In the
Supreme Court of Ohio

STATE OF OHIO.,	:	Case Nos. 2024-1083
	:	
Appellee,	:	On Appeal from the
	:	Franklin County
v.	:	Court of Appeals,
	:	Tenth Appellate District
MAMADOU DIAW,	:	
	:	Court of Appeals
Appellant.	:	Case No. 22AP-614

MERIT BRIEF OF *AMICUS CURIAE* OHIO ATTORNEY GENERAL DAVE YOST IN SUPPORT OF APPELLEE

ADAM G. BURKE (0083184)
625 City Park Avenue
Columbus, Ohio 43206
614.280.9122
burke142@gmail.com

Counsel for Appellant
Mamadou Diaw

G. GARY TYACK (0017254)
Prosecuting Attorney
SETH L. GILBERT (0072929)
Chief Counsel, Appeals Unit
373 South High Street–13th Fl.
Columbus, Ohio 43215
614.525.3555
sgilbert@franklincountyohio.gov

Counsel for Appellee
State of Ohio

DAVE YOST (0056290)
Attorney General of Ohio

T. ELLIOT GAISER* (0096145)
Solicitor General
**Counsel of Record*
ZACHERY P. KELLER (0086930)
Deputy Solicitor General
30 East Broad Street, 17th Floor
Columbus, Ohio 43215
614.466.8980
614.466.5087 fax
thomas.gaiser@ohioago.gov

Counsel for *Amicus Curiae*
Ohio Attorney General Dave Yost

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES iii

INTRODUCTION 1

STATEMENT OF *AMICUS* INTEREST 4

STATEMENT OF THE CASE AND FACTS 4

I. A pair of robbers used an online marketplace to advertise a fictitious sale; the robbers' online posting eventually traced back to Mamadou Diaw. 4

II. A grand jury indicted Diaw for robbery, but the trial court suppressed all evidence obtained from the investigative subpoenas. 7

III. The State appealed and the Tenth District reversed the trial court's suppression ruling. 8

IV. Diaw appealed to this Court presenting a single, narrow proposition. 10

ARGUMENT 11

Amicus Curiae Ohio Attorney General's Proposition of Law: 11

For purposes of the Fourth Amendment to the United States Constitution, when a person uses an online marketplace to advertise a sale, that person has no reasonable expectation of privacy in location data that the person voluntarily shares by using the marketplace. 11

I. The Fourth Amendment does not normally protect information that people share with others. 12

A. The Fourth Amendment protects people's reasonable expectations of privacy; but, under the third-party doctrine, people lack a reasonable expectation of privacy in information they voluntarily expose to others. 13

B. *Carpenter* carved out a narrow exception to the third-party doctrine. 17

II. Diaw lacked any reasonable expectation of privacy in isolated location data that he voluntarily exposed to an online marketplace. 23

A. Diaw's claim fails under the third-party doctrine and other standard Fourth Amendment principles. 23

B. Diaw's claim also fails under the *Carpenter* factors. 25

III. Diaw's contrary arguments are unpersuasive. 30

A. Diaw misunderstands Fourth Amendment precedent. 31

B. Diaw misapplies the *Carpenter* factors. 32

C. Diaw's remaining arguments are unconvincing. 34

CONCLUSION 37

CERTIFICATE OF SERVICE 38

TABLE OF AUTHORITIES

Cases **Page(s)**

Bosse v. Oklahoma,
580 U.S. 1 (2016).....31

Boyd v. United States,
116 U. S. 616 (1886).....13

Carpenter v. United States,
585 U.S. 296 (2018)..... *passim*

Commonwealth v. Almonor,
482 Mass. 35 (2019).....31, 32

Commonwealth v. Dunkins,
669 Pa. 456 (2021) 20

Davis v. United States,
564 U.S. 229 (2011).....36, 37

Donovan v. Lone Steer,
464 U.S. 408 (1984).....17, 35

Katz v. United States,
389 U.S. 347 (1967).....14, 15

Minnesota v. Carter,
525 U.S. 83 (1998).....14

Oklahoma Press Pub. Co. v. Walling,
327 U.S. 186 (1946).....16

Olmstead v. United States,
277 U.S. 438 (1928).....14

Powell v. United States,
2021 WL 4241273 (6th Cir. April 5, 2021).....20

Riley v. California,
573 U.S. 373 (2014).....13, 15, 16

Sanchez v. L.A. Dep't of Transp.,
39 F.4th 548 (9th Cir. 2022) 20, 21

See v. Seattle,
387 U.S. 541 (1967) 17

Smith v. Maryland,
442 U.S. 735 (1979) 2, 15, 16, 24

State v. Amos,
2016-Ohio-1319 (1st Dist.) 1

State v. Bourn,
2022-Ohio-4321 26

State v. Brown,
2024-Ohio-749 1

State v. Burroughs,
2022-Ohio-2146 32

State v. Campbell,
2022-Ohio-3626 ..... 8, 36

State v. Clayton,
2014-Ohio-2165 (9th Dist.) 1

State v. Clayton,
2015-Ohio-2499 (9th Dist.) 1

State v. Culver,
2014-Ohio-681 (9th Dist.) 1

State v. Dotson,
2017-Ohio-5565 (5th Dist.) 1

State v. Fox,
2015-Ohio-5523 (11th Dist.) 1

State v. Johnson,
2014-Ohio-5021 36

State v. Lee,
2017-Ohio-7377 (1st Dist.) 1

State v. Mosley,
2014-Ohio-2266 (8th Dist.) 1

State v. Thompson,
2015-Ohio-655 (10th Dist.) 1

United States v. Adkinson,
916 F.3d 605 (7th Cir. 2019) 21

United States v. Bledsoe,
630 F. Supp. 3d 1 (D.D.C. 2022) 20

United States v. Dewilfond,
54 F.4th 578 (8th Cir. 2022) 19

United States v. Hammond,
996 F.3d 374 (7th Cir. 2021) 20

United States v. Hansen,
599 U.S. 762 (2023) 17, 34

United States v. Hay,
95 F.4th 1304 (10th Cir. 2024) 19

United States v. Jones,
565 U.S. 400 (2012) 13, 15

United States v. Knotts,
460 U.S. 276 (1983) 15, 18, 24, 31

United States v. Lauria,
70 F.4th 106 (2d Cir. 2023) 19, 20

United States v. Miller,
425 U.S. 435 (1976) ..... *passim*

United States v. Morel,
922 F.3d 1 (1st Cir. 2019) 20

United States v. Rosenow,
50 F.4th 715 (9th Cir. 2022) 2, 20, 24

United States v. Soybel,
13 F.4th 584 (7th Cir. 2021) 20

United States v. Trader,
981 F.3d 961 (11th Cir. 2020) 20, 21

United States v. Wellbeloved-Stone,
777 F. App'x 605 (4th Cir. 2019) 20

United States v. Whipple,
92 F.4th 605 (6th Cir. 2024) 20

Utah v. Strieff,
579 U.S. 232 (2016) 12

Statutes and Constitutional Provisions

U.S. Const. amend. IV 11, 12, 16, 26

R.C. 109.02 4

R.C. 2935.23 ..... 5, 7, 35

R.C. 2935.53 ..... 8, 10

Other Authorities

10/30/2024 Case Announcements, 2024-Ohio-5173 10

Alex Baker, *3 arrested for armed robbery of online marketplace seller*, KRON 4
(July 26, 2024) 29

Control the location information you share on iPhone, iPhone User Guide 30

*Des Moines man arrested for alleged robbery during online marketplace
transaction*, KCCI (Dec. 24, 2024) 28

James Lynch, *Selling online? Expert recommends safety tips following Seattle
robbery*, Kiro Newsradio (July 3, 2024) 29

Kelly Kennedy, *Akron Police still searching for suspect in multiple Facebook Marketplace robberies*, 19 News (Sept. 10, 2024) 28

Las Vegas police urge caution with online marketplaces as scams rise, News 3 (Jan. 6, 2025) 28

Laura K. Donohue, *Functional Equivalence and Residual Rights Post-Carpenter: Framing a Test Consistent with Precedent and Original Meaning*, 2018 Sup. Ct. Rev. 347 (2018) 26

Manage location permissions for apps, Android Help 29

Matthew Tokson, *The Aftermath of Carpenter: An Empirical Study of Fourth Amendment Law, 2018-2021*, 135 Harv. L. Rev. 1790 (2022) 21

Nydia Han, *Safety and security warning for Facebook Marketplace users after recent Philly robberies*, ABC 6 (May 31, 2023) 29

Paul Ohm, *the Many Revolutions of Carpenter*, 32 Harv. J. L. & Tech. 357 (2019) 21

Privacy Policy, Craigslist (May 29, 2024) 30

Privacy Policy, OfferUp (Jan. 9, 2025) 30

Sarah Perez, *Online marketplace OfferUp raises $120M, acquires top competitor letgo*, TechCrunch (Mar. 25, 2020) 30

Sean Humphrey, *Hartford man sentenced to prison for gunpoint robberies targeting online sellers of luxury goods*, Fox 61 (Jan. 23, 2025) 28

INTRODUCTION

At their best, online marketplaces are useful public forums to help sellers and buyers connect. But such convenience comes with a downside. As this Court and others are aware, criminals often use online marketplaces to facilitate their crimes. *See, e.g.*, *State v. Brown*, 2024-Ohio-749, ¶¶1, 4; *State v. Lee*, 2017-Ohio-7377, ¶2 (1st Dist.); *State v. Dotson*, 2017-Ohio-5565, ¶¶2–5 (5th Dist.); *State v. Amos*, 2016-Ohio-1319, ¶4 (1st Dist.); *State v. Fox*, 2015-Ohio-5523, ¶1 (11th Dist.); *State v. Clayton*, 2015-Ohio-2499, ¶2 (9th Dist.); *State v. Thompson*, 2015-Ohio-655, ¶¶7–12 (10th Dist.); *State v. Mosley*, 2014-Ohio-2266, ¶3 (8th Dist.); *State v. Clayton*, 2014-Ohio-2165, ¶2 (9th Dist.); *State v. Culver*, 2014-Ohio-681, ¶¶37, 39 (9th Dist.); *see also below* at 28–29 (collecting recent news articles). One common scheme involves robbers using online marketplaces to advertise items for sale. The advertisement lures an interested buyer to a location, where the robbers proceed with the robbery.

This case involves that familiar scam. A pair of robbers created an account with an online marketplace—"Letgo"—publicly advertising that they had a computer for sale. The advertisement lured a buyer to a grocery-store parking lot, where he soon became a victim. In response to a subpoena, Letgo provided a detective with information that the purported seller shared by using the online marketplace. That information traced back to Mamadou Diaw. Most relevant to this case, Letgo provided the police with a single GPS location; a McDonald's that turned out to be near Diaw's address. From that and

other information, the detective surmised that Diaw used the wireless connection of the McDonald's to access his Letgo account.

Although this case involves a familiar-sounding crime, Diaw attempts a legal twist. He argues, under the Fourth Amendment to the U.S. Constitution, that he had a reasonable expectation of privacy in the location where he "entered" (that is, logged onto) the online marketplace. That argument fails under the third-party doctrine. The doctrine establishes that people lack a reasonable expectation of privacy in information they voluntarily share with others. *United States v. Miller*, 425 U.S. 435, 442 (1976). Applying the doctrine here, modern-day internet users realize that when they create and use online accounts, they share information with the relevant platform. *See United States v. Rosenow*, 50 F.4th 715, 737–38 (9th Cir. 2022); *cf. also Smith v. Maryland*, 442 U.S. 735, 742 (1979) (acknowledging that "telephone users realize" they convey private information to telephone companies). It follows that Diaw voluntarily exposed information to an online marketplace by creating an account and posting an item for sale.

Even setting aside the legalese, common sense leads to the same answer. There is nothing private about a marketplace. Rather, the point of a marketplace—whether online or elsewhere—is to facilitate open communication between sellers and buyers. And there is no natural reason for a seller to anticipate confidentiality from a marketplace. A seller using a traditional marketplace would not expect the marketplace to hide the location of

the seller's booth from police. Likewise, a seller using an online marketplace cannot reasonably expect secrecy from the platform.

To argue otherwise, Diaw leans heavily on *Carpenter v. United States*, 585 U.S. 296 (2018). But that case bears little resemblance to this one. *Carpenter* involved the government's broad requests to wireless carriers for cell-site-location information. *Id.* at 302. The disclosure of that information—involving *thousands* of location datapoints—allowed the government to catalogue a suspect's movements over a months-long stretch. *Id.* In a "narrow" decision, the Court held that the government's acquisition of cell-site-location information, in such a sweeping manner, implicated the Fourth Amendment. *Id.* at 316; *see also id.* at 310 n.3. The Court reasoned that the modern availability of such comprehensive location data did not destroy a person's "reasonable expectation of privacy in *the whole* of his physical movements." *Id.* at 313 (emphasis added). When unpacked, *Carpenter* stands for an unremarkable premise: people do not, by merely possessing a cell phone, give up all privacy expectations in their historic movements.

To say that Diaw prevails here because of *Carpenter*'s narrow decision makes no sense. This case does *not* focus on a request to a wireless carrier for historic cell-site-location information. Rather, the investigation here zoomed in on a suspect's discrete activities in an online marketplace. Diaw, in other words, did far more than passively possess a cell phone. He took full advantage of the online marketplace, actively advertising to the world that he had a computer for sale. He cannot now cry "privacy."

STATEMENT OF *AMICUS* INTEREST

The Attorney General is Ohio's chief law officer and "shall appear for the state in the trial and argument of all civil and criminal causes in the supreme court in which the state is directly or indirectly interested." R.C. 109.02. The State is interested in this case because it presents an important question regarding how police officers, consistent with constitutional protections, investigate crimes in the digital age.

STATEMENT OF THE CASE AND FACTS

I. A pair of robbers used an online marketplace to advertise a fictitious sale; the robbers' online posting eventually traced back to Mamadou Diaw.

Five years ago, Kareem Wafa tried to buy a MacBook laptop. *See State v. Diaw*, 2024-Ohio-2237, ¶3 (10th Dist.) ("App.Op."). To find a good deal, Wafa went onto a website called "Letgo," an online marketplace much like Craigslist. Supp. Hearing Tr. 12 (Feb. 24, 2022). Wafa eventually encountered a purported seller, going by the username "John Malick," who was advertising the laptop Wafa wanted. *Id.* at 13–14. Wafa agreed to complete the sale in a Kroger parking lot in Groveport, Ohio. *Id.* at 13. When Wafa arrived at the parking lot, he met with two individuals. *Id.* Wafa handed over cash and an iPhone in exchange for the laptop. App.Op. ¶4. But rather than giving Wafa the laptop, one of the individuals punched Wafa in the face. *See id.* The robbers then fled the scene. *Id.* at ¶4.

Detective Michael Sturgill, a Groveport police officer, investigated the crime. Based on Wafa's account of the events, Sturgill had five pieces of information to go on: (1) a

description of the robbers; (2) a Letgo username, "John Malick," and the posting for the computer sale; (3) a description of the robbers' car, a reddish Honda Accord; (4) the last four digits of that car's license plate; and (5) the telephone number that the robbers used to set up the false sale. *Id.* at ¶5; Supp. Hearing Tr. 13–15.

Armed with that information, Detective Sturgill went looking for more. Among other tactics, Sturgill utilized investigative subpoenas. App.Op. ¶6. Under Ohio law, police officers may request, and courts may issue, subpoenas to witnesses for information after "a felony has been committed" but "before any arrest has been made." R.C. 2935.23. Here, Sturgill requested—and the Franklin County Municipal Court issued—a subpoena to Letgo. App.Op. ¶6. The subpoena ordered a representative of Letgo to appear before that court and supply the following information:

> Please provide any and all records including all names, addresses, phone numbers, I.P. addresses and email addresses associated with the customer using the name of John Malick (possibly utilizing the phone number of 720-203-7022) and posting for sale a Mackbook [sic] Pro 2017 13 inch lap top computer for sale through Letgo posted in Columbus Ohio between the dates of 02-16-2020 through 02-18-2020.

Supp. Hearing State Ex. A-1. Alternatively, the subpoena noted that, rather than appearing in court, Letgo could provide the information directly to Sturgill. *Id.*

Letgo did not challenge this subpoena. *See* Supp. Hearing Tr. 17. It instead provided Detective Sturgill with an IP address, an email address, and a single latitude and longitude. App.Op. ¶8. Letgo did not explain this information, but Sturgill assumed that the latitude and longitude was GPS data associated with the John Malick account. *See*

Supp. Hearing Tr. 25–26. Sturgill drove to the location, which turned out to be a McDonald's in the local area. *Id.* But at that point—without more information—the location of the McDonald's was of little significance to Sturgill. *Id.* at 64.

The email address from Letgo proved a more valuable lead. Because the email address was a "gmail" account, Detective Sturgill subpoenaed Google for information about the account. App.Op. ¶10. The account belonged to Mamadou Diaw. *Id.* Sturgill searched that name in Ohio's Law Enforcement Gateway ("OHLEG") and obtained Diaw's driver's license photo. *Id.* That photo, Sturgill observed, matched Wafa's description of one of the robbers. *Id.* Sturgill thus created a photo lineup, which another detective (unfamiliar with the suspect) presented to Wafa. *Id.*; Supp. Hearing Tr. 32–33. From the lineup, Wafa immediately identified Diaw as one of the robbers—the one who punched him in the face. *See* Supp. Hearing Tr. 33; App.Op. ¶4.

The discovery of Diaw's driver's license yielded other information as well. It revealed (1) Diaw's address and (2) a Honda Accord registered in Diaw's name. App.Op. ¶10; *see* Supp. Hearing Tr. 26. As it turned out, the address was a stone's throw away from the McDonald's that Detective Sturgill had visited earlier, when following up on the GPS location he received from Letgo. Supp. Hearing Tr. 26. That suggested, at least to Sturgill, that Diaw used the McDonald's wireless connection to log into Letgo. *Id.* at 64, 74.

Amid his investigation, Detective Sturgill received a call from Wafa. *Id.* at 34. Wafa informed the detective that "John Malick" was posting again—this time on "OfferUp."

Id. Based on this information, Sturgill requested additional subpoenas, which eventually led Sturgill to a new "Cedar Drive" address. App.Op. ¶11. Sturgill was already aware of Diaw by that point, but he investigated the new address anyway. Supp. Hearing Tr. 39. When Sturgill went to the address, he saw a Honda Accord parked at the residence; the license plate of the car matched the partial place Wafa had initially provided. *Id.*

One further aspect of Detective Sturgill's investigation warrants quick mention. Sturgill eventally obtained a search warrant, which he sent to a telecommunications company (Sprint). App.Op. ¶12. The warrant sought GPS and location data—over an eighteen-day period—for the phone number Wafa had reported. Supp. Hearing State Ex. A-8. Sprint never responded to the warrant. App.Op. ¶12.

II. A grand jury indicted Diaw for robbery, but the trial court suppressed all evidence obtained from the investigative subpoenas.

A grand jury indicted Diaw for multiple robbery offenses. App.Op. ¶2. Diaw moved to suppress the evidence against him, challenging Officer Sturgill's use of subpoenas in his case. Mot. to Dismiss/Suppress Evidence (Jun. 14, 2021), Trial R.26. Diaw argued that the subpoenas violated his Fourth Amendment rights because he had a privacy interest in his "online accounts and the data included therein." *Id.* at 4.

The trial court held a suppression hearing, at which Detective Sturgill recounted the just-discussed investigation. After the hearing, the trial court granted Diaw's motion to suppress. Decision & Entry (Oct. 3, 2022), Trial R.81. Initially, the court concluded that the subpoenas in this case failed to comply with R.C. 2935.23, which presumes that

subpoenaed witnesses will give information through sworn testimony in court. *Id.* at 3–4. In the trial court's view, this perceived statutory violation was a basis for suppressing "any information derived from the investigative subpoenas." *Id.* at 4.

The court next addressed the Fourth Amendment. On that front, the court held that the subpoenas were "too sweeping." *Id.* at 5. The court found it inappropriate for a subpoena to seek "'any and all record' pertaining to a customer with certain identifying information." *Id.* at 4.

III. The State appealed and the Tenth District reversed the trial court's suppression ruling.

The State appealed, and the Tenth District reversed. The Tenth District first held that the trial court erred in relying on a statutory violation to exclude evidence. App.Op. ¶¶23–24. The exclusionary rule, the Tenth District explained, "is generally reserved for violations of a constitutional nature." *Id.* at ¶23 (citing *State v. Campbell*, 2022-Ohio-3626, ¶22). Thus, any failure of the subpoenas to conform with R.C. 2935.53 was not a proper basis for suppressing evidence. *Id.* at ¶24.

As for the Fourth Amendment, the Tenth District found no constitutional violation. *Id.* at ¶63. It recognized that the Fourth Amendment does not typically empower a defendant to challenge a third party's choice to turn over records in response to a subpoena. *Id.* at ¶26. It further recognized that the Fourth Amendment does not generally bar the "the government from obtaining information voluntarily provided to a third party." *Id.* at ¶34. Rather, the Fourth Amendment applies only when an individual

retains a legitimate expectation of privacy in the information. *Id.* at ¶32. The key question thus became whether Diaw "had a reasonable expectation of privacy over the information obtained through the Letgo investigative subpoena." *Id.*

To answer that question, the Tenth District divided the disclosed information into three categories: (1) subscriber information, (2) internet protocol ("IP") addresses, and (3) "a single latitude and longitude data point." *Id.* at ¶36. The Tenth District concluded that Diaw did not have a legitimate expectation of privacy in subscriber information, including the email address he used to create a Letgo account. *Id.* at ¶¶37–40. Because that information "was voluntarily conveyed to" Letgo, Diaw assumed the risk of Letgo "disclosing that information to law enforcement." *Id.* at ¶40.

The Tenth District reached the same conclusion for Diaw's IP address. *Id.* at ¶¶41–44. By way of background, an IP address is a string of numbers unique to a device that connects to the internet. *Id.* at ¶41. The Tenth District concluded—relying on "overwhelming[]" authority from other courts—that internet users have no reasonable expectation of privacy in IP addresses. *Id.* at ¶44. The court reasoned that internet users are aware, or at least should be aware, that this information is provided to internet service providers. *Id.* at ¶42.

Finally, the Court likewise concluded that Diaw did not have a "reasonable expectation of privacy over the single coordinate" of location data that Letgo disclosed. *Id.* at ¶63. To reach this last conclusion, the Tenth District considering a variety of factors,

which it drew from the U.S. Supreme Court's analysis in *Carpenter* about cell-site-location information. App.Op. ¶¶54–63. The Tenth District stressed that a "latitude and longitude data point" tracking Diaw's "single movement in a public space" was not overly revealing in nature. *Id.* at ¶58. The court further emphasized that this case was "a far cry from" *Carpenter* in terms of the amount of data the police obtained. *Id.* at ¶60. And in this case, the court went on, Diaw "voluntarily conveyed" his location information through the "affirmative" use of an online marketplace. *Id.* at ¶61.

IV. Diaw appealed to this Court presenting a single, narrow proposition.

Diaw appealed to this Court. But he left many aspects of the Tenth District's decision unchallenged. Diaw did not raise any proposition regarding the suppression of evidence under R.C. 2935.53. *See* App.Op. ¶23. Nor did he challenge the Tenth District's privacy-expectation determinations regarding subscriber information or IP addresses. *See id.* at ¶¶37–44. Instead, Diaw presented only a single proposition of law concerning how the U.S. Supreme Court's decision in *Carpenter* applies to "cases involving limited location data." Diaw Jur. Memo. 3 (July 29, 2024). This Court accepted Diaw's proposition for review. *10/30/2024 Case Announcements*, 2024-Ohio-5173.

ARGUMENT

Amicus Curiae Ohio Attorney General's Proposition of Law:

> *For purposes of the Fourth Amendment to the United States Constitution, when a person uses an online marketplace to advertise a sale, that person has no reasonable expectation of privacy in location data that the person voluntarily shares by using the marketplace.*

The Fourth Amendment, which applies to the States through the Fourteenth 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. Historically, that protection focused on "common-law trespass" and barred the government from "physically intruding on a constitutionally protected area." *Carpenter*, 585 U.S. at 304 (quotation omitted). The U.S. Supreme Court has since "expanded" its "conception of the Amendment to protect certain expectations of privacy as well." *Id.* But the Court has set key limits on which expectations of privacy are reasonable. Most significant here, the third-party doctrine says that people have *no* legitimate expectation of privacy in information that they voluntarily share with others. *Id.* at 307–08. To add a final wrinkle, in *Carpenter*, the Court carved out a limited exception to the third-party doctrine for historic cell-site-location information. *Id.* at 314–15; *see below* at 17–18 (discussing the unique nature of cell-site-location information).

Against these layers of precedent, this case asks if a user of an online marketplace has a reasonable privacy expectation in isolated location data that the user shares with the

marketplace by logging in. The answer is "no," under both general Fourth Amendment principles and *Carpenter*'s more context-specific analysis.

But before diving into the merits, the Attorney General pauses to emphasize this point: Diaw can hope for only a narrow remedy in this case. The exclusionary rule that attaches to Fourth Amendment violations is a rule of "last resort" that imposes "substantial societal costs." *Utah v. Strieff*, 579 U.S. 232, 237–38 (2016) (quotation omitted). The rule does not justify suppressing evidence that police officers discovered, or would have discovered, through lawful means. *See id.* at 238. That matters here because Diaw's current argument zooms in on "a single data point of GPS coordinate data." *See* Diaw Br. 10. By contrast, Diaw presents *no* legal challenge about the disclosure of his email address. *See* App.Op. ¶¶37–40. And that email was what cracked the case for the State. *Above* at 6. As a result, this appeal provides no grounds for "reinstat[ing] the trial court's order," *contra* Diaw Br. 16, which would have suppressed *all* the subpoenaed evidence. *See* Decision & Entry 3–4 (Oct. 3, 2022), Trial R.81. Instead, a win for Diaw would at most mean excluding ancillary evidence about the McDonald's near Diaw's residence.

I. The Fourth Amendment does not normally protect information that people share with others.

Turn, then, to the merits. Again, 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. In *Carpenter*, the U.S. Supreme Court concluded that those words protect against the government tracking people's historic

movements through broad requests (to wireless carriers) for cell-site-location information. *See* 585 U.S. at 302, 313, 316. But to understand *Carpenter*—and its limits—one must understand how Fourth Amendment doctrine has developed over the years. The Attorney General starts with that development and then addresses *Carpenter*.

A. The Fourth Amendment protects people's reasonable expectations of privacy; but, under the third-party doctrine, people lack a reasonable expectation of privacy in information they voluntarily expose to others.

1. *Trespass conception.* Begin at the start. The founding generation crafted the Fourth Amendment in response to the "general warrants" and "writs of assistance" of the colonial era. *Riley v. California*, 573 U.S. 373, 403 (2014). Those "reviled" practices "allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity." *Id.* "Opposition to such searches was in fact one of the driving forces behind the Revolution itself." *Id.*; *see also Boyd v. United States*, 116 U. S. 616, 625 (1886).

Consistent with those origins, "Fourth Amendment jurisprudence was tied to common-law trespass" for much of this country's history. *United States v. Jones*, 565 U.S. 400, 405 (2012). This "trespass" conception generally prevented the government from obtaining "information by physically intruding on a constitutionally protected area." *Id.* at 406 n.3. But if the government could obtain information without physically intruding on protected areas, there was no constitutional problem. In the 1920s, for example, the U.S. Supreme Court concluded that the Fourth Amendment did *not* prevent law

enforcement from wiretapping public telephones. *Olmstead v. United States*, 277 U.S. 438, 466 (1928). Because such wiretapping involved "no entry of the houses or offices of the defendants," no warrant was needed. *Id.* at 464.

2. Expectations of privacy. Over time, the U.S. Supreme Court expanded its conception of the Fourth Amendment. *Carpenter*, 585 U.S. at 304. Starting in the 1960s, the Court began stressing that "the Fourth Amendment protects people, not places." *Katz v. United States*, 389 U.S. 347, 351 (1967). From that notion, the Court eventually established that the Fourth Amendment applies when a person "seeks to preserve something as private" and the person's "expectation of privacy is one that society is prepared to recognize as reasonable." *Carpenter*, 585 U.S. at 304 (quotation omitted); *accord Katz*, 389 U.S. at 361 (Harlan, J., concurring). This conception of the Fourth Amendment is admittedly "fuzzy." *See Minnesota v. Carter*, 525 U.S. 83, 91 (1998) (Scalia, J., concurring). It empowers judges to discern (and then constitutionalize) the expectations of privacy that society is prepared to accept. *See id.* at 97. But, whatever its drawbacks, this "expectations of privacy" conception remains a part of the current Fourth Amendment landscape. *See Carpenter*, 585 U.S. at 304–05.

In practice, deciding which privacy expectations are reasonable is often a matter of degree. Take, for instance, people's expectations about their physical movements. The U.S. Supreme Court has held that a person traveling "from one place to another" on "public thoroughfares has no reasonable expectation of privacy in his movements."

United States v. Knotts, 460 U.S. 276, 281 (1983). But the Court has since signaled that, unlike surveillance of "discrete" movements, the government's long-term surveillance of a person's historic movements can raise legitimate "privacy concerns." *Carpenter*, 585 U.S. at 306–07 (quotation omitted, citing concurrences from *Jones*, 565 U.S. 400).

Decisions about phones have also produced mixed results. The U.S. Supreme Court has concluded that people do not have a legitimate expectation of privacy in the telephone numbers they dial. *Smith*, 442 U.S. at 742. Telephone users, the Court reasoned in *Smith*, "realize that they must 'convey'" information to the telephone company so "that their calls are completed." *Id.* By contrast, police officers must obtain warrants to search the contents of cell phones that they confiscate during arrests. *Riley*, 573 U.S. at 403. That flows from the reality that cell phones store a great deal of personal information and have become "a pervasive and insistent part of daily life." *Id.* at 385.

3. The third-party doctrine. While expectations of privacy are fuzzy in many respects, the third-party doctrine offers one firm boundary. The doctrine teaches that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Carpenter*, 585 U.S. at 308 (quoting *Smith*, 442 U.S. at 520). The doctrine has roots in *Katz*, which stressed, "What a person knowingly exposes to the public … is not a subject of Fourth Amendment protection." 389 U.S. at 351. The Court later elaborated that when a person "reveal[s] his affairs to another," that person necessarily "takes the risk … that the information will be conveyed by that person to the Government." *Miller*,

425 U.S. at 443. The third-party doctrine thus "draw[s] a line between what a person keeps to himself and what he shares with others." *Carpenter*, 585 U.S. at 307–08. That line leaves the government "typically free to obtain [the shared] information from the recipient without triggering Fourth Amendment protections." *Id.* at 308.

Importantly, the third-party doctrine applies even when potentially sensitive information is at stake. *Smith* held that when people "voluntarily convey[] numerical information to the telephone company"—by calling someone's number from their home phones—they lose any privacy expectation in that information. 442 U.S. at 744. *Miller* likewise held that people have "no legitimate 'expectation of privacy'" in financial information that they "voluntarily convey[]" to banks. 425 U.S. at 442.

4. Subpoenas. Subpoenas are a final aspect of the Fourth Amendment equation. The founding generation was quite familiar with the practice of subpoenaing information and evidence from witnesses. *See Carpenter*, 585 U.S. at 363–68 (Alito, J., dissenting). Subpoenas, however, did not pose the same concerns as general warrants and writs of assistance. After all, subpoenas rely on the subpoenaed party to produce information; they do not invite the government "to rummage" through one's home or things. *See Riley*, 573 U.S. at 403; *accord Oklahoma Press Pub. Co. v. Walling*, 327 U.S. 186, 195 (1946). A subpoena, moreover, allows for the "opportunity to present objections." *Oklahoma Press*, 327 U.S. at 195. Such differences are likely why the Fourth Amendment does not directly address subpoenas or compulsory process. *See* U.S. Const. amend. IV.

To be sure, at their outer boundaries, subpoenas sometimes implicate the Fourth Amendment. But, generally speaking, subpoenas pose no constitutional problem if they are "sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome." *Donovan v. Lone Steer*, 464 U.S. 408, 415 (1984) (quoting *See v. Seattle*, 387 U.S. 541, 544 (1967)). Noticeably, the just-stated test focuses on the rights of—and burdens to—a *subpoenaed party*, not a criminal defendant. That matches "the general rule that the issuance of a subpoena to a third party to obtain the records of that party does not violate the rights of a defendant." *Miller*, 425 U.S. at 444; *accord United States v. Hansen*, 599 U.S. 762, 769 (2023) ("[L]itigants typically lack standing to assert the constitutional rights of third parties.").

B. *Carpenter* carved out a narrow exception to the third-party doctrine.

1. Carpenter. The above principles set the stage for *Carpenter*. The question presented there was whether the government's acquisition of broad cell-site-location information from wireless carriers invaded a suspect's reasonable expectation of privacy. In an explicitly "narrow" decision, the Court held that it did. *Carpenter*, 585 U.S. at 316.

To understand *Carpenter*, one must first understand cell-site-location information. (*Carpenter* refers to cell-site-location information as "CSLI." For ease of reading, this brief resists the acronym.) "Cell phones continuously scan their environment looking for the best signal, which generally comes from the closest cell site." *Id.* at 300. As a result, cell phones "tap into the wireless network several times a minute." *Id.* Each connection

between a cell phone and a cell site generates location information—information that has become "increasingly precise" over the years. *Id.* at 301–02. Cell phones generate this cell-site-location information "whenever their signal is on," regardless of whether the owner is actively "using one of the phone's features." *Id* at 300–01. In *Carpenter*, the government made broad requests to wireless carriers for a suspect's cell-site-location information. *Id.* at 302. From those requests, the government obtained roughly 13,000 location points, spanning about three months. *Id.* at 302. That allowed the government to "catalog[ue]" the suspect's long-term movements. *Id.*

Carpenter held that the government's acquisition of such a broad universe of cell-site-location information implicated the Fourth Amendment. *Id.* The Court specifically determined that a person possesses a "reasonable expectation of privacy *in the whole* of his physical movements." *Id.* at 313 (emphasis added). That distinguished *Carpenter* from the Court's earlier decision in *Knotts*, which held that a person has no reasonable expectation of privacy in a *discrete* journey. *See id.* at 306; *Knotts*, 460 U.S. at 281. For wholistic movements, *Carpenter* reasoned, the third-party doctrine was inapplicable, even though third parties (wireless carriers) gather and store cell-site-location information. *See Carpenter*, 585 U.S. at 301, 314–15, 320.

The Court, however, kept *Carpenter* "narrow." *Id.* at 316. It resisted announcing any new "rubric" for privacy expectations in the digital age. *See id.* at 304. The Court similarly avoided deciding any "matters not before" it. *Id.* at 316. The decision thus left existing

doctrines largely (if not wholly) intact. The third-party doctrine, the Court said, would still leave the government "typically free to obtain such information from the recipient without triggering Fourth Amendment protections." *Id.* at 308; *see also id.* at 316. And the government, the Court went on, would still "be able to use subpoenas to acquire records in the overwhelming majority of investigations." *Id.* at 319. It would only be the "rare case," the Court promised, where a suspect would have "a legitimate privacy interest in records held by a third party." *Id.*

Indeed, *Carpenter* even avoided setting a definitive rule for cell-site-location information. The Court limited its holding to requests for cell-site-location information that spanned seven or more days. It left undecided whether there was a more "limited period for which the Government may obtain an individual's historical [cell-site-location information] free from Fourth Amendment scrutiny." *Id.* at 310 n.3. Similarly, the Court left open whether the government could obtain "real-time" cell-site-location information without a warrant. *Id.* at 316.

2. Post-Carpenter cases. Since *Carpenter*, lower courts have generally respected the decision's strict confines. *See, e.g.*, *United States v. Hay*, 95 F.4th 1304, 1316 (10th Cir. 2024); *United States v. Lauria*, 70 F.4th 106, 129 n.12 (2d Cir. 2023); *United States v. Dewilfond*, 54 F.4th 578, 581 (8th Cir. 2022) (*per curiam*). The U.S. Court of Appeals for the Eleventh Circuit, for instance, has described Carpenter as a "narrow exception" to the third-party doctrine, which "applies only to some" scenarios involving cell-site-location information.

United States v. Trader, 981 F.3d 961, 968–69 (11th Cir. 2020) (quotation omitted); *accord Powell v. United States*, 2021 WL 4241273, at *3 (6th Cir. April 5, 2021) (Donald, J., order). The U.S. Court of Appeals for the First Circuit has similarly explained that *Carpenter* did not "effect[] a sea change in the law of reasonable expectation of privacy." *United States v. Morel*, 922 F.3d 1, 8 (1st Cir. 2019).

Lower courts have thus continued to apply the third-party doctrine to digital information. Many circuits have held that the doctrine applies to information that internet users voluntarily share with online platforms, such as IP addresses and subscriber information. *See, e.g. Trader*, 981 F.3d at 967–69; *Rosenow*, 50 F.4th at 737–38; *United States v. Soybel*, 13 F.4th 584, 592 (7th Cir. 2021); *Morel*, 922 F.3d at 9–11; *United States v. Wellbeloved-Stone*, 777 F. App'x 605, 607 (4th Cir. 2019) (*per curiam*); *cf. also Commonwealth v. Dunkins*, 669 Pa. 456, 469–70 (2021) (holding that a person voluntarily logging into a college's wireless network had no privacy expectations in "connection records"). The Sixth Circuit, for example, recently applied the doctrine to information "voluntarily disclosed" via a "Walmart-Pay" application. *United States v. Whipple*, 92 F.4th 605, 612 (6th Cir. 2024).

Various courts have also held or suggested that the government may request discrete location data from third parties without implicating the Fourth Amendment. *See, e.g.*, *Lauria*, 70 F.4th at 129 n.12; *Sanchez v. L.A. Dep't of Transp.*, 39 F.4th 548, 559–61 (9th Cir. 2022); *United States v. Hammond*, 996 F.3d 374, 389–90 (7th Cir. 2021); *United States v.*

Bledsoe, 630 F. Supp. 3d 1, 12–17 (D.D.C. 2022); *United States v. Adkinson*, 916 F.3d 605, 611 (7th Cir. 2019) (*per curiam*). In *Sanchez*, for example, the Ninth Circuit held that the third-party doctrine applied to location data associated with an e-scooter account. 39 F.4th at 561. The Seventh Circuit has likewise concluded that *Carpenter* does not "invalidate warrantless tower dump," where the government seeks to identify all phones "near one location … at one time." *Adkinson*, 916 F.3d at 611 (emphases omitted).

3. The Carpenter factors. Given its narrow nature, *Carpenter* has little if any application to cases that do not involve requests to wireless carriers for historic cell-site-location information. *See Trader*, 981 F.3d at 967. But, on the chance the Court disagrees, it is worth saying just a bit more about *Carpenter*'s internal logic.

Though *Carpenter* resisted any "rubric," 585 U.S. at 304, its analysis of cell-site-location information breaks into multiple factors. *See, e.g.*, Matthew Tokson, *The Aftermath of Carpenter: An Empirical Study of Fourth Amendment Law, 2018–2021*, 135 Harv. L. Rev. 1790, 1800–04 (2022); Paul Ohm, *the Many Revolutions of Carpenter*, 32 Harv. J. L. & Tech. 357, 361 (2019); *cf. Carpenter*, 585 U.S. at 340 (Kennedy, J., dissenting) (criticizing the majority's "multifactor analysis"). Four factors stand out.

First, *Carpenter* considered history. The Court made express that "historical understandings" of the Fourth Amendment inform "which expectations of privacy are entitled to protection." 585 U.S. at 304–05. It further suggested that allowing the government to easily obtain extensive cell-site-location information conflicted with the

founding generation's "central aim" of blocking "permeating police surveillance." *Id.* at 305 (quotation omitted); *see also id.* at 320 ("[T]his tool risks Government encroachment of the sort the Framers … drafted the Fourth Amendment to prevent.").

Second, *Carpenter* noted the "deeply revealing nature of" historic cell-site-location information. *Id.* Such information, the Court emphasized, revealed more than a person's "movement at a particular time" or that a person was "using a phone." *Id.* at 315. Rather, historic cell-site information allowed for "a detailed chronicle of a person's physical presence compiled every day, every moment, over several years." *Id.*

Third, *Carpenter* focused on the amount of information at stake—the "depth, breadth, and comprehensive reach" of cell-site-location information. *Id.* at 320. The government in *Carpenter* was able to gather thousands of location points spanning over a hundred days. *Id.* at 302. That amount of data was readily available to the government because of how wireless carriers "collect and store" cell-site-location information "for their business purposes." *Id.* at 301.

Fourth, *Carpenter* questioned whether cell-site-location information was truly a product of "voluntary exposure" to third parties. *Id.* at 315. The Court emphasized that "carrying" a cell phone has become "indispensable to participation in modern society." *Id.* at 315. It followed, the Court continued, that one does not "voluntarily" assume the risk of pervasive tracking merely by possessing a cell phone. *Id.* In other words, carrying

a cell phone has become largely "inescapable," making wireless carriers' "collection" of cell-site-location information "automatic" rather than "voluntary." *Id.* at 315, 320.

II. Diaw lacked any reasonable expectation of privacy in isolated location data that he voluntarily exposed to an online marketplace.

Now apply the above principles to this case. To that end, recall the basic facts. Detective Sturgill subpoenaed an online marketplace—Letgo—seeking information about a specific user's computer-sale postings during a three-day period. Supp. Hearing State Ex. A-1; App.Op. ¶6. Letgo responded with a few pieces of information, including a single GPS datapoint. App.Op. ¶8. Sturgill eventually linked that location datapoint to a McDonald's near Diaw's address. *Id.*

The question is whether Diaw had a reasonable expectation of privacy in that isolated piece of location data. The answer is "no, he did not." And that answer holds true regardless of whether the Court analyzes this case under normal Fourth Amendment principles or through the lens of *Carpenter*'s special factors.

A. Diaw's claim fails under the third-party doctrine and other standard Fourth Amendment principles.

Taking *Carpenter* at its words, that "narrow" decision did "not express a view on" the much different circumstances here. *See* 585 U.S. at 316. This case does not involve broad requests to wireless carriers for a suspect's historic cell-site-location information. *See id.* at 301–02. It instead involves a single request to an online marketplace for three days' worth of records related to a specific computer-sale posting. App.Op. ¶6. The Court

should therefore decide this case using normal Fourth Amendment rules. Under those rules, Diaw's privacy-expectation argument fails for several interrelated reasons.

Consider first the third-party doctrine. In the late 1970s, telephone users realized that, in dialing someone's phone number, "they must 'convey'" information to the telephone companies so that "their calls are completed." *Smith*, 442 U.S. at 742. Similarly today, internet users know that they provide information—including location data—when they create accounts for and log into online platforms. *See Rosenow*, 50 F.4th at 738; *below* at 29–30 (discussing online applications in greater detail). In this case, by creating an account with an online marketplace and advertising a sale, Diaw voluntarily shared information with the online marketplace. He thus assumed the risk that the marketplace might share that information with law enforcement. It follows that Diaw had no legitimate expectation of privacy in the shared information. *See Miller*, 425 U.S. at 442–43.

The U.S. Supreme Court's decision in *Knotts* points in the same direction. There, the Court held a suspect had no expectation of privacy when, using public streets, he took a discrete "automotive journey" from Minneapolis, Minnesota to Shell Lake, Wisconsin (about a two-hour drive). *Knotts*, 460 U.S. at 277, 281, 285; *accord Carpenter*, 585 U.S. at 306. Comparatively speaking, it is hard to fathom how Diaw could have a legitimate expectation of privacy in single GPS datapoint revealing a local McDonald's.

Remember, also, that the GPS datapoint resulted from a subpoena seeking an online marketplace's records, *not* Diaw's records. In the "overwhelming majority of investigations," law enforcement can "use subpoenas to acquire" such records. *Carpenter*, 585 U.S. at 319. Here, Diaw identifies nothing—concerning his relationship with Letgo—that makes this the "rare case" where a defendant somehow retained "a legitimate privacy interest in records held by a third party." *See id.* Rather, Diaw's case fits neatly within "the general rule that the issuance of a subpoena to a third party to obtain the records of that party" has no effect on the Fourth Amendment rights "of a defendant." *See Miller*, 425 U.S. at 444.

B. Diaw's claim also fails under the *Carpenter* factors.

If the Court agrees that this case falls outside *Carpenter*'s narrow exception to normal rules, then no more analysis is needed. But, even applying *Carpenter*'s multi-factor logic, Diaw fails to show a reasonable expectation of privacy in a single GPS datapoint obtained from an online marketplace. Indeed, all of the *Carpenter* factors cut against Diaw.

1. Historical understanding. Recall first that for much of this Nation's history, the Fourth Amendment was "tied to common-law trespass" and prevented the government from "physically intruding on a constitutionally protected area." *Carpenter*, 585 U.S. at 304 (quotation omitted). And, to the founding generation, there was nothing inherently suspect about the government subpoenaing information from potential witnesses. *See above* at 16–17. Combining these points, there is no plausible history-based argument that

the State trespassed against Diaw's property by subpoenaing the records of another. Diaw does not say otherwise.

This case, moreover, does not raise the broader historical concerns that *Carpenter* relied upon. *Carpenter* worried that easy government access to historic cell-site-location information would allow the very "permeating police surveillance" the Framers feared. *Carpenter*, 585 U.S. at 305, 320 (quotation omitted). The information online marketplaces possess, however, is far less than that of wireless carriers. No rational fear exists that the government's acquisition of online-marketplace information—involving short periods of time—will amount to "permeating police surveillance." *See id.* (quotation omitted).

One final aside about history. From an original-meaning perspective, some have criticized the third-party doctrine as too broad. The idea is that, under common-law principles of "bailment," people sometimes entrust possession of their property to third parties. *See Carpenter*, 585 U.S. at 399 (Gorsuch, J., dissenting); Laura K. Donohue, *Functional Equivalence and Residual Rights Post-Carpenter: Framing a Test Consistent with Precedent and Original Meaning*, 2018 Sup. Ct. Rev. 347, 353–54 (2018). The argument continues that people should not automatically lose protection in "their … papers, and effects," *see* U.S. Const. amend. IV, simply because they have turned over possession to others. *See Carpenter*, 585 U.S. at 399–400 (Gorsuch, J., dissenting). Of course, this Court—as a lower court on matters of federal law—has no authority to depart from the U.S. Supreme Court's third-party doctrine. *See State v. Bourn*, 2022-Ohio-4321, ¶73 (DeWine,

J., concurring in the judgment only). But even setting that aside, the argument does not fit this case. Absent special circumstances (and Diaw has brought none to light), no confidential, "bailee"-like relationship exists between online marketplaces and their sellers. If anything, the opposite is true: online marketplaces, trying to protect the integrity of their platforms, have strong reason to inform on those abusing their services.

2. Revealing nature. *Carpenter*'s "revealing nature" factor is no better for Diaw. The historic cell-site-information at stake in *Carpenter* allowed for "a detailed chronicle of a person's physical presence compiled every day, every moment, over several years." 585 U.S. at 315. That risked providing "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.* at 311 (quotation omitted). Location information associated with online-marketplace activities over a short timeframe, *see* App.Op. ¶6, provides nowhere near the same intimate window into someone's life. Tellingly, the State received only a single GPS datapoint corresponding to a McDonald's in the area. *See* Supp. Hearing Tr. 25–26, 64. That provided just "a mere snapshot of" Diaw's location; "a single movement in a public space." App.Op. ¶58.

3. Amount of data. The amount of data at stake in the two cases is also night and day. In *Carpenter*, the government asked wireless carriers to provide a suspect's historic cell-site-location information for a months-long stretch. *Carpenter*, 585 U.S. at 302. Unsurprisingly, the government's broad requests yielded broad information about the

suspect's long-term movements. *Id.* Contrastingly, the subpoena here asked an online marketplace for only three days of information about a specific posting. App.Op. ¶6. As anyone would expect, the online marketplace did not have anywhere near the same amount of data as a wireless carrier. *Compare* App.Op. ¶8 (disclosure of "a single latitude and longitude"), *with Carpenter*, 585 U.S. at 302 (disclosure of "12,898 location points").

4. Voluntary exposure. Finally, this case involves the voluntary exposure of information in a way that *Carpenter* did not. As *Carpenter* emphasized, carrying a cell phone is a largely passive activity. In a literal sense, one "chooses" to have a cell phone; but it is not much of a choice in today's world. Rather, possessing a cell phone has become an "inescapable" and "indispensable" part of modern life for most. *Carpenter*, 585 U.S. at 315, 320. Given those realities, cell-site-location information is "not truly 'shared'" with wireless carriers "as one normally understands the term." *Id.* at 315.

None of that holds true for participation in online marketplaces. Online marketplaces are not an "inescapable" part of modern life. Many people no doubt avoid such platforms altogether because of their dangers. *See, e.g.*, Kelly Kennedy, *Akron Police still searching for suspect in multiple Facebook Marketplace robberies*, 19 News (Sept. 10, 2024), https://tinyurl.com/4dkhrs7h; Sean Humphrey, *Hartford man sentenced to prison for gunpoint robberies targeting online sellers of luxury goods*, Fox 61 (Jan. 23, 2025), https://tinyurl.com/2fh6h66n; *Las Vegas police urge caution with online marketplaces as scams rise*, News 3 (Jan. 6, 2025), https://tinyurl.com/3s3ae9b5; *Des Moines man arrested for alleged*

robbery during online marketplace transaction, KCCI (Dec. 24, 2024), https://tinyurl.com/bp5rucer; Alex Baker, *3 arrested for armed robbery of online marketplace seller*, KRON 4 (July 26, 2024), https://tinyurl.com/4yeycyrv; James Lynch, *Selling online? Expert recommends safety tips following Seattle robbery*, Kiro Newsradio (July 3, 2024), https://tinyurl.com/227pwhyz; Nydia Han, *Safety and security warning for Facebook Marketplace users after recent Philly robberies*, ABC 6 (May 31, 2023), https://tinyurl.com/4xsr6khs.

Online marketplaces, moreover, require deliberate opt-in actions. Users create accounts, log into accounts, and communicate with others about potential transactions. Such conscious activity is much different than passively carrying a cell phone. In this case, Diaw voluntarily created a Letgo account and then used the marketplace to advertise an item for sale. By doing those things, Diaw voluntarily "shared" information with the platform under the ordinary sense of that term. It follows that, unlike in *Carpenter*, the "rationale underlying the third-party doctrine" rings true in *this* case. *See* 585 U.S. at 315.

To sharpen the voluntary-exposure point further, consider the nature of modern applications. Today's technology gives people considerable freedom to decide when to share location data. Andriods and iPhones—to highlight two common devices—allow their users to control when they are sharing location data with applications. *See Manage*

location permissions for apps, Android Help, https://tinyurl.com/2u2wfvzj; *Control the location information you share on iPhone*, iPhone User Guide, https://tinyurl.com/5azy562x.

And, for many applications, location data is a big part of what makes a platform effective and efficient. A critical goal of online marketplaces, for instance, is to connect local buyers with local sellers. Online marketplaces, therefore, openly acknowledge that they collect and use location data. Notably here, OfferUp—which acquired Letgo a few years back—tells its users that the platform "automatically collect[s] … location information" upon their consent. *Privacy Policy*, OfferUp (Jan. 9, 2025), https://offerup.com/privacy; *see* Sarah Perez, *Online marketplace OfferUp raises $120M, acquires top competitor letgo*, TechCrunch (Mar. 25, 2020), https://tinyurl.com/5n7v69td. That platform also informs its users that it might share information to resolve disputes between users, and at the request of law enforcement. *Privacy Policy*, OfferUp; *see also Privacy Policy*, Craigslist (May 29, 2024), https://tinyurl.com/4dvxxy5c (informing users that Craigslist collects location data and may share that data in response to subpoenas). Thus, to say that those using online marketplaces do not voluntarily expose their location data is to ignore how these platforms work and are commonly understood.

III. Diaw's contrary arguments are unpersuasive.

Diaw argues that he has a reasonable expectation of privacy in a single location datapoint, but his analysis makes several mistakes.

A. Diaw misunderstands Fourth Amendment precedent.

Diaw misreads the U.S. Supreme Court's cases. Most notably, Diaw wrongly argues that *Carpenter* "removed an individual's location data from the ambit of the third-party doctrine." Diaw Br. 10. *Carpenter* was nowhere near that broad. By its own terms, *Carpenter* expressed no "view on matters not before" it, including questions about more limited amounts of location data. 585 U.S. at 310 n.3, 316. *Carpenter* expressly left open whether the government could obtain less than seven days of cell-site-location information without a warrant. *Id.* at 310 n.3. It also expressly left open the question of "real-time" location data. *Id.* at 316. Thus, reading *Carpenter* as a categorical rule for all location data fails to fairly engage with what *Carpenter* actually said.

To make matters worse, Diaw's opening brief does not mention the U.S. Supreme Court's decision in *Knotts*. That is a big oversight. Once again, *Knotts* held that people lack a protected privacy expectation in discrete public journeys (like, say, a trip to the local McDonald's). *See* 460 U.S. at 281. *Carpenter* discussed *Knotts* at length and did not overrule it. 585 U.S. at 306–07. So, other courts cannot read *Knotts* as implicitly overruled. *See Bosse v. Oklahoma*, 580 U.S. 1, 3 (2016) ("Our decisions remain binding precedent until we see fit to reconsider them, regardless of whether subsequent cases have raised doubts about their continuing vitality." (quotation omitted)).

Beyond misinterpreting the U.S. Supreme Court's cases, Diaw places too much stock in *Commonwealth v. Almonor*, 482 Mass. 35 (2019). *See* Diaw Br. 14. There, the Supreme

Judicial Court of Massachusetts held that police must generally have a warrant to obtain "real-time location" data from a suspect's cell phone. *Id.* at 36–37. But *Almonor* reached that conclusion under the Massachusetts Constitution, not the Fourth Amendment. *Id.* at 36–37, 41–42 & n.9. Here, Diaw has not developed any arguments specific to the Ohio Constitution. *See, e.g.*, Diaw Br. 8 n.1. This case, it follows, is not a chance for the Court to explore whether the Ohio Constitution offers any greater protection in this area. *State v. Burroughs*, 2022-Ohio-2146, ¶11.

B. Diaw misapplies the *Carpenter* factors.

Diaw does not argue (at least in any developed fashion) that he prevails under a standard Fourth Amendment analysis. Instead, Diaw presumes that *Carpenter*'s case-specific, multi-factor analysis applies to this case. *See* Diaw Br. 10–16. As discussed above (at 18– 21, 23), it does not. This Court should therefore apply normal Fourth Amendment rules—including the third-party doctrine—rather than discovering new exceptions to existing U.S. Supreme Court precedent.

In any event, Diaw misapplies the *Carpenter* factors. For starters, Diaw completely misses *Carpenter*'s first factor. He offers nothing about how "historical understandings" inform his analysis. *See Carpenter*, 585 U.S. at 304–05. Instead, Diaw openly endorses an ahistoric approach. He appeals to a supposed "growing inclination to afford" people "greater privacy protections." Diaw Br. 8. But contrary to Diaw's suggestions, *Carpenter* does not invite that type of free-wheeling, evolving-inclination inquiry.

Diaw fares no better on *Carpenter*'s other factors. For the "revealing nature" factor, Diaw argues that GPS data is more precise than cell-site-location information. Diaw Br. 10–11. Diaw, however, identifies no technical evidence supporting that understanding. Even accepting the unproven premise, *Carpenter*'s analysis of the revealing nature of cell-site-location information stressed the "detailed chronicle" such information can provide. 585 U.S. at 315. Diaw thus offers no true response to the fact that *Carpenter* involved a months-long chronicle of a suspect's movements, while this case involves only a single location datapoint. Diaw also implies that the GPS data revealed his "private residence." *See* Diaw Br. 11–12. But that is incorrect. It was a *different* disclosure from the Letgo subpoena (the email address) that revealed Diaw's residence. *See* App.Op. ¶10. And Diaw's proposition does not challenge that disclosure. *See above* at 10, 12.

For *Carpenter*'s "amount" factor, Diaw does not argue that this case involves as much data. *See* Diaw Br. 13–14. That is a wise concession since there is no plausible argument to be made. Instead of making any comparison, Diaw merely repeats his overarching belief that "*Carpenter*'s core principle" extends to "a single location datapoint." *Id.* But that belief makes no sense when one revisits *Carpenter*. If *Carpenter* meant to establish a categorical rule for all location data, it would not have stressed the "depth, breadth, and comprehensive reach" of cell-site-location information as a determining factor in its analysis. *See* 585 U.S. at 320.

Diaw's analysis of *Carpenter*'s "voluntary exposure" factor likewise falls flat. Diaw says that, in using an online marketplace, he did not take "any affirmative act" beyond what was "contemplated in *Carpenter*." Diaw Br. 15. He is again wrong. *Carpenter* stressed that a cell phone generates cell-site-location information "by dint of" the phone's "operation, without any affirmative act on the part of the user beyond powering up." 585 U.S. at 315; *see also id.* at 300–01 (emphasizing that cell phones "tap into the wireless network" regardless of whether the owner is "using one of the phone's features"). By contrast here, Diaw needed to do more than simply "power up" a device to share information with Letgo. For there to be any information responsive to the relevant subpoena, *see* App.Op. ¶6, Diaw needed to affirmatively create a Letgo account and advertise a computer sale.

C. Diaw's remaining arguments are unconvincing.

Diaw sprinkles in a few other arguments, but none withstands scrutiny. For example, Diaw suggests that the subpoena to Letgo was impermissibly broad because it sought "any and all records" about the false computer sale. *See* Diaw Br. 9, 11, 16. The immediate problem is that Diaw does not have standing to pursue the rights of Letgo—the subpoenaed third party here. *See Miller*, 425 U.S. at 444; *Hansen*, 599 U.S. at 769. If Letgo wanted to challenge the subpoena for *its* records, it could have done so. It did not.

Regardless, any overbreadth challenge lacks merit. Recall that subpoenas generally pose no problem if they are "sufficiently limited in scope, relevant in purpose, and specific in directive." *Donovan*, 464 U.S. at 415; *above* at 17. Here, the subpoena said this:

> Please provide any and all records including all names, addresses, phone numbers, I.P. addresses and email addresses associated with the customer using the name of John Malick (possibly utilizing the phone number of 720-203-7022) and posting for sale a Mackbook [sic] Pro 2017 13 inch lap top computer for sale through Letgo posted in Columbus Ohio between the dates of 02-16-2020 through 02-18-2020.

Supp. Hearing State Ex. A-1. Parsing this language, a record was responsive *only if* (1) it was associated with a specific account, the "John Malick" account, (2) it related to the sale of a specific computer model/year, and (3) it fell within a three-day window. Thus, while the subpoena requested "any and all records," that request was for a *very* narrow universe. Given the three qualifiers—user, computer-sale posting, and timeframe—the subpoena was limited, relevant, and specific. *See Donovan*, 464 U.S. at 415. And, considering Letgo's perspective, nothing in the record suggests that this subpoena was "unreasonably burdensome." *See id.* Letgo possessed just a few pieces of responsive information, which the company (by all indications) quickly found. *See* App.Op. ¶8.

Diaw hints at another subpoena-related argument, but one that is outside this appeal's scope. Specifically, Diaw argues that the Letgo subpoena "violated statutory mandates" within R.C. 2935.23. Diaw Br. 9 & n.5. The text of that statute, the argument goes, does not expressly say that a subpoenaed party may provide information directly to police in lieu of appearing in court. *See id.* Because Diaw did not submit a proposition about any

statutory violation, the argument is just a distraction. Regardless, this Court has repeatedly held that, absent a legislative mandate, statutory violations do not justify excluding evidence. *Campbell*, 2022-Ohio-3626 at ¶22.

Diaw also misunderstands the good-faith exception to the Fourth Amendment's exclusionary rule. He posits that, if he wins on the merits, the good-faith exception could not apply. Diaw Br. 16 n.8. That is wrong. Under the good-faith exception, exclusion of evidence is unjustified when "the police act with an objectively reasonable good-faith belief that their conduct is lawful." *Davis v. United States*, 564 U.S. 229, 238 (2011) (quotation omitted). And whether a police officer has an objectively reasonable good-faith belief depends on the state of the law at the time. *See State v. Johnson*, 2014-Ohio-5021, ¶¶43–50. By Diaw's own admission, this case at the very least "implicates an ambiguous area in the application of the Fourth Amendment." Diaw Br. 8. Given the present state of the law, it was at least reasonable (indeed, correct) for Detective Sturgill to think that he did not need a warrant to obtain information from an online marketplace.

One final thread to unravel. As noted above (at 7), Detective Sturgill eventually sought a warrant for eighteen days' worth of location data from Sprint. *See* Supp. Hearing State Ex. A-8. Diaw suggests that seeking a warrant for *that* information signals a problem with seeking different information from an online marketplace without a warrant. *See* Diaw Br. 12. Diaw's logic does not hold up. Seeking weeks of location data from a telecommunications company largely mirrors what happened in *Carpenter*;

seeking isolated records from an online marketplace does not. If anything, this distinction in Detective Sturgill's conduct hammers home that he was conforming his investigation to existing legal rules. *See Davis*, 564 U.S. at 241.

CONCLUSION

For the above reasons, the Court should affirm the Tenth District.

Respectfully submitted,

DAVE YOST
Attorney General of Ohio

/s T. Elliot Gaiser
T. ELLIOT GAISER* (0096145)
Solicitor General
**Counsel of Record*
ZACHERY P. KELLER (0086930)
Deputy Solicitor General
30 East Broad Street, 17th Floor
Columbus, Ohio 43215
614.466.8980
614.466.5087 fax
thomas.gaiser@ohioago.gov

Counsel for *Amicus Curiae*
Ohio Attorney General Dave Yost

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing Merit Brief of *Amicus Curiae* Ohio Attorney General Dave Yost in Support of Appellee was served this 14th day of February, 2025, by e-mail on the following:

Adam G. Burke
625 City Park Avenue
Columbus, Ohio 43206
burke142@gmail.com

Seth L. Gilbert
Chief Counsel, Appeals Unit
373 South High Street–13th Fl.
Columbus, Ohio 43215
sgilbert@franklincountyohio.gov

/s T. Elliot Gaiser
T. Elliot Gaiser
Solicitor General