

THE STATE OF OHIO, APPELLEE, v. DIAW, APPELLANT.

[Cite as *State v. Diaw*, 2025-Ohio-2323.]

Criminal law—Fourth Amendment to United States Constitution—Because a person generally has no expectation of privacy in information voluntarily shared with third parties, Fourth Amendment does not require law enforcement to obtain a search warrant before securing a single historical location data point from third-party online-marketplace app—Court of appeals’ judgment affirmed and cause remanded to trial court.

(No. 2024-1083—Submitted April 23, 2025—Decided July 2, 2025.)

APPEAL from the Court of Appeals for Franklin County,

No. 22AP-614, 2024-Ohio-2237.

KENNEDY, C.J., authored the opinion of the court, which FISCHER, DEWINE, BRUNNER, DETERS, HAWKINS, and SHANAHAN, JJ., joined.

KENNEDY, C.J.

{¶ 1} In this discretionary appeal from the Tenth District Court of Appeals, we consider whether a person who voluntarily shares a location data point with a third-party online-marketplace app has a reasonable expectation of privacy in that information. Because a person generally has no expectation of privacy in information that is voluntarily shared with third parties, we hold that the Fourth Amendment to the United States Constitution does not require law enforcement to obtain a search warrant before securing a single historical location data point from a third party. Therefore, we affirm the Tenth District’s judgment and remand this cause to the trial court for proceedings consistent with this opinion.

Facts and Procedural History

{¶ 2} Letgo is an online-marketplace app that allows users to post items that they have for sale. It also lets users message each other so that they can coordinate a time and place to meet and complete the transaction.

{¶ 3} The allegations against appellant, Mamadou Diaw, are as follows: K.W. agreed to buy a MacBook Pro laptop from a seller on Letgo who was operating under the alias John Malick. K.W. showed up at their agreed meeting location to buy the laptop from “Malick”—whom law enforcement later identified as Diaw. K.W. entered Diaw’s car to buy the laptop from him and an accomplice. After K.W. entered the vehicle, Diaw stole an iPhone and money that K.W. had brought to exchange for the laptop, pulled the laptop away from K.W., and began punching him in the head and face. Diaw’s accomplice then pointed a gun at K.W. K.W. exited the vehicle, and Diaw followed, pushed him to the ground, and repeatedly kicked him, injuring his ribs.

{¶ 4} Pursuant to R.C. 2935.23, which allows law enforcement to subpoena witnesses after “a felony has been committed” but “before any arrest has been made,” Columbus Police Detective Michael Sturgill subpoenaed Letgo for

all names, addresses, phone numbers, I.P. addresses and email addresses associated with the customer using the name of John Malick . . . and posting for sale a MacBook Pro 2017 13-inch laptop computer for sale through Letgo posted in Columbus, Ohio between the dates of 02-16-2020 through 02-18-2020.

{¶ 5} Letgo provided the detective with an IP address, an email address associated with the posting, and a single latitude-and-longitude point. According to Detective Sturgill, the latitude-and-longitude point corresponds with a

McDonald’s restaurant located on East Broad Street in Columbus, adjacent to Diaw’s apartment.

{¶ 6} Diaw moved to suppress the information Letgo provided in response to the subpoena. The trial court granted his motion, finding that the police acquired the information in violation of the Fourth Amendment. Franklin C.P. No. 21CR-379, 9 (Oct. 3, 2022). The Tenth District reversed. It relied on the United States Supreme Court’s decision in *Carpenter v. United States*, 585 U.S. 296 (2018), to hold that Diaw did not have a reasonable expectation of privacy in his location data, because police obtained only a single, voluntarily communicated data point that was historical in nature and was not a real-time location or Diaw’s home. 2024-Ohio-2237, ¶ 58, 60-62 (10th Dist.).

{¶ 7} Diaw appealed to this court, arguing that he had a reasonable expectation of privacy in the location data his cellphone communicated to Letgo. We agreed to review his sole proposition of law: “The United States Supreme Court’s holding in *Carpenter* and related cases held that individuals maintain a privacy interest and Fourth Amendment protections in the whole of their movements, including their physical location.” *See* 2024-Ohio-5173.

Law and Analysis

Standard of Review

{¶ 8} The review of a motion to suppress is a mixed question of law and fact. *State v. Castagnola*, 2015-Ohio-1565, ¶ 32. An appellate court reviewing a motion to suppress accepts the trial court’s findings of fact if they are supported by competent, credible evidence and reviews its legal conclusions de novo. *State v. Burnside*, 2003-Ohio-5372, ¶ 8.

The Fourth Amendment

{¶ 9} The Fourth Amendment, applicable to the states through the Fourteenth Amendment, *Mapp v. Ohio*, 367 U.S. 643, 660 (1961), guarantees “the right of the people to be secure in their persons, houses, papers, and effects, against

unreasonable searches and seizures,” *id.* at 646, fn. 4. Its protections against “arbitrary intrusion by the police” are “basic to a free society.” *Coolidge v. New Hampshire*, 403 U.S. 443, 453 (1971). Subject to exceptions not relevant here, the Fourth Amendment “stays the hands of the police unless they have a search warrant issued by a magistrate on probable cause supported by oath or affirmation,” *McDonald v. United States*, 335 U.S. 451, 453 (1948).

{¶ 10} A search occurs in violation of the Fourth Amendment “when the government gains evidence by physically intruding on [a] constitutionally protected area[]” or when the government’s intrusion violated a person’s reasonable expectation of privacy. *Florida v. Jardines*, 569 U.S. 1, 11 (2013).

{¶ 11} Until the middle of the twentieth century, the Court’s Fourth Amendment jurisprudence focused on whether the government trespassed on a person’s private property. *See Kyllo v. United States*, 533 U.S. 27, 31 (2001) (collecting cases). Later, however, the Court recognized that in addition to protecting private property, the Fourth Amendment protects against governmental intrusion when two criteria are met: “first [the] person [has] exhibited an actual (subjective) expectation of privacy and, second, that the expectation [is] one that society is prepared to recognize as ‘reasonable,’” *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); *see also Smith v. Maryland*, 442 U.S. 735, 740 (1979); *United States v. Carriger*, 541 F.2d 545, 549-550 (6th Cir. 1976) (holding that the reasonable-expectation-of-privacy test did not replace but, rather, added to the Fourth Amendment’s property-based approach).

{¶ 12} Put differently, a defendant must show that his or her expectation of privacy, “viewed objectively,” was “‘justifiable’ under the circumstances.” *Smith v. Maryland*, 442 U.S. 735, 740 (1979), quoting *Katz* at 353; *see also Rawlings v. Kentucky*, 448 U.S. 98, 104 (1980) (holding that a defendant has the burden of showing a legitimate expectation of privacy in what the government seeks); *Florida*

v. Riley, 488 U.S. 445, 455 (1989) (O’Connor, J., concurring) (“the defendant must bear the burden of proving that his expectation of privacy was a reasonable one”).

{¶ 13} Although the Court has focused on the objective prong of the *Katz* test, it has given examples of when a person has exhibited a subjective expectation of privacy. In *California v. Ciraolo*, 476 U.S. 207, 211 (1986), it recognized that a person who placed a ten-foot-high fence around his property exhibited a subjective expectation of privacy. And in *United States v. Chadwick*, 433 U.S. 1, 11 (1977), the Court held that a person had a subjective expectation of privacy in a double-locked footlocker. But the Court has also held that a defendant did not have a reasonable expectation of privacy in the purse of an acquaintance that he had known for only a few days and to which others had access. *Rawlings* at 105. Essentially, an inquiry into a person’s subjective expectation of privacy asks whether the person manifested the belief that he or she was keeping something private, rather than the mere “hope” that it would remain private. *Ciraolo* at 212.

{¶ 14} Next, no single factor determines whether a person has exhibited a subjective expectation of privacy that society is prepared to accept as reasonable. *Oliver v. United States*, 466 U.S. 170, 177-178 (1984), citing *Rakas v. Illinois*, 439 U.S. 128, 152-153 (1978) (Powell, J., concurring). However, the Court has drawn a “firm line” at people’s reasonable expectation of privacy in their homes. *Payton v. New York*, 445 U.S. 573, 590 (1980).

{¶ 15} The Court has also examined the severity of the government’s intrusion to determine whether a defendant had an objectively reasonable subjective expectation of privacy. In *Riley*, the Court held that a police helicopter flying over a home that revealed no intimate details inside the home and created no “undue noise, and no wind, dust, or threat of injury” did not violate an objective expectation of privacy. 488 U.S. at 452.

{¶ 16} Finally, in what has become known as the third-party doctrine—and most relevant here—the Court has held that a person has no reasonable expectation

of privacy in information that he or she voluntarily turns over to third parties. *Smith*, 442 U.S. at 743. By voluntarily turning over information to a third party, a person takes the risk that the information will end up in the hands of the government. *Id.* at 743-744.

The Third-Party Doctrine

{¶ 17} Of course, “[n]ot all government actions are invasive enough to implicate the Fourth Amendment.” *United States v. Warshak*, 631 F.3d 266, 284 (6th Cir. 2010). Applying the *Katz* test, the Court “consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.” *Smith* at 743-744; *see id.* at 744 (collecting cases).

{¶ 18} In *Smith*, the Court used the *Katz* test to analyze the petitioner’s argument that the installation of a pen register, which transmitted numbers dialed on his home phone to the police, constituted a search that violated the Fourth Amendment. The Court cited *Hoffa v. United States*, 385 U.S. 293 (1966), a case in which an informant provided the government with details of a conversation the informant had with the defendant. There, the Court held that “we necessarily assume whenever we speak” the “risk of being overheard by an eavesdropper or betrayed by an informer or deceived as to the identity of one with whom one deals,” *id.* at 303, quoting *Lopez v. United States*, 373 U.S. 427, 465 (1963) (Brennan, J., dissenting).

{¶ 19} That risk—“inherent in the conditions of human society”—led the Court to hold that a person has “no interest legitimately protected by the Fourth Amendment” in his or her statements made to a third party who turned out to be a police informant. *Id.*; *see On Lee v. United States*, 343 U.S. 747, 753-754 (1952) (holding that the Fourth Amendment did not protect a conversation the defendant had with a third-party that police listened to through a wire). Consequently, the Fourth Amendment does not protect “a wrongdoer’s misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.” *Hoffa* at 302.

And although *Hoffa* is pre-*Katz*, the Court noted in *United States v. White* that *Katz* left *Hoffa* “undisturbed.” 401 U.S. 745, 749 (1971) (plurality opinion).

{¶ 20} Then the *Smith* Court turned from cases addressing statements to cases considering whether individuals have a reasonable expectation of privacy in information that they disclose to others. In *United States v. Miller*, 425 U.S. 435, 442 (1976), the Court held that people do not have a viable privacy claim in financial documents turned over to third parties. In *Miller*, the Court, stressing the lack of confidentiality in the “nature of the particular documents sought to be protected,” held that a bank depositor had “no legitimate ‘expectation of privacy’ ” in financial records “voluntarily conveyed to . . . banks and exposed to their employees in the ordinary course of business,” *id.*, because the depositor risks, “in revealing his affairs to another, that the information will be conveyed by that person to the Government,” *id.* at 443. Likewise, the Court determined in *Smith* that the defendant who “voluntarily conveyed numerical information to the telephone company . . . assumed the risk that the company would reveal to police the numbers he dialed,” *Smith*, 442 U.S. at 744.

{¶ 21} *Smith* and *Miller*—leaving *Katz*’s reasonable-expectation-of-privacy test intact—give us the simple rule that those who voluntarily disclose information about themselves to a third party assume the risk that the third party may pass along their information to the government and therefore forfeit any expectation that their information will remain private.

