APPENDIX TABLE OF CONTENTS

SLIP OPINION, SUPREME COURT OF OHIO (JULY 2, 2025)

[Until this opinion appears in the Ohio Official Reports advance sheets, it may be cited as *State v. Diaw*, Slip Opinion No. 2025-Ohio-2323.]

SUPREME COURT OF OHIO

THE STATE OF OHIO,

Appellee,

v.

DIAW,

Appellant.

No. 2025-OHIO-2323

(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.

Before: 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 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" —who law enforcement later identified as Diaw. K.W. entered Diaw's car to buy the laptop from him and an accomplice. After the victim entered the vehicle, Diaw stole an iPhone and money that K.W. brought to exchange for the laptop, pulled the laptop away from the victim, and began punching him in the head and face. Diaw's accomplice then pointed a gun at K.W. The victim 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.

{¶ 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 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 remained 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 held 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 v. United States*, 585 U.S. 296 (2018). 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 cell-site 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 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. *Id.* at 316. Although the Court applied "no single rubric," 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.'" *Carpenter*, 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. Previously, in *United States v. Jones*, Justice Alito and three other members of the Court 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 *Jones v. United States*, 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*. *Id.* 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," further demonstrating that using Letgo is voluntary. *See Riley v. California*, 573 U.S. 373, 385 (2014).

{¶ 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* 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 subpoena revealing 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 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 expect-

ation 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.

JUDGMENT ENTRY,
SUPREME COURT OF OHIO
(JULY 2, 2025)

THE STATE OF OHIO,

Appellee,

v.

DIAW,

Appellant.

No. 2025-OHIO-2323

JUDGMENT ENTRY
APPEAL FROM THE COURT OF APPEALS

This cause, here on appeal from the Court of Appeals for Franklin County, was considered in the manner prescribed by law. On consideration thereof, the judgment of the court of appeals is affirmed and this cause is remanded to the trial court, consistent with the opinion rendered herein.

It is further ordered that mandates be sent to and filed with the clerks of the Court of Appeals for Franklin County and the Court of Common Pleas for Franklin County.

(Franklin County Court of Appeals; No. 22AP-614)

/s/ Sharon L. Kennedy
Sharon L. Kennedy
Chief Justice

DECISION, COURT OF APPEALS OF OHIO, TENTH APPELLATE DISTRICT (JUNE 11, 2024)

THE COURT OF APPEALS OF OHIO
TENTH APPELLATE DISTRICT

STATE OF OHIO,

Plaintiff-Appellant,

v.

MAMADOU DIAW,

Defendant-Appellee.

No. 22AP-614

(C.P.C. No. 21CR-0379)

Appeal from the Franklin County Court of Common Pleas

Before: MENTEL, P.J., BOGGS and EDELSTEIN, JJ.

DECISION

MENTEL, P.J.

{¶ 1} Plaintiff-appellant, State of Ohio, appeals from an October 3, 2022 decision and entry granting the motion to suppress of defendant-appellee, Mamadou Diaw. For the reasons that follow, we reverse.

I. Facts and Procedural History

{¶ 2} On January 28, 2021, Mr. Diaw was indicted by a Franklin County grand jury on one count of aggravated robbery, in violation of R.C. 2911.01, a felony of the first degree (Count One); one count of robbery in violation of R.C. 2911.02, a felony of the second degree (Count Two); and one count of robbery in violation of R.C. 2911.02, a felony of the third degree (Count Three). All three counts included a three-year firearm specification in violation of R.C. 2941.145(A). Mr. Diaw entered a plea of not guilty on February 2, 2021.

{¶ 3} On June 14, 2021, Mr. Diaw filed a combined motion to dismiss the January 28, 2021 indictment or, alternatively, motion to suppress evidence resulting from the illegal search of Mr. Diaw's "GPS/location date, digital data, and account information." (June 14, 2021 Mot. to Suppress at 1.) In the filing, Mr. Diaw argued that law enforcement's use of various R.C. 2935.23 investigative subpoenas, rather than search warrants, violated his constitutional rights as he had a reasonable expectation of privacy over the online information. Mr. Diaw also alleged that the subpoenas at issue were overly broad in their terms to be regarded as reasonable. On June 28, 2021, the state filed a memorandum in opposition arguing that R.C. 2935.23 authorized law enforcement to gather information through both witness testimony and other sources of information such as data and documents. The state posited that the investigative subpoenas were reasonably tailored in scope, and Mr. Diaw had no genuine privacy interests in the online accounts and information contained therein. After a series of continuances, this matter was set for an evidentiary

hearing on February 24, 2022. The following evidence was adduced at the hearing.

{¶ 4} Detective Michael Sturgill testified that he has worked at the Groveport Police Department for approximately 24 years. (Feb. 24, 2022 Tr. at 9.) In February 2020, Sturgill became involved in the investigation of an aggravated robbery case that occurred at a Kroger parking lot located on Groveport Road. (Tr. at 12.) According to Sturgill, the victim in this case, K.W., had arranged for the purchase of a MacBook laptop at the parking lot through the company, Letgo. Sturgill described Letgo as "similar to Craigslist * * * you can take your property and sell it on there." (Tr. at 12.) Upon arrival at the parking lot, K.W. met with two individuals, one later identified as Mr. Diaw, regarding the purchase of the laptop. (Tr. at 13.) According to the grand jury summary, "Mr. Diaw and the accomplice took an i[P]hone and $360.00 cash from the victim for the sale/trade of the computer but Mr. Diaw then pulled the computer away from the victim and began punching the victim in his head and face." (Def. Ex. 2 at 1.) The individuals then fled the scene.

{¶ 5} Sturgill testified that K.W. was able to provide law enforcement (1) descriptions of the individuals involved in the robbery, (2) a description of the vehicle—a red Honda Accord with tinted windows—, (3) account information from the Letgo website, which included the username "John Malick" and the original posting for the computer, (4) the last four digits of the vehicle's license plate; and (5) the telephone number that the individual used to communicate with the victim. (Tr. at 13-14.) Sturgill attempted to search the Ohio Law Enforcement Gateway ("OHLEG") system using the description of the vehicle and the partial

license plate number but was unsuccessful. (Tr. at 16.) Sturgill then conducted a Google search of the telephone number provided by the victim. The search revealed that the cellphone carrier was Boost Mobile, which, according to Sturgill, used Sprint cellphone towers. (Tr. at 17.)

{¶ 6} During the course of the investigation, Sturgill issued several investigative subpoenas to various digital account providers. On February 19, 2020, Sturgill requested an investigative subpoena to Letgo through the Franklin County Municipal Court. The subpoena represented that R.C. 2934.23 authorized the Franklin County Municipal Court to issue subpoenas in aid of felony investigations. The subpoena also identified the felony investigation at issue, aggravated robbery/20-000339, and ordered the Letgo representative "to appear before this Court at the time, date, and location set forth" to offer 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 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.

(Sic passim.) (State's Ex. A-1.)

{¶ 7} The subpoena directed that "[Letgo] can comply with this Investigative Subpoena without the court appearance scheduled below by providing the requested information to the law enforcement officer

who requested this subpoena, and whose contact information is set forth below, prior to the date scheduled for the appearance." (State's Ex. A-1.)

{¶ 8} In response to the investigative subpoena, Letgo provided an IP address, an email address associated with the posting, and a single latitude and longitude. (Tr. at 18, 21-25.) Sturgill described the longitude and latitude data point as a "GPS [coordinate] that will take you to a place." (Tr. at 25.) According to Sturgill, the coordinate corresponded with a McDonald's located on East Broad Street. (Tr. at 25.) During the course of the investigation, Sturgill determined that that the suspect's apartment was located directly behind the McDonald's. (Tr. at 26, 28.)

{¶ 9} Sturgill next sent a subpoena to Sprint, which responded by providing the name on the account, "John Malick," and an address located in Colorado. (State's Ex. A-2; Tr. at 28.) According to Sturgill, based on the information, he determined the name and address were likely fake. (Tr. at 19, 28-29.) Sturgill also testified that the subpoena issued to Boost Mobile, identified as State's Exhibit A-5, produced no results. (Tr. at 29-31.)

{¶ 10} Based on the email address provided by Letgo, Sturgill issued an investigative subpoena to Google to acquire any and all identifying information and records associated with the email address. (State's Ex. A-3; Tr. at 31.) In response to the subpoena, Google identified the name associated with the account as Mamadou Diaw. (Tr. at 31.) Sturgill searched Mr. Diaw's name in OHLEG and procured a driver's license photograph, which he observed matched the victim's description of one of the individuals involved in the robbery. Sturgill created a photo array with Mr.

Diaw's photograph, and a blind administrator presented the array to K.W. who identified Mr. Diaw. (Tr. at 32-33.) Sturgill also obtained Mr. Diaw's driver's license information through OHLEG. According to Sturgill, a Honda Accord was registered to Mr. Diaw. (Tr. at 39-40.)

{¶ 11} During the course of the investigation, the victim contacted Sturgill and notified him that the same individual identified as "John Malick" was posting on another website, OfferUp. (Tr. at 34.) Sturgill issued a subpoena to OfferUp, which resulted in an additional Gmail address and IP address. (State's Ex. A-6; Tr. at 36-37.) Sturgill also sent a subpoena to Charter Communications, Inc. ("Charter") who serviced the IP addresses provided by Letgo and OfferUp. (State's Ex. A-4; Tr. at 34-35, 39.)[1] Charter provided another Gmail address, phone number, and subscriber name that was associated with an address on Cedar Drive. (Tr. at 38-39.) Upon investigating the Cedar Drive address, Sturgill observed a Honda Accord parked at the residence that matched the description and partial license plate number provided by the victim. (Tr. at 39.)

{¶ 12} Sturgill testified that he did not specifically ask for location data in any of the investigative subpoenas. (Tr. at 41.) Sturgill, however, did acknowledge that he sent a search warrant to Sprint, marked as State's Exhibit A-8, seeking "GPS location data, IP address information, cell tower location, customers connected to, including the direction of cell towers were facing." (Tr. at 42.) While Sprint did not respond

---

[1] A second subpoena was issued to Charter, marked State's Exhibit A-7, but it did not yield any relevant results. (Tr. at 41.)

to the search warrant, Sturgill testified, "I wasn't too concerned with the records once I found him because I found him, his car at Cedar Drive. Once I found that, I didn't really care about this." (Tr. at 43-44.) Sturgill went on to state that the subpoenas were not intended to "track anyone's particular movements," "the only time [he] tried that was with * * * a Sprint search warrant, and I didn't get the records." (Tr. at 46.)

{¶ 13} On cross-examination, Sturgill acknowledged that the results from the Letgo subpoena led to the Google subpoena, which led him to obtaining Mr. Diaw's name. (Tr. at 49.) As a result of procuring Mr. Diaw's name, Sturgill was able to run his information in OHLEG to match the vehicle and partial license plate. (Tr. at 49-50.) According to Sturgill, the OfferUp and Charter subpoenas were "essentially a dead end." (Tr. at 51.) Sturgill conceded that the subpoena to Letgo included the language "any and all records" because he did not want to limit the records Letgo could produce in response to the subpoena. (Tr. at 53-54.) "[I]f I don't put any a[nd] all, they'll only give me–they'll only give me just what I specifically spell out. So if–any information they give me, absolutely, I'll take it." (Tr. at 53-54.) Sturgill conceded that he used the coordinate in the investigation and, in fact, cited it in the police summary. (Tr. at 55.) Sturgill testified that he was able to connect the longitude and latitude data point with the residence where he located Mr. Diaw. (Tr. at 55, 65, 68.)

{¶ 14} On redirect, Sturgill testified that the single coordinate, in his opinion, "would track [the] last time [Mr. Diaw] logged into Letgo, and it would have hit his location he was at from there at the time he logged into that site." (Tr. at 75.) While Sturgill initially did

not get any information from the partial license plate, he later learned that he could modify the search to input the license plate and car information to reach a result. (Tr. at 77.) Sturgill testified that if he had searched "a Honda 4S, meaning four doors, and then the partial tag * * * it leads you right to him just the same way. There's a list of, you know, people you got to sort through, but he's on that list." (Tr. at 77-78.) On recross, Sturgill conceded that he learned about how to modify his search after the fact if he "had done things a different way," and it was not how this investigation unfolded. (Tr. at 80.)

{¶ 15} The parties provided extensive closing statements to the trial court. Relevant to the instant case, the parties addressed the trial court's concerns as to the R.C. 2935.23 provision that a witness must appear at the hearing. The trial court permitted the parties to file post-hearing briefs in the matter. In March 2022, the parties filed post-hearing supplemental memoranda regarding Mr. Diaw's outstanding motions.

{¶ 16} On October 3, 2022, the trial court denied Mr. Diaw's motion to dismiss but granted his motion to suppress. The trial court first found that the evidence should be suppressed as the state violated the statutory requirements of R.C. 2935.23 by failing to have a witness testify as to information provided in response to the investigative subpoenas. The trial court next found that the language employed in the investigative subpoenas were overly broad and too sweeping to be considered reasonable. Finally, the trial court found that investigative subpoenas violated Mr. Diaw's rights under the Fourth Amendment to the U.S. Constitution and Article One, Section 14 of

the Ohio Constitution as he had a reasonable expectation of privacy over the information.

{¶ 17} The state filed a timely appeal on October 7, 2022.

II. Assignment of Error

{¶ 18} The state assigns the following as trial court error:

> The trial court committed reversible error in granting the defense's motion to suppress.

III. Standard of Review

{¶ 19} Appellate review of a trial court's decision to grant a motion to suppress presents a mixed question of law and fact. *State v. Robertson,* 10th Dist. No. 22AP-227, 2023-Ohio-2746, ¶ 13, citing *State v. Harrison,* 166 Ohio St.3d 479, 2021-Ohio-4465, ¶ 11, citing *State v. Burnside,* 100 Ohio St.3d 152, 2003-Ohio-5372, ¶ 8.

{¶ 20} An appellate court's standard of review of a trial court's decision concerning a motion to suppress is two-fold. (Further citation omitted.) *State v. Ivery,* 10th Dist. No. 23AP-92, 2023-Ohio-3495, ¶ 30, citing *State v. Pilgrim,* 184 Ohio App.3d 675, 2009-Ohio-5357, ¶ 13 (10th Dist.). In a suppression hearing, the trial court first assumes the role of the trier of fact and, as such, is best positioned to resolve questions of fact and determine the credibility of the witnesses. *Robertson* at ¶ 13, citing *State v. Mills,* 62 Ohio St.3d 357, 366 (1992). Accordingly, a reviewing court should defer to the trial court's factual determinations when supported by "competent, credible evidence." *State v. Leak,* 145 Ohio St.3d 165, 2016-Ohio-154, ¶ 12, citing

Burnside at ¶ 8, citing *State v. Fanning,* 1 Ohio St.3d 19, 20 (1982). Upon accepting the factual determinations of the trial court, a reviewing court, must then independently resolve whether the facts satisfy the applicable legal standard without deference to the trial court's legal conclusions. *Harrison* at ¶ 11, citing *Burnside* at ¶ 8. A reviewing court must consider the trial court's legal conclusions de novo. *State v. Oliver,* 10th Dist. No. 21AP-449, 2023-Ohio-1550, ¶ 36, citing *State v. Banks-Harvey,* 152 Ohio St.3d 368, 2018-Ohio-201, ¶ 14, citing *Burnside* at ¶ 8.

IV. Legal Analysis

A. R.C. 2935.23

{¶ 21} The state first argues that the trial court erred by finding that the absence of sworn testimony regarding the contents of the investigative subpoena requires suppression of evidence under R.C. 2935.23.

{¶ 22} R.C. 2935.23 governs the issuance of subpoenas employed in felony investigations. R.C. 2935.23 directs that the state may cause a subpoena to be issued "for any person to give information concerning such felony. The subpoenas shall require the witness to appear forthwith. * * * He shall then be sworn and be examined under oath by the prosecuting attorney, or the court or magistrate, subject to the constitutional rights of the witness." Here, the subpoenas at issue state that the entity "can comply with this Investigative Subpoena without the court appearance * * * by providing the requested information * * * prior to the date scheduled for the appearance." (State's Ex. A-1 through A-7.) The language employed in each of the investigative subpoenas—permitting

the subpoenaed third-party to provide the requested information in lieu of appearing in court—conflict with the plain language of R.C. 2935.23. There is no excuse for law enforcement's failure to comply with such an explicit statutory provision.

{¶ 23} While we agree with the trial court that the subpoenas do not reflect the mandatory appearance requirement provided in R.C. 2935.23, the remedy sought by Mr. Diaw, *i.e.*, suppression of the evidence, is not available in this instance. The Supreme Court of Ohio has held that the exclusionary rule is generally reserved for violations of a constitutional nature. *State v. Campbell, 170* Ohio St.3d 278, 2022-Ohio-3626, ¶ 22, citing *Kettering v. Hollen,* 64 Ohio St.2d 232, 234 (1980). *Accord State v. Emerson,* 134 Ohio St.3d 191, 2012-Ohio-5047, ¶ 32; *State v. Jones,* 121 Ohio St.3d 103, 2009-Ohio-316, ¶ 15 (finding "a violation of a state statute, * * * in and of itself, [does not] give rise to a Fourth Amendment violation and result in the suppression of evidence"). Thus, absent a "'legislative mandate requiring the application of the exclusionary rule,'" suppression of the evidence is reserved for constitutional violations. *Campbell* at ¶ 22, quoting *Kettering* at 234. Our review of R.C. 2935.23 reveals no express mandate to impose the exclusionary rule for a violation of the statute. *Compare* R.C. 2933.63(A) (permitting, among other remedies, the suppression of evidence derived from an unlawful wiretap). Accordingly, absent an express legislative directive, we are not permitted to impose the exclusion of evidence in this instance as an available remedy for noncompliance with the statute.

{¶ 24} This court addressed this exact question in *State v. Fielding,* 10th Dist. No. 13AP-654, 2014-Ohio-

3105, ¶ 18-19 (rejecting the argument that evidence obtained from a R.C. 2935.23 investigative subpoena should be suppressed because AT&T failed to appear to testify under oath). At least one other Ohio district court has also concluded that suppression is not an available remedy under R.C. 2935.23. *See, e.g., State v. Hamrick,* 12th Dist. No. CA2011-01-002, 2011-Ohio-5357, ¶ 15-16; *State v. Lemasters,* 12th Dist. No. CA-2012-12-028, 2013-Ohio-2969. Thus, the trial court erred concluding that the absence of sworn testimony regarding the contents of the investigative subpoena warranted the suppression of evidence under R.C. 2935.23.

B. Investigative Subpoena

{¶ 25} We turn to Mr. Diaw's next argument that the investigative subpoenas were impermissibly broad. Mr. Diaw focuses his argument on the language employed in the Letgo subpoena that requested, among other specific information, "any and all records."

{¶ 26} While distinct in their analyses, subpoenas, like search warrants, can implicate an individual's Fourth Amendment rights. *United States v. Bigi,* S.D.Ohio No. 3:09-CR-153, 2010 U.S. Dist. LEXIS 105954, *14 (Sept. 22, 2010). Indeed, when it comes to a search warrant or an investigative subpoena, an individual has "[t]he right to be let alone-the most comprehensive of rights and the most valued by civilized men is not confined literally to search and seizures as such, but extends as well to the orderly taking under compulsion of process." (Internal citation and quotations omitted.) *United States v. Morton Salt, Co.,* 338 U.S. 632, 651-52 (1950. Whereas the issuance of a search warrant requires a showing of probable cause, a subpoena is analyzed only under the Fourth

Amendment's general reasonableness standard. *Doe v. United States (In re Adm. Subpoena), 253 F.3d* 256, 264 (6th Cir.2001), citing *In re Subpoena Duces Tecum,* 228 F.3d 341, 347 (4th Cir.2000); *Hale v. Henkel,* 201 U.S. 43, 76, *77* (1906). A subpoena complies with the Fourth Amendment's reasonableness standard when "it is [1] sufficiently limited in scope, [2] relevant in purpose, and [3] specific in directive so that compliance will not be unreasonably burdensome." (Internal citation and quotations omitted.) *Carpenter v. United States, 585* U.S. 296, 330 (2018). However, individuals with "no meaningful interests in the records sought by a subpoena" have no rights to object to a third-party's disclosure of the records. *Id.*

{¶ 27} In the present case, while the requested information in the Letgo subpoena was relevant in purpose to the investigation, the scope of the subpoena was exceedingly broad. The investigative subpoena to Letgo can best be read in two parts: (1) a request for "any and all records" and (2) a demand for specific pieces of information "including all names, addresses, phone numbers, I.P. addresses and email addresses * * * between the dates of 02-16-2020 through 02-18-2020." (State's Ex. A-1.) While the latter portion of subpoena was narrowly tailored—explicitly requesting the name, email address, and IP address associated with the account within a three-day period—the former provision amounts to a broad demand for "any and all records." The initial all-encompassing demand for records is distinct from the subsequent particularized request and is devoid of any limiting language to govern its scope.

{¶ 28} The state contends that the Letgo subpoena was temporally limited. While it is true that a temporal

period between February 16, 2020 through February 18, 2020 was provided in the investigative subpoena, the limiting language was in reference to the second particularized request and was subsequent to the initial broad demand for "any and all records." The record bears this out as it appears Letgo interpreted the subpoena to require production of information outside the identified period. In response to the subpoena, Letgo provided the "first_seen.ios" dated February 11, 2020 and the "last_seen.ios" on February 21, 2020. These dates are plainly outside the temporal period identified in the subpoena.

{¶ 29} While the record is foggy as to date of the single coordinate, identified in the production as "last_latitude.ios" and "last_longitude.ios," based on Sturgill's own testimony, we can surmise that it could have also reasonably fallen outside the temporal period. According to Sturgill the latitude and longitude "would track [the] last time [Mr. Diaw] logged into Letgo, and it would have hit his location he was at from there at the time he logged into that site." (Tr. at 75.) If Sturgill is correct, the coordinates would have been captured on the date that corresponds with "last_seen. ios," February 21, 2020. Given linguistic construction the investigative subpoena, as well as the evidence provided, the state's argument that the subpoena was temporally limited is without merit.

{¶ 30} The state also contends that location information was never expressly requested in any of the investigative subpoenas. We find this argument equally unavailing. While it is true location data was not expressly requested, the open-ended nature of the demand for "any and all records" failed to provide any types of guardrails as to the scope of the request. To

make matters worse, Sturgill acknowledged the subpoena was drafted to be open-ended and appeared wholly indifferent towards his duty to narrowly tailor the investigative subpoena's demand for production. When asked about the breath of the "any and all records" request, Sturgill stated, "if I don't put any at all, they'll only give me–they'll only give me just what I specifically spell out. So if–any information they give me, absolutely, I'll take it. Yes." (Tr. at 53-54.) There is no doubt that Sturgill wanted to make the subpoenas, particularly the Letgo subpoena, as open-ended as possible and welcomed any information he failed to identify in the request.

{¶ 31} This court has previously addressed a similar issue concerning the use of "any and all" language in a search warrant. *See State v. Shaskus,* 10th Dist. No. 14AP-812, 2016-Ohio-7942, In *Shaskus,* law enforcement issued a search warrant to Yahoo concerning "any and all emails" in the defendant's account. *Id.* at ¶ 40. The defendant moved to suppress the evidence gathered from the warrant claiming it was overly broad and not temporally limited. *Id.* at ¶ 40. While the trial court granted the motion to suppress, we reversed finding that the warrant "contained sufficient subject-matter limitations to satisfy the particularity requirement." (Internal citation omitted.) *Id.* at ¶ 50. Here, unlike the search warrant in *Shaskus,* the Letgo subpoena failed to provide any type of subject-matter limitation in the first part of the subpoena. The Letgo investigative subpoena first sought any information associated with the account and a second, particularized request for subscriber information within the relevant three-day period.

{¶ 32} While the Letgo investigative subpoena was impermissibly broad, an illegal search only violates the rights of those that have a "'legitimate expectation of privacy in the invaded place.'" *Bigi* at 15, quoting *Rakas v. Illinois,* 439 U.S. 128, 134 (1978). When an individual has no reasonable expectation of privacy over information provided to a third party, "Fourth Amendment protections are not implicated because a search does not occur." *Fielding* at ¶ 16. Accordingly, in order to warrant Fourth Amendment protections, a defendant must have a legitimate expectation of privacy attached to the records turned over to the third party. *United States v. Miller,* 425 U.S. 435, 444 (1976). The question becomes whether Mr. Diaw had a reasonable expectation of privacy over the information obtained through the Letgo investigative subpoena.

C. Third-Party Doctrine

{¶ 33} The Fourth Amendment to the United States Constitution, as made applicable to the states through the Fourteenth Amendment, and Article One, Section 14 of the Ohio Constitution, protect individuals against unreasonable searches and seizures. *Banks-Harvey* at ¶ 15-17, citing *United States v. Ross*, 456 U.S. 798, 825 (1982); *State v. Jones,* 143 Ohio St.3d 266, 2015-Ohio-483, ¶ 12. These safeguards offer a restraint on the government and, more specifically, law enforcement, to protect an individual's privacy interests and security from arbitrary invasions by government officials. *State v. Rogers,* 10th Dist. No. 21AP-546, 2023-Ohio-2749, ¶ 13, citing *Camara v. Mun. Court of San Francisco,* 387 U.S. 523, 528 (1967); Iv*ery* at ¶ 34, citing *Banks-Harvey* at ¶ 17. "The Fourth Amendment protects privacy interests within the reasonable expectation of privacy. That is, '[w]hen an individual "seeks to pre-

serve [something] as private,'" * * * and 'his expectation of privacy is "one that society is prepared to recognize as reasonable."'" *State v. Jackson,* 171 Ohio St.3d 412, 2022-Ohio-4365, ¶ 58, quoting *Carpenter* at 304, quoting *Katz v. United States,* 389 U.S. 347, 351 (1967); *Carpenter* at 343, quoting *Katz* at 361 (Harlan, J. concurring).

{¶ 34} Outside several well-established exceptions, warrantless searches are per se unreasonable. *Robertson* at ¶ 15, citing *Los Angeles v. Patel,* 576 U.S. 409, 419 (2015), citing *Arizona v. Gant*, 556 U.S. 332, 338 (2009). The Supreme Court has recognized one such exception under the third-party doctrine. Under the doctrine, the Fourth Amendment generally does not preclude the government from obtaining information voluntarily provided to a third party. *State v. Rogers,* 10th Dist. No. 21AP-546, 2023-Ohio-2749, ¶14, citing *Smith v. Maryland,* 442 U.S. 735, 743-44 (1979) (finding law enforcement's use of a pen register to capture telephone numbers dialed by the defendant's telephone did not constitute a search under the Fourth Amendment as there was no expectation of privacy when the information was voluntarily turned over to a third party, the telephone company); *Miller* at 443 (finding a financial institution's disclosure of bank records with law enforcement, in response to a subpoena, did not constitute a search under the Fourth Amendment). Under these circumstances, "the Government is typically free to obtain such information from the recipient without triggering Fourth Amendment protections." *Carpenter* at 308.

{¶ 35} As a check on improper warrantless searches, United States Supreme Court created the exclusionary rule, which bars the use of evidence

obtained in violation of the Fourth Amendment in a criminal proceeding. *Davis v. United States,* 564 U.S. 229, 236 (2011), citing *Elkins v. United States,* 364 U.S. 206, 217 (1960). Not only is the initial evidence obtained in violation of the Fourth Amendment from an unconstitutional search excluded but the derivative evidence obtained by exploitation of the illegal search, often referred to as "fruit of the poisonous tree," must also be suppressed. *Wong Sun v. United States, 371* U.S. 471, 484-89 (1963); *Banks-Harvey* at ¶ 25.

{¶ 36} Based upon the information provided by K.W, Sturgill sent a series of investigative subpoenas to various third parties. The following categories of information were obtained in response to the investigative subpoenas: names, addresses, email addresses, IP addresses, and a single latitude and longitude data point. We will consider each type of information in turn.

1. Subscriber Information

{¶ 37} The term "subscriber information" has been applied to basic identifying information that an individual provides to a third party in order to receive services. In an online context, this court has defined "[s]ubscriber information, such as name, address, and phone number, [a]s information that the customer provides to the internet service provider in order to receive internet service." *State v. Thornton,* 10th Dist. No. 09AP-108, 2009-Ohio-5125, ¶13. Federal courts have similarly defined "[s]ubscriber information" to "include the name, address, and other identifying information for the person to whom the phone number is registered." *United State v. Beverly,* 943 F.3d 225, 231 (5th Cir.2019) fn. 2. The Electronic Communications

Privacy Act, 18 U.S.C.S. 2703(c)(2), directs that "[a] provider of electronic communication service or remote computing service," upon receiving an authorized administrative subpoena, shall disclose the following subscriber information: name; address; local and long distance telephone connections records, or records of session times and durations; length of service and types of service utilized; telephone or instrument number or other subscriber number or identity; and means and source of payment for such service (including any credit card or bank account number).[2] For our purposes, however, we need not examine the distinctions in these definitions as the information at issue—name, address, and email address—falls squarely within the general category of subscriber information.

---

[2] Other states have classified similar material as "subscriber information." *See, e.g.,* California Electronic Communications Privacy Act ("CalECPA"), codified as Cal.Penal Code 1546, et seq. (defining "subscriber information" as "the name, street address, telephone number, email address, or similar contact information provided by the subscriber to the service provider to establish or maintain an account or communication channel, a subscriber or account number or identifier, the length of service, and the types of services used by a user of or subscriber to a service provider."). The statute provides a property right in digitally stored content and online accounts like photographs, text messages, postings, spread sheets, email, etc. The statute "mandates a warrant for state law enforcement access to any CSLI, as well as metadata and information stored on a device or in the cloud." Matthew G. Baker, *The Third Party Doctrine and Physical Location: The Privacy Implications of Warrantless Acquisition of Historical Cell Site Location Information,* 66 Cath.U.L.Rev. 667, 680 (2017). Such state statutes are informative of what the citizens of each state are willing to accept as reasonable. *Id.* Ohio, however, has no such statute at this time.

{¶ 38} Prior to *Carpenter,* federal circuit courts had universally found that an individual had no reasonable expectation of privacy over subscriber information that they provided in their ordinary use of the Internet. *See United States v. Trader,* 981 F.3d 961, 968 (11th Cir.2020), citing *United States v. Weast,* 811 F.3d 743, 747-48 (5th Cir.2016); *United States v. Caira,* 833 F.3d 803, 806-09 (7th Cir.2016); *United States v. Wheelock,* 772 F.3d 825, 828-29 (8th Cir.2014); *United States v. Perrine,* 518 F.3d 1196, 1204-05 (10th Cir.2008); *United States v. Christie,* 624 F.3d 558, 573-74 (3d Cir.2010); *United States v. Bynum,* 604 F.3d 161, 164 (4th Cir.2010). *See also Guest v. Leis,* 255 F.3d 325, 336 (6th Cir.2001) (finding that "computer users do not have a legitimate expectation of privacy in their subscriber information because they have conveyed it to another person-the system operator."). While *Carpenter* has modified the third-party analysis, *see infra* ¶ 47-53, federal circuit courts have continued to reach the same result when it comes to the disclosure of subscriber information to third parties. *See United States v. Whipple,* 92 F.4th 605, 611-12 (6th Cir.2024); *Trader* at 968, citing *United States v. Morel,* 922 F.3d 1, 9 (1st Cir.2019); *United States v. Contreras,* 905 F.3d 853, 857 (5th Cir.2018); *United States v. Wellbeloved-Stone,* 777 Fed.Appx. 605, 607 (4th Cir.2019); *United States v. VanDyck,* 776 Fed.Appx. 495, 496 (9th Cir.2019); *see also Beverly* at 239.

{¶ 39} Ohio courts, including this one, have also found there are no Fourth Amendment protections afforded to the disclosure of subscriber information to third parties. *See, e.g., Fielding* at ¶ 17, citing *Thornton* at ¶ 14 ("a customer does not have a reasonable expectation of privacy in subscriber information given

to an internet service provider"); *see also Hamrick* at ¶ 18 (finding appellant had no reasonable expectation of privacy over his subscriber information obtained by law enforcement from Time Warner Cable); *Lemasters* at ¶ 9 (finding defendant had no reasonable expectation of privacy over subscriber information obtained by the police from his internet service provider). Given the breath of federal and Ohio courts that have addressed this question, we conclude Mr. Diaw had no reasonable expectation of privacy over the disclosure of his subscriber information and, therefore, cannot establish a Fourth Amendment violation.

{¶ 40} Mr. Diaw asks us to apply the analysis in *Riley v. California,* 573 U.S. 373 (2014), which held that law enforcement generally must obtain a warrant prior to searching the digital contents of a cellphone as incident to a defendant's arrest. The *Riley* court recognized that cellphones hold "the privacies of life[]" and "[t]he fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought." (Internal citations omitted.) *Riley* at 403. However, unlike a search of the contents of an individual's cellphone, when a defendant provides subscriber information to an internet or telephone company, they assume the risk of the companies disclosing that information to law enforcement. *Wellbeloved-Stone* at 607, citing *Bynum* at 164. As such, an individual has no subjective expectation of privacy in the subscriber information as it was voluntarily conveyed to the company. *Id.; see also United States v. McClain,* W.D.N.Y. No. 19-CR-40A, 2019 U.S. Dist. LEXIS 229688, *15 (Dec. 9, 2019) (finding subscriber

information "certainly does not fall in the category of information addressed in *Carpenter* and *Riley*").

2. Internet Protocol ("IP") Address

{¶ 41} An IP address is a "string of numbers associated with a device that had, at one time, accessed a wireless network." *United States v. Hood,* 920 F.3d 87, 92 (1st Cir.2019). An IP address identifies the location, not necessarily the user, where a device accessed the internet. *United States v. Jenkins,* N.D.Ga. No. 1:18-CR-00181, 2019 U.S. Dist. LEXIS 62776, *11 (Apr. 11, 2019).

{¶ 42} Federal circuit courts have universally found a defendant has no expectation of privacy over an IP address as the user "'should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information." *United States v. Rosenow,* 50 F.4th 715, 738 (9th Cir.2022), quoting *United States v. Forrester,* 512 F.2d 500, 510 (9th Cir.2008). *See also Morel* at 8-9; *United States v. Suing,* 712 F.3d 1209, 1213 (8th Cir. 2013); *Christie* at 573. Courts have compared an IP address to a telephone number associated with a landline or information associated with an individual's residence. *See United States v. Soybel*, 13 F.4th 584, 587 (7th Cir.2021) ("[defendant] has no expectation of privacy in the captured [IP] routing information, any more than the numbers he might dial from a landline telephone"). The *Rosenow* court analogized an IP address to information an individual would put on the outside of mail, "which the Supreme Court has long held can be searched without a warrant because it is voluntarily transmitted to third parties; therefore, there is no legitimate expectation of privacy in such

information." (Internal citation and quotation omitted.) *Rosenow* at 738. Unlike individual location data or the substance of a communication, an IP address is associated with an individual's residence or other location where an individual accesses the internet; it does not concern a person's daily movements. *Contreras* at 857. Conversely, the search of the contents of email messages and other private communications, which are comparable to the contents of a sealed letter, generally requires a warrant. *Rosenow* at 738, citing *Forrester* at 511.

{¶ 43} This court's prior decisions, which rejected the argument that a third-party disclosure of an IP address warrants Fourth Amendment protections align with federal precedent. *See, e.g., Fielding* at ¶ 19; *Thornton* at ¶ 12 (finding the defendant had no reasonable expectation of privacy in the IP address associated with his computer); *see also Lemasters* at ¶ 9; *Hamrick* at ¶ 19.

{¶ 44} As both federal and Ohio courts have overwhelmingly found there is no reasonable expectation of privacy on an IP address, Mr. Diaw is not afforded Fourth Amendment protections based on the third-party disclosure of the information to law enforcement in response to the Letgo investigative subpoena.

3. Latitude and Longitude

a. Pre-Carpenter Analysis of Location Data

{¶ 45} While the analysis regarding whether an IP address and subscriber information are afforded Fourth Amendment protections under third-party doctrine is fairly straightforward, the third-party disclosure

of the latitude and longitude data point is more complex.

{¶ 46} Prior to *Carpenter,* federal circuit courts had held that an individual does not have a reasonable expectation of privacy over location data as it fell within established third-party-doctrine analysis. *See, e.g., United States v. Thompson,* 866 F.3d 1149, 1156, 1160 (10th Cir.2017); *United States v. Graham,* 824 F.3d 421, 426 (4th Cir.2016) (en banc); *United States v. Davis,* 785 F.3d 498, 511 (11th Cir.2015) (en banc) (holding that defendant has no "objective[ly] reasonable expectation of privacy in MetroPCS's business records showing the cell tower locations that wirelessly connected his calls"); *In re Application of the United States for Historical Cell Site Data,* 724 F.3d 600, 616 (5th Cir.2013) (finding cell site data is not afforded Fourth Amendment protections); *In re U.S. for an Order Directing Provider of Electronic Communication Serv. to Disclose Records to Govt.,* 620 F.3d 304, 313, 317 (3d Cir.2010). This court had reached a similar conclusion. *See, e.g., State v. Jones,* 10th Dist. No. 18AP-33, 2019-Ohio-2134, ¶ 46 ("At the time, [cell-site location information ("CSLI")][3] was attainable pursuant

---

[3] The *Carpenter* court described CSLI as follows:

> Cell phones continuously scan their environment looking for the best signal, which generally comes from the closest cell site. Most modern devices, such as smartphones, tap into the wireless network several times a minute whenever their signal is on, even if the owner is not using one of the phone's features. Each time the phone connects to a cell site, it generates a time-stamped record known as cell-site location information ("CSLI"). The precision of this information depends on the size of the geographic area covered by the cell site. The greater the

to a court order.") Thus, an individual's location data could be distributed at the discretion of the third-party service provider without implicating Fourth Amendment protections. The third-party doctrine analysis, however, shifted after the United States Supreme Court's decision in *Carpenter*. A brief review is instructive.

b. Carpenter

{¶ 47} In 2011, law enforcement suspected that Timothy Carpenter was involved in several robberies around Detroit. *Id.* at 301. Law enforcement initially arrested several other suspects, one of which confessed to being involved in nine robberies in Michigan and Ohio. *Id.* The same suspect identified Carpenter as someone involved in the heists and provided the FBI with various telephone numbers. *Id.* The state applied for court orders, pursuant to the Stored Communications Act, which directed two wireless carriers to disclose Carpenter's historical cell site information for the four months that the robberies took place. *Id.* at 302. The Stored Communications Act allowed the state to obtain a court order upon offering "specific and articulable facts" that demonstrated "reasonable grounds" to believe the records were "relevant and material to an ongoing criminal investigation." 18 U.S.C.S. 2703(d). "Altogether the Government obtained 12,898 location points cataloging Carpenter's

---

> concentration of cell sites, the smaller the coverage area. As data usage from cell phones has increased, wireless carriers have installed more cell sites to handle the traffic. That has led to increasingly compact coverage areas, especially in urban areas.

Carpenter at 300-01.

movements—an average of 101 data points per day." *Carpenter* at 302. Based on the cell-site data, Carpenter was charged with multiple counts of robbery and carrying a firearm during a federal crime of violence. *Id.* Carpenter moved to suppress the evidence arguing that his Fourth Amendment rights were violated when the state seized his CSLI from the wireless carriers without a valid warrant. *Id.* The district court denied the motion, and Carpenter was later convicted at trial. *Id.* at 302-03.

{¶ 48} On appeal, the Sixth Circuit Court of Appeals affirmed the district court's decision to deny the motion to suppress finding Carpenter had no reasonable expectation of privacy over the data as he had voluntarily disclosed the information to the cellphone carriers and, therefore, he was not entitled to Fourth Amendment protections. *Id.* at 303. The Supreme Court granted certiorari. *Id.*

{¶ 49} On June 22, 2018, the Supreme Court, by a 5-4 decision, reversed and remanded the judgment. Chief Justice Roberts, joined by Justices Breyer, Ginsburg, Kagan, and Sotomayor delivered the opinion of the Court.

{¶ 50} The question before the Court was "whether the Government conducts a search under the Fourth Amendment when it accesses historical cellphone records that provides a comprehensive chronicle of the user's past movements." *Id.* at 300. The Court considered "how to apply the Fourth Amendment to a new phenomenon: the ability to chronicle a person's past movements through the record of his cell phone signals." *Id.* at 309.

{¶ 51} The Court held that law enforcement's acquisition of CSLI data in this case constituted a search under the Fourth Amendment, and the state must generally obtain a warrant supported by probable cause before acquiring such records. *Id.* at 316. The majority opinion likened the "all-encompassing record of the holder's whereabouts" to *United States v. Jones*, 565 U.S. 400, 405 (2012)[4] and noted that the data was "detailed, encyclopedic, and effortlessly compiled." *Id.* at 309, 311. The Court explained that while the data was collected for business purposes, and owned by the cellphone provider, "individuals have a reasonable expectation of privacy [concerning] the whole of their physical movements." *Id.* at 310. Despite the information being voluntarily provided to cellphone companies, the only way to prevent the collection of the cellphone data is to disconnect oneself from the network. *Id.* at 315. "[A person's cellphone] faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales." *Id.* at 311.

{¶ 52} The *Carpenter* court makes clear that the state can no longer assert the third-party doctrine "mechanically appl[ies]" when an individual shares information to a third party. *Id.* at 314. "In light of the

---

[4] In *Jones,* the Supreme Court considered whether the state conducted a search under the Fourth Amendment when it attached a GPS device to a defendant's vehicle in order to track the vehicle's movements during a 28-day period. The *Jones* court found the state's actions amounted to a search as "[t]he government physically occupied private property for the purpose of obtaining information" by installing a tracking device and then monitoring the vehicle's movements. *Id.* at 404.

deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection." *Id.* at 320. The majority, however, emphasized that *Carpenter* should be viewed narrowly and does not dispute the application of other third-party doctrine cases "or call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information." *Id.* at 316.

c. *Post-Carpenter* Analysis of Location Data

{¶ 53} While the decision was initially hailed as groundbreaking[5], courts have struggled to apply *Carpenter* as it failed to set out a clear test for determining when information disclosed to a third party is protected by the Fourth Amendment. Matthew Tokson, *The Carpenter Test as A Transformation of Fourth Amendment Law,* 2023 U.Ill.L.Rev. 507, 517 (2023). As noted in *Carpenter,* there is "no single rubric [that] definitively resolves which expectations of privacy are entitled to protection." *Carpenter* at 304. The *Carpenter* court did, however, identify several factors to consider as part of its analysis. Among the considerations discussed were "the revealing nature of location data, the amount of data collected, the number of people affected, the inescapable and automatic nature of the data disclosure, and the low cost of

---

[5] *See* Matthew Tokson, *The Aftermath of Carpenter: An Empirical Study of the Fourth Amendment Law, 2018-2021*+,135 Harv.L.Rev. 1790,1792-93 (2002).

tracking people via their cell phone." Tokson, 135 Harv.L.Rev. at 1792. While other factors remain viable points to examine the nature of the third-party disclosure, three factors "drive" the analysis: "(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." Tokson, 2023 U.Ill.L.Rev. at 510; Tokson, 135 Harv.L.Rev. at 1851.

1. Revealing Nature

{¶ 54} The first factor concerns the revealing nature of the data collected. The *Carpenter* court noted that certain information, such as location data, possess a higher risk of providing an "intimate window into a person's life, revealing not only his particular movements, but through them his 'familiar, political, professional, religious, and sexual associations.'" *Carpenter* at 311, quoting *Jones, 565* U.S. at 415 (Sotomayor, J., concurring). The heart of the concern centers on the disclosure of sensitive information regarding a person's life to agents of the state. Tokson, 2023 U.Ill.L.Rev. at 529. "Such data may be used for illegitimate purposes, give state agents undue power over a citizen, cause substantial privacy harms to data subjects, or simply compromise the security promised by the Fourth Amendment." *Id.* at 529-30.

{¶ 55} There are numerous examples of courts finding law enforcement's use of location information, including a single data point, constituted a search under the Fourth Amendment based, in large part, on the revealing nature of the information. *See, e.g., Commonwealth v. Pacheco,* 263 A.3d 626 (Pa.2021) (finding defendant had a legitimate expectation of

privacy over 108 days of continuous real-time location information); *Commonwealth v. Almonor,* 482 Mass. 35 (2019). In *Almonor,* the murder suspect was found in a residence after law enforcement contacted his cell company to reveal his real-time global positioning system coordinates, *i.e.*, "pinging," which led to the defendant's arrest. *Id.* at 36, 44. The Massachusetts Supreme Court found that "society reasonably expects that the police will not be able to secretly manipulate our personal cell phones for any purpose, let alone for the purpose of transmitting our personal location data." *Id.* at 44. While *Almonor* found that the defendant had a reasonable expectation of privacy in the real-time location of his cellphone, it held that exigent circumstances precluded suppression of the evidence as law enforcement "had reasonable grounds to believe that obtaining a warrant would be impracticable because taking the time to do so would have posed a significant risk that the suspect may flee, evidence may be destroyed, or the safety of the police or others may be endangered." *Id.* at 52. *See also State v. Muhammad,* 194 Wn.2d 577 (Wa.2019) (finding that while the "ping" of the defendant's cellphone was a search under the Fourth Amendment, it was permissible based on exigent circumstances).

{¶ 56} At least one Ohio appellate court has reached the same conclusion. *See, e.g., State v. Gause,* 2d Dist. No. 29162, 2022-Ohio-2168, ¶ 19-20 (concluding that exigent circumstances existed justifying the warrantless pinging of the defendant's cellphone as the suspect was armed and had fled the scene of the crime); *State v. Davison,* 2d Dist. No. 28579, 2021-Ohio-728, ¶ 10-11 (finding exigent circumstances, as well as the good-faith exception, warranted the pinging

of the fleeing suspect's cellphone during the morning of the shooting); *State v. Snowden,* 2d Dist. No. 28096, 2019-Ohio-3006, ¶ 37-40 (finding that while pinging defendant's cellphone the night of the shooting and subsequent day, without a warrant, violated his Fourth Amendment rights, such evidence need not be suppressed as exigent circumstances and the good-faith exception were applicable).

{¶ 57} While courts have taken varying approaches to analyzing real-time location information under *Carpenter,* they have concluded that when exigent circumstances are present, suppression of the evidence is not warranted. *See, e.g., In re Taylor,* 6th Cir. No. 22-3553, 2022 U.S. App. LEXIS 30976 (Nov. 8, 2022) (denying order authorizing the district court to consider a second petition for a writ of habeas corpus as the state was absolved of any obligation to obtain a search warrant for his real-time CSLI information based on exigent circumstances); *State v. Martin,* 8th Dist. No. 108189, 2019-Ohio-4463, ¶ 15-16 (finding *Carpenter* inapplicable as the use of real-time cellphone location information was not used as evidence but a means to locate the suspect once a warrant was issued for the defendant's arrest).

{¶ 58} While the latitude and longitude data point is the type of information that possess some of the biggest privacy concerns, there are reasons to believe that it is less revealing under the facts of this case. First, the coordinate was historical in nature and not a real-time location. Unlike cases where law enforcement "ping" a defendant's telephone, the location data in this case was meaningfully removed from Mr. Diaw's actual location. When historical cell-site information, or coordinate in this case, provide a mere snapshot of

Mr. Diaw's location, the revealing nature of the information is limited. Moreover, the actual location of the latitude and longitude data point must be considered. While the coordinate at issue, which corresponds to the McDonald's located on East Broad Street is near Mr. Diaw's apartment, his single movement in a public space is far less revealing than if it corresponded with his actual residence. *See United States v. Hammond,* 996 F.3d 374, 389 (7th Cir.2021) (concluding the use of real-time CSLI for a few hours on public roadways to find armed suspect did not implicate the Fourth Amendment); *United States v. Riley,* 858 F.3d 1012, 1018 (6th Cir.2017) (finding that the use of seven hours of GPS location data to find a suspect for whom a valid search warrant had been issued was not a search "so long as the tracking [did] not reveal movements *within* the home (or hotel room), [did] not cross the sacred threshold of the home."). (Emphasis sic.) Given the single data point was historical in nature and was not associated with Mr. Diaw's residence, we find this factor favors the state's position that the information does not warrant Fourth Amendment protection.

2. Amount

{¶ 59} Next, we consider the amount of data that was collected by law enforcement. In *Carpenter,* the government gathered 12,898 location points over 127 days, or 101 data points per day, which provided a comprehensive chronicle of the defendant's prior movements. *Id.* at 302. "Large amounts of data such as those at issue in *Carpenter* increase the potential for invasions of the target's privacy." Tokson, 2023 U.Ill.L.Rev. at 530. It is difficult to dispute that the 12,898 location points collected in *Carpenter* amount

to an exceedingly high volume of location data. *See also State v. Brown,* 331 Conn. 258 (2019) (finding three months of historical CSLI data, without a warrant, violated the defendant's Fourth Amendment rights). However, even much smaller amounts of location information could constitute as search as *Carpenter* noted that "for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search." *Carpenter* at 310, fn. 3. However, courts are mixed as to whether historical CSLI of less than seven days constitutes a search under the Fourth Amendment. *Compare People v. Edwards,* 63 Misc.3d 827, 828 (N.Y.Sup.Ct.2019) (finding two days of CSLI data was not a search pursuant to Fourth Amendment) *with State v. Gibbs,* S.C. Dist. No. 2020-UP-244, 2020 S.C. App.Unpub. LEXIS 301 (Aug. 19, 2020) (finding five days of historical CSLI data was a search).

{¶ 60} In the instant case, however, law enforcement obtained a single latitude and longitude data point. This is a far cry from the 12,898 location points at issue in *Carpenter* or even the seven days of data the *Carpenter* court noted would warrant Fourth Amendment protections. The limited cases that have applied the *Carpenter* analysis to smaller amounts of historical location information have reached the same conclusion. In *In re Google Location History Litigation,* 428 F.Supp.3d 185, 198 (N.D.Cal.2019), the district court found that the location information collected and stored by Google media fell outside *Carpenter* as "not all of Plaintiff's movements were being collected, only specific movements or locations." (Emphasis omitted.) The *Google* court reasoned that "[s]uch 'bits and pieces' do[es] not meet the standard of privacy estab-

lished in *Carpenter." Id.* While there are several cases that have found *Carpenter* applies to a single location data point, *see supra* ¶ 55-56, those cases concern real-time location information exposing a far more "intimate window into a person's life." *Carpenter* 311.

3. Voluntarily Disclosure

{¶ 61} The third factor concerns whether the location data at issue was voluntarily disclosed. This factor originates from the line of third-party doctrine cases prior to the limitation imposed by *Carpenter*. Tokson, 2023 U.Ill.L.Rev. at 532. "In theory, information that is not voluntarily disclosed to another is more private than information voluntarily disclosed to some other party or parties." *Id.* We must consider whether the disclosure was truly voluntary compared to those that are practically unavoidable. In *Carpenter,* the CSLI data was deemed unavoidable as the information was automatically collected by the cellphone. "Virtually any activity on the phone generates CSLI, including incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates." *Carpenter* at 315. A cellphone is an "inescapable" part of life giving the owner little choice in carrying the device during their daily movements. *Id.* Unlike the CSLI data that was collected from Carpenter through the course of his mere possession of the cellphone, the latitude and longitude data point was voluntarily conveyed through Mr. Diaw's use of Letgo. While this point is somewhat unclear in the record, Mr. Diaw either downloaded the Letgo application on his cellphone or used the Letgo website on a computer. *See* Oct. 5, 2023 Oral Argument 26:11; 28:40. In either case, Mr. Diaw took the affirmative step of

creating an account on the platform and took no steps to avoid disclosure of the location. Unlike the practically unavoidable obligation of carrying a cellphone, the usage of Letgo is certainly not "inescapable" or an essential part of modern life. *Carpenter* at 315, citing *Riley* at 385; *Carpenter* at 320.

{¶ 62} Other courts have found that the voluntary use of certain websites or applications bolstered their finding that there was no reasonable expectation of privacy in the third-party disclosure. In *United States v. Bledsoe,* 630 F.Supp.3d 1 (D.C.2022), the district court found that there was no reasonable expectation of privacy over the location data provided by Facebook to investigators of accounts livestreaming or uploading videos at the United States Capitol on January 6, 2021. "[U]nlike * * * CSLI * * * the only way that Facebook was able to determine when and where a user engaged in account activity on January 6, 2021, is by virtue of the user making an affirmative and voluntary choice to download the Facebook or Instagram application * * * create an account * * * and, critically, take no available steps to avoid disclosing his location." *Id.* at *13. *See also Sanchez v. Los Angeles Dept. of Transp.,* 39 F.4th 548, 559-61 (9th Cir.2022) (finding that the collection of data by the Los Angeles Department of Transportation was not a search, and did not violate the Fourth Amendment, as the plaintiff voluntarily agreed to provide location data to the e-scooter operators every time he rented a device). As was the case in *Bledsoe* and *Sanchez,* Mr. Diaw's use of Letgo was no automatic and inescapable but a voluntary disclosure of his location information.

{¶ 63} Thus, while we agree with the trial court that the Letgo investigative subpoena was imper-

missibly broad, there was no reasonable expectation of privacy over the single coordinate disclosed in the investigative subpoena. *See Bigi* at 17 *(pre-Carpenter* case finding that while the subpoenas were overly broad, defendant had no reasonable expectation of privacy, under the third-party doctrine