. Brown*, 2003-Ohio-3931, but this case does not involve a minor misdemeanor. The Court should not extend *Brown* here and there is better reason to hold that Ohio's Constitution is co-extensive with the Fourth Amendment given the virtually

identical language used in both provisions and because Diaw frames his issue under *Carpenter*.

The Court has recognized that, “[t]he Fourth Amendment protects persons from unreasonable searches only to the extent that they have a reasonable expectation of privacy.” *Athens v. Wolf*, 38 Ohio St.2d 237, 240 (1974). See also *State v. LaRosa*, 2021-Ohio-4060 (holding that defendant did not have expectation of privacy in hospital washcloth used). Thus, the core question is whether Diaw had an expectation of privacy in the Letgo record at issue in this case.

II. Contrary to the Tenth District opinion the investigative subpoena was sufficient limited in scope and relevant

The Tenth District, although reversing the trial court’s judgment, commented that:

there were many missteps in the investigative phase of this case. While suppression of evidence is not permitted, law enforcement’s haphazard use of investigative subpoenas to collect Mr. Diaw’s personal information, while disclosed voluntarily, is the type of behavior that creates distrust in our legal system...Without remedial action, the state operates at its own peril by jeopardizing lawful investigation and risking further injury to the constitutional rights of Ohioans.

State v. Diaw, 2024-Ohio-2237, ¶66 (10th Dist).

Amicus Curiae disagrees. Here, the investigative subpoena was issued because of a reported crime. Crim. R. 17(C) permits a subpoena to command a person to produce the books or records and the rule applies to “[e]very subpoena.” A subpoena complies with the Fourth Amendment if it is “sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome.” *Donovan v. Lone Steer, Inc.*, 464 U.S. 408, 415 (1984), quoting *See v. City of Seattle*, 387 U.S. 541, 544 (1967). Here, the subpoena was sufficiently limited in scope as the language request records associated with associated with “John Malick” and the transaction related to the MacBook posting. See

State's Ex. A-1. In other words, the request for "any and all records" was sufficiently limited by the request for records associated with "John Malick." It was reasonable to make that request to identify "Malick" and to obtain additional information related to the MacBook posting, given that the posting was a ruse to lure Wafa to the location where he was robbed.

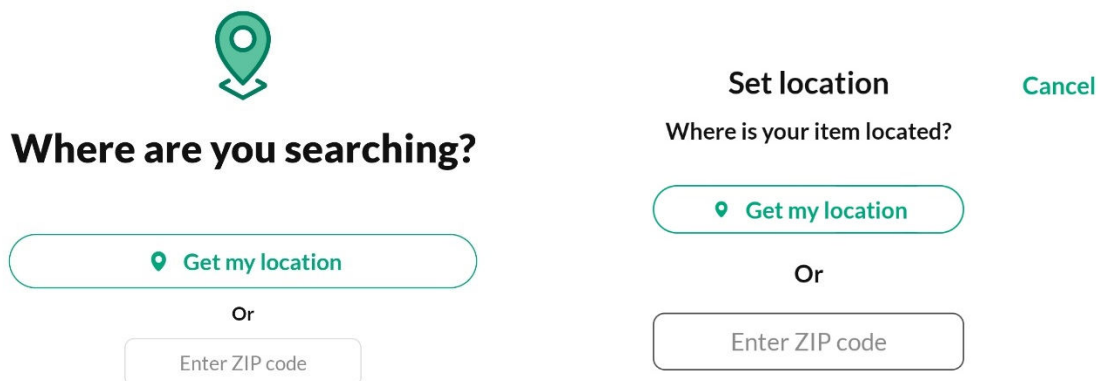
Obtaining records through a subpoena remain a valuable tool for investigative purposes when appropriate. And here there was no gross abuse of the subpoena power. But, in any event, the question before the Court is whether Diaw had an expectation of privacy in the single location point. He did not.

III. Diaw's location was tracked based on voluntary acts.

OfferUp (which acquired and merged with Letgo in 2020) is a mobile marketplace application that enables local buying and selling of goods between users¹. The application's location-sharing functionality operates on an explicit opt-in basis, requiring affirmative steps by users before their location data becomes accessible to other users or the platform. Within today's OfferUp application, the user has the option when searching for items or posting an item to either search based on one's location or by entering a zip code.

¹ The relevant records here pertain to Letgo which at the time operated separately from the OfferUp platform. See OfferUp and letgo combine marketplaces, post-acquisition, <https://perma.cc/S9NZ-T5NW> (captured February 18, 2025). Today, the letgo website appears to pertain to users outside of the United States.

Consider the fact that logging into today's OfferUp app gives the following prompts:



Where are you searching?

Get my location

Or

Enter ZIP code

Set location Cancel

Where is your item located?

Get my location

Or

Enter ZIP code

The Tenth District described, at the time of this offense, that Diaw affirmatively shared his location through the voluntary use of the Letgo app. *Diaw*, 2024-Ohio-2237, ¶62. The current Privacy Policy of OfferUp confirm that location data is shared upon a voluntary act of sharing. The privacy policy, available at <https://perma.cc/KU4H-9BBL> (last accessed February 18, 2025), states in part:

1. When you first download our mobile app or the first time you attempt to use any features that use location information, you will be asked to consent to our collection of this information. You may revoke your consent to our tracking location information at any time by changing your preferences in the settings menu on your mobile device or by following the standard uninstall process to remove our mobile application from your device.
2. Even if you do not consent to collect the precise location from your mobile device, we may use your IP address to infer an approximation of your location when using certain features of the OfferUp Services, such as the OfferUp payments solution.
3. In some features, OfferUp uses mapping services from Google Maps/Google Earth, including Google Maps API(s). Your use of these services is subject to Google's terms of service.

Thus, in its current form Offerup requires affirmative consent to share a user's location with the company. At the device level, both Apple and Android operating systems require a user

to provide an app permission to gain access to a person's location, noting that some applications may not work without having access to that location information. See Apple Location Services Information, available at <https://perma.cc/YK3A-KU6E> (captured February 18, 2025); Manage location permissions for apps (Android), available at <https://perma.cc/UAF3-K7K6> (captured February 18, 2025). And as the Tenth District concluded the location sharing here was a voluntary act by virtue of using the application. *State v. Diaw*, 2024-Ohio-2237, ¶61 (10th Dist.). The voluntary nature of sharing the location data as explained below is an important consideration in determining that Diaw did not have an expectation of privacy in the single location point that was captured when he utilized the Letgo service to facilitate the offense.

IV. Carpenter is inapplicable to a single point of location data obtained from an app.

As technology has advanced, courts have been forced to adapt to a rapidly changing landscape presenting new privacy concerns. A Fourth Amendment analysis is “informed by historical understandings of ‘what was deemed an unreasonable search and seizure when [the Fourth Amendment] was adopted.’” *Carpenter*, 585 U.S. at 305 quoting *Carroll v. United States*, 267 U. S. 132, 149 (1925). Among the central aims of the Framers was “to place obstacles in the way of a too permeating police surveillance.” *Id.* quoting *United States v. Di Re*, 332 U. S. 581, 595 (1948). Even in the face of advancing technology, the Supreme Court explained that it has “kept this attention to founding-era understandings in mind when applying the Fourth Amendment to innovations in surveillance tools.” *Id.*

In *Carpenter*, law enforcement had warrantlessly collected months of location data, leading the Court to reexamine a person's expectation of privacy in their physical location

and movements. It is apparent that the type of surveillance that the Court found troubling in *Carpenter* is much less sweeping than that claimed here. Indeed, the Court has approved even more invasive means of surveillance than a single data point. For example, the Court found no Fourth Amendment violation in surveillance conducted by way of a radio transmitter that police placed in a drum of chloroform purchased by the defendants in the case. *United States v. Knotts*, 460 U.S. 276, 277(1983). The Court explained that there was a lesser expectation of privacy in a vehicle because “its function is transportation and it seldom serves as one’s residence or as the repository of personal effects.” *Id.* at 281 quoting *Cardwell v. Lewis*, 417 U.S. 583, 590 (1974) (plurality opinion). Following the movements of a vehicle is of little concern because when the vehicle containing the radio transmitter traveled over public streets, the driver “voluntarily conveyed to anyone who wanted to look that he was traveling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.” *Id.* at 281-82.

Of course, the concern in *Carpenter* was more far-reaching. Rather than a transmitter broadcasting the details of a single trip on public roads, Timothy Carpenter’s cell-site location information included 12,898 location points over 127 days. *Carpenter* at 296. As the Court noted, cellular telephones “tap into the wireless network several times a minute, even if the owner is not using one of the phone’s features.” *Id.* at 300-01. Unlike a single car trip, “[m]apping a cell phone’s location over the course of 127 days provides an all-encompassing record of the holder’s whereabouts.” *Id.* at 311. This kind of surveillance “provides an intimate window into a person’s life, revealing not only his particular movements, but through them his ‘familial, political, professional, religious, and sexual

associations” *Id.* quoting *United States v. Jones*, 565 U.S. 400, 415 (2012). And given the ubiquity of cell phones, “when the Government tracks the location of a cell phone, it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone’s user.” *Id.* at 311-12. When considering the Supreme Court’s concerns about cell phone location data, it quickly becomes apparent that these concerns are inapplicable to a situation like Diaw’s. Indeed, the *Carpenter* Court explicitly stated that it did not “address other business records that might incidentally reveal location information[.]” *Id.* at 298. Nor does the *Carpenter* decision “call into question conventional surveillance techniques and tools, such as security cameras.” *Id.*

V. The *Carpenter* Court’s concerns are inapplicable to *Diaw*.

It is against this background that this Court must consider Diaw’s single data point. Diaw relies heavily on *Carpenter*, despite the Supreme Court specifically excluding the decision from situations like Diaw’s. Diaw complains of a “single latitude and longitude” that “corresponded with a McDonald’s located on East Broad Street” in Columbus. *Diaw*, 2024-Ohio-2237 at ¶ 8. Further investigation revealed that Diaw lived nearby. *Id.* According to the testimony in the case, the single coordinate “would track [the] last time [Mr. Diaw] logged into Letgo, and it would have hit his location he was at from there at the last time he logged into the site.” *Id.* at ¶ 14 quoting Tr. 75. In analyzing the disclosure of the single data point, the Tenth District focused on three factors: 1) the revealing nature of the data collected; 2) the amount of data collected; and 3) whether the suspect voluntarily disclosed their information to others. *Id.* at ¶ 53.

The GPS coordinate here was not revealing enough to implicate *Carpenter*'s privacy concerns. The coordinate placed Diaw at a McDonald's, indisputably a public place, near his home. This is certainly not the kind of "all-encompassing record of the holder's whereabouts" that concerned the Supreme Court. *Carpenter* at 311. The identification of Diaw's presence in a public place is more like the police radio transmitter in *Knotts*. While there is nothing to suggest that Diaw was driving a car, his presence in a public place nonetheless "voluntarily conveyed to anyone who wanted to look" that he was there. *Knotts* at 281. Even though the McDonald's was close to Diaw's home, nothing about the single location point revealed that information. Considered alone, it was hardly helpful to the investigation at all. For example, further investigation and additional subpoenas were necessary to determine that the McDonald's was close to Diaw's residence. *Diaw* at ¶

In his effort to bend *Carpenter* to suit his needs, Diaw relies on several decisions that are not helpful to him. *Snowden*, for example, dealt with real-time "pings" of cell phones; that is, the ability to locate a cell phone in real time using its cell site data. *State v. Snowden*, 2019-Ohio-3006, (2d Dist.), ¶28. The Second District acknowledged that the Supreme Court "has not addressed the narrow issue" presented in *Snowden*. *Id.* at ¶ 27. Undeterred, the Second District forged ahead with a brief *Carpenter*-based analysis, concluding that "the State's request for [cell site location information] was limited to a two-day period, there is no rationale that such a request is not a 'search'". *Id.* at ¶ 33. The Second District ultimately concluded that the warrantless search was supported by exigent circumstances and the good faith exception. *Id.* at ¶ 35. *Gause* presented the Second District with a similar set of circumstances, namely a "warrantless ping of his cellphone [*sic*] by the police prior to his arrest[.]" *State v. Gause*, 2022-Ohio-2168, ¶ 12 (2d Dist.). The pinging in this case amounted

to approximately two hours before Gause was located. *Id.* at ¶ 5. Applying *Snowden*, the Gause court concluded that the warrantless ping was necessary due to the exigent circumstances. *Id.* at ¶ 18-19.

Finally, in *Almonor*, the Supreme Court of Massachusetts was confronted with real time pings. *Commonwealth v. Almonor*, 482 Mass. 35, 36 (2019). Like the Second District, the court eventually concluded that the warrantless ping was supported by exigent circumstances. *Id.* at 52. Before reaching that conclusion, the *Almonor* court's analysis shed light on the difference between pinging a cell phone to determine its location and the incidental data point revealed in *Diaw*. Pinging a cell phone "effectively means that individuals are constantly, and often unknowingly, carrying a hidden tracking device that can be activated by law enforcement at any moment, subject only to the constraints of whether law enforcement knows the phone number[.]" *Id.* at 45. Real time pings are an "extraordinarily powerful surveillance tool" that "finds no analog in the traditional surveillance methods of law enforcement[.]" *Id.* The court was careful to distinguish pinging from historical data. Massachusetts courts permit law enforcement to obtain without a warrant up to six hours of "telephone call" cell site location information, which is retained by the service provider when the user voluntarily makes or receives a telephone call. *Id.* at 48-49.

VI. A single point of location data is more akin to capturing someone on surveillance footage or providing a subscriber address.

Surveillance cameras, capturing movements of people on public streets and in public locations, have become almost ubiquitous. At any given time, a person's presence in a public place, even close to traditionally private locations, may be captured on camera.

Diaw complains that his visit to a local McDonald's was captured by a single GPS location point disclosed to law enforcement. This single visit could have easily been captured on any number of surveillance cameras, imparting the same information as a single point of location data. *Carpenter's* concern was, of course, that cell site location data allows such precise tracking of a person that they may as well be wearing an ankle monitor. See *Carpenter* at 311. On the other hand, surveillance systems, even those located close to residences, capture people who happen to be in a particular place at a particular time. Their use has been routinely upheld.

Take for example a pole camera. A pole camera is not merely a security camera set up inside a public location such as McDonald's. Instead, it is set up by law enforcement in a public location, to monitor public movements of a suspect. The Eleventh Circuit recently dealt with this scenario in *United States v. Gregory*, __ F.4th __, 2025 U.S. App. LEXIS 3431 (Feb. 13, 2025). In *Gregory*, one of the appellants complained that a pole camera set up in the public street outside his house was an unconstitutional warrantless search. *Id.* at *18. The appellant argued that the camera invaded his reasonable expectation of privacy because it was focused on his home and recorded continuously. *Id.* The Eleventh District disagreed, noting that the camera could only view areas of the appellant's front yard and back yard that were visible from the street. *Id.* Compare *People v. Tafoya*, 494 P.3d 613 (Colo. 2021) (finding pole camera surveillance unconstitutional when the camera could view the target residence's backyard over a six-foot privacy fence). See also *United States v. Dennis*, 41 F.4th 732, 740-41 (5th Cir. 2022) (explaining that a pole camera was not a search because the camera captured what was open to public view from the street); *United States v. Hay*, 95 F.4th 1304 (10th Cir.2024) (same); *Commonwealth v. Mora*, 485 Mass. 360, (2020) (distinguishing

between long-term and short-term surveillance based on amount of information longer surveillance reveals). The *Gregory* court made one final distinction important here: surveillance cameras and GPS tracking are “meaningfully different forms of surveillance” because one is stationary and the other tracks every movement. *Id.* at *21. Based on these distinctions, *Carpenter*’s concerns about pervasive surveillance is not implicated by records revealing Diaw’s presence in a public place in the past.

VII. The third-party doctrine is inapplicable to location data voluntarily shared with an app.

As the *Diaw* court acknowledged, the Supreme Court of the United States has recognized the third-party doctrine as an exception to the Fourth Amendment’s warrant requirement. *Diaw*, 2024-Ohio-2237 at ¶ 34. In general, the third-party doctrine does not preclude the government from obtaining information voluntarily disclosed to a third party. *Id.* The doctrine “partly stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another.” *Carpenter* at 298. Also important is the nature of the information sought and the limitations on any legitimate expectation of privacy in the content of the information sought. *Id.* The second rationale supporting the third-party doctrine is the voluntariness of the exposure. *Id.* It is here that an important distinction can be drawn with the type of location data obtained with cell site location information. *Carpenter*’s concerns with the third-party doctrine are inapposite to *Diaw*. First, *Carpenter* acknowledged that cell site location data was far more extensive than “a person’s movement at a particular time.” *Carpenter* at 315. Next, it pointed out that the information was not subject to voluntary exposure in the same way that other information might be. Instead, a cell phone interacts with various cell sites as a standard part of its

operation, without any affirmative input from the user beyond powering up the device. *Id.* The associated location data is unavoidable. *Id.*

i. Carpenter presented a narrow exception to the third-party doctrine

In general, the third-party doctrine provides that “a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.” *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979). In other words, if information is voluntarily conveyed to a third party, like a business, the Fourth Amendment does not prohibit that third party from conveying the shared information to the government. *United States v. Miller*, 425 U.S. 435, 443 (1976). This is true even if the information was provided with the expectation that it would only be used for a limited purpose. *Id.* The third-party doctrine’s origins relate to bank records. In *Miller*, the challenge was to a subpoena for bank records, including bank statements, deposit slips, and canceled checks. *Id.* at 438. The Supreme Court rejected the challenge, finding that Miller could “assert neither ownership nor possession” of the bank’s records of his account. *Id.* at 440. In addition, the Court explained that the checks and statements were never intended to be confidential communications; rather, they were “exposed to [bank] employees in the ordinary course of business. *Id.* In essence, Miller had “take[n] the risk, in revealing his affairs to another, that the information [would] be conveyed by that person to the Government.” *Id.* at 443.

In a later case, the Supreme Court extended the third-party doctrine to “pen registers,” devices that record dialed telephone numbers. When a call is placed, the dialed number is “voluntarily conveyed” to the telephone company by “expos[ing] that information

to its equipment in the ordinary course of business. The Court explained that “even if petitioner did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is ‘not one that society is prepared to recognize as ‘reasonable’” *Id.* at 743 quoting *Katz v. United States*, 389 U.S. 347, 361 (1967). As technology has advanced, the third-party doctrine has had to evolve. Assuming the risk of a third-party’s exposure of information that has been voluntarily provided may be “ill-suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.” *United States v. Jones*, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

When the Court decided *Carpenter* six years later, it rejected the application of the third-party doctrine to the collection of cell site historical data. But the exception was a narrow one. It focused on the kind of data that is passively shared; that enables law enforcement reach back into the past to uncover detailed location tracking that exists because a user merely powered on a cell phone. *See Carpenter* at 298. The *Carpenter* Court expressly declined to overrule *Miller* and *Smith* and emphasized that it was not deciding anything related to similar technologies, including real-time cell phone pings, or retrieval of information from a single cell tower. *Id.* at 316. Since *Carpenter*, federal appellate courts have grappled with the Fourth Amendment’s application to cell phone apps like those that Diaw used to set up his victims. With Letgo and Offer Up, rather than a passive sharing, the user completes voluntary acts that result in any sharing of location data. This significant distinction removes Diaw from the concerns of *Carpenter* in the application of the third-party doctrine.

ii. *Apps like “Letgo” require users to consent to sharing location data.*

“Letgo” and “Offer Up” are not alone in the occasional recording of location data. Other apps record the same kind of data, and some of these have been considered by federal appellate courts. The First Circuit Court of Appeals found that the third-party doctrine applied to information gathered by subpoena from the electronic service provider “Kik,” including IP addresses used to access the app that, in turn, identified the user’s location. Indeed, the appellant complained that the IP address data collected concerned his internet activity on Kik and enabled investigators to determine his “precise location” when he logged on to Kik. *Id.* at 91. The First Circuit pointed out that, unlike the cell site location data in *Carpenter*, the IP address data acquired from Kik is generated “only by making the affirmative decision to access a website or application.” *Id.* at 92. The court found that this was a contrast to a cell phone, sitting untouched in a pocket or purse, “continually chronicling that user’s movements throughout the day.” *Id.* See also *United States v. Contreras*, 905 F.3d 853 (5th Cir.2018) (third party doctrine applied to address and IP information obtained from telecommunications company because the association of the IP address with the residence had “no bearing on any person’s day-to-day movement.”)

Even more extensive location data than is at issue here has been subject to the third-party doctrine. The Ninth Circuit Court of Appeals held that the third-party doctrine applied to location data collected from users of an app associated with the short-term rental of “e-scooters” in Los Angeles, California. *Sanchez v. Los Angeles Dept. of Transp.*, 39 F.4th 548 (9th Cir.2022). To obtain a permit to offer e-scooters for rent, the Los Angeles Department of Transportation required that e-scooter operators provide location data. *Id.* at 552. Operators of the e-scooters were required to have an app on their cell phones that assisted

in compiling real-time location data to track the e-scooter. *Id.* *Sanchez* was not a criminal case; rather, the plaintiff alleged in a civil rights action that location data collection violated, among other things, his Fourth Amendment rights. *Id.* at 553. The precision of the location data was such that the data could be used “in conjunction with other information to identify trips by individuals to sensitive locations.” *Id.*

The Ninth Circuit rejected Sanchez’s Fourth Amendment claim. Unlike the passive sharing that concerned the Supreme Court in *Carpenter*, an e-scooter user “must affirmatively cho[o]se to disclose location data to e-scooter operators each time he rent[s] a device.” *Sanchez* at 559. “[B]efore renting an e-scooter, [the user] must agree to the operator’s privacy policies.” *Id.* Thus, when a user rents an e-scooter, “he plainly understands that the e-scooter company must collect location data for the scooter through its smartphone applications.” *Id.* A reasonable expectation of privacy cannot be found where location data is voluntarily conveyed in the ordinary course of business. *Id.* Finally, the tracking at discrete locations, such as the beginning and end of scooter trips, “does not ‘pervasive[ly] track’ users over an extended period of time.” *Id.* at 560. Ultimately, the Ninth Circuit concluded that the Supreme Court’s concerns in *Carpenter* were inapplicable to the location data collected in the course of renting an e-scooter. *Id.* at 561.

Relying on *Carpenter*, Diaw presents this Court with a series of concerns that are inapplicable to him. The near-constant surveillance available through cell site data has no relationship to the single data point that was revealed pursuant to a subpoena. Diaw presents no argument to the contrary. He instead asks this Court for an unwarranted expansion of *Carpenter* to cover a single location point, data that Diaw voluntarily provided

to use an app. There is simply no comparison. As there is no relationship between Diaw's location point and *Carpenter's* pervasive surveillance, this Court should decline his invitation.

CONCLUSION

Based on the foregoing, Amicus Curiae asks the Court to affirm the Tenth District's judgment.

Respectfully Submitted,

Michael C. O'Malley
Cuyahoga County Prosecutor

/s/ Daniel T. Van
Daniel T. Van
Assistant Prosecuting Attorney
Counsel of Record
Kristen L. Hatcher
Assistant Prosecuting Attorney
1200 Ontario Street, 8th Floor
Cleveland, OH 44113
(216) 443-7865
dvan@prosecutor.cuyahogacounty.us

CERTIFICATE OF SERVICE

A copy of the foregoing has been sent on this 18th day of February, 2025 via electronic mail to the following: Adam Burke at burke142@gmail.com; Seth Gilbert at sgilbert@franklincountyohio.gov; and T. Elliot Gaiser at thomas.gaiser@ohioattorneygeneral.gov.

/s/ Daniel T. Van