{¶ 22} Then came *Carpenter*, 585 U.S. 296. There, law enforcement arrested four men suspected of robbing an electronics retailer and a cellphone store in Detroit. *Id.* at 301. These men provided the FBI with some of their accomplices’ phone numbers. *Id.* Using those phone numbers, the FBI obtained, without a warrant, Timothy Carpenter’s cell-site location information (“location information”) from MetroPCS and Sprint. *Id.* at 301-302. Cellphones generate location information by connecting to the closest cell tower, even if the user is not

using the phone, and pinging the user’s proximity to the tower. *Id.* at 300. This gives law enforcement information about an accurate assessment of the person’s location at a given time.

{¶ 23} The first phone company provided agents with 127 days’ worth of information. *Id.* at 302. The second provided them with two days of records, when Carpenter was “roaming” (i.e., outside of the first phone company’s cell coverage). *Id.* From those records, the government obtained roughly 13,000 location points. *Id.* Carpenter challenged the government’s right to obtain that information, arguing that he had a reasonable expectation of privacy in that data.

{¶ 24} The Court, in a narrow decision, careful not to “disturb the application of *Smith* and *Miller*,” held that the third-party doctrine does not apply to such a large swath of location information that Carpenter did not voluntarily convey. *Carpenter* at 316. Although the Court applied “no single rubric,” *id.* at 304, multiple factors guided its decision, *id.* at 304-305.

{¶ 25} First, the Court noted that when ratified, the Fourth Amendment was understood to guard “‘the privacies of life’ against ‘arbitrary power.’” *Id.*, 585 U.S. at 305, quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886). The Fourth Amendment also places “‘obstacles in the way of a too permeating police surveillance.’” *Id.*, quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948). The Court was concerned that allowing government access, without a warrant, to the location information of 400 million cellphones would violate those principles. *Id.* at 312.

{¶ 26} Second, the Court discussed its decisions addressing a person’s expectation of privacy in his or her physical location and movements. The Court noted that in *United States v. Jones*, Justice Alito and three other members of the Court had concluded that “‘longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy’—regardless of whether those movements were disclosed to the public at large.” *Carpenter* at 307, quoting *United*

States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring), and citing *Jones* at 415 (Sotomayor, J., concurring). For the concurring justices in *Jones*, 28 days’ worth of data that “tracked every movement that [the defendant] made in the vehicle he was driving” violated the Fourth Amendment, *Jones* at 430 (Alito, J., concurring).

{¶ 27} Third, the Court discussed the third-party doctrine, concluding that it did not apply to location information, because location information chronicles a person’s physical presence and because Carpenter did not voluntarily reveal this information to a third party. *Carpenter* at 315.

{¶ 28} The Court compared the nature of the information sought in *Smith* and *Miller* with the “all-encompassing [location information] record” at issue in *Carpenter*. *Carpenter*, 585 U.S. at 311. The record in *Carpenter* amounted to a “detailed chronicle of [Carpenter’s] physical presence compiled every day, every moment, over several years,” *id.* at 315—a far cry from financial documents that were ““not confidential communications but negotiable instruments to be used in commercial transactions,”” *id.* at 308, quoting *Miller*, 425 U.S. at 442, or a pen register that revealed only numbers dialed and no ““identifying information,”” *id.* at 314, quoting *Smith*, 442 U.S. at 742.

{¶ 29} The Court then determined that users do not voluntarily create location information because a cellphone is an ““insistent part of daily life’ [and] . . . carrying one is indispensable to participation in a modern society,”” *id.* at 315, quoting *Riley v. California*, 573 U.S. 373, 385 (2014), and is now “almost a ‘feature of human anatomy,’” *id.* at 311, quoting *Riley* at 385. Moreover, location information is involuntarily created because a person’s cellphone generates location information without any action from the user.

{¶ 30} By its terms, *Carpenter* was “a narrow decision” that did “not disturb the application” of the third-party doctrine articulated in *Smith* and *Miller*. Therefore, federal courts continue to apply the third-party doctrine. *See, e.g.*,

United States v. Rosenow, 50 F.4th 715, 737-738 (9th Cir. 2022) (holding that a person has no reasonable expectation of privacy in IP addresses communicated to a third party); *Sanchez v. Los Angeles Dept. of Transp.*, 39 F.4th 548, 559-561 (9th Cir. 2022) (holding that a defendant had no reasonable expectation of privacy in location data communicated by a cellphone app to an electric-scooter company).

The Third-Party Doctrine Applies to Diaw’s Use of Letgo

{¶ 31} Start with voluntariness. There is little difficulty concluding that Letgo users voluntarily provide their location information to a third party. Users make the affirmative choice to download Letgo. They also make the choice to create a Letgo account.

{¶ 32} Having voluntarily conveyed his location to Letgo in the ordinary course of using the app, Diaw cannot now assert a reasonable expectation of privacy in that information. *See Miller*, 425 U.S. at 442 (holding that a person has no reasonable expectation of privacy in documents containing information voluntarily conveyed to employees in the ordinary course of business). Lastly, Diaw also has not shown that Letgo, unlike a cellphone, is an “insistent part of daily life,” *Riley*, 573 U.S. at 385, further demonstrating that using Letgo is voluntary.

{¶ 33} Turn to the nature of the information Letgo provided to law enforcement: a single latitude-and-longitude point indicating that Diaw used Letgo at a McDonald’s. That location reveals only where Diaw used Letgo, which is designed for users to sell items locally. *See Roland v. Letgo, Inc.*, 2024 WL 372218, *1 (10th Cir. Feb. 1, 2024).

{¶ 34} Moreover, Diaw has no reasonable expectation of privacy in what he “‘knowingly exposes to the public,’” *Ciraolo*, 476 U.S. at 213, quoting *Katz*, 389 U.S. at 351. And he has no reasonable expectation of privacy while physically present at a McDonald’s because there is no reasonable expectation of privacy when “on public thoroughfares,” because such movements are “voluntarily conveyed to anyone who wanted to look,” *United States v. Knotts*, 460 U.S. 276,

281 (1983). Diaw cannot now claim a privacy interest in information he otherwise would not have a reasonable expectation of privacy in just because it was disclosed by a third party to law enforcement.

{¶ 35} Finally, the privacy concerns expressed in *Jones* are not present here. In this case, police subpoenaed three days’ worth of information but received location data for only a single day. In *Jones*, the 28 days’ worth of location data that “tracked every movement that [Jones] made” constituted a search. *Jones*, 565 U.S. at 430 (Alito, J., concurring). Accordingly, a subpoenaed information that reveals only a single location point on a single day does not implicate the same privacy concerns that the concurring justices raised in *Jones*.

{¶ 36} Using Letgo falls squarely within the third-party doctrine. Users voluntarily choose to use Letgo. And the data that Letgo provided to law enforcement in this case revealed the location where the user had logged in to use the app but did not reveal any information that the Fourth Amendment protects. Indeed, people who use a cellphone app that facilitates local sales through in-person transactions do not have a reasonable expectation of privacy in that information, because they are revealing their location to the public by using the app.

Conclusion

{¶ 37} We hold that a person maintains no reasonable expectation of privacy in a single location data point communicated to an online-marketplace app. We affirm the Tenth District Court of Appeals’ judgment and remand this cause to the trial court for proceedings consistent with this opinion.

Judgment affirmed
and cause remanded to the trial court.

Shayla D. Favor, Franklin County Prosecuting Attorney, and Seth L. Gilbert, Assistant Prosecuting Attorney, for appellee.

Adam G. Burke, for appellant.

SUPREME COURT OF OHIO

Dave Yost, Attorney General, T. Elliot Gaiser, Solicitor General, and Zachary P. Keller, Deputy Solicitor General, urging affirmance for amicus curiae Ohio Attorney General Dave Yost.

Michael C. O'Malley, Cuyahoga County Prosecutor, and Daniel T. Van and Kristen L. Hatcher, Assistant Prosecuting Attorneys, urging affirmance for amicus curiae Ohio Prosecuting Attorneys Association.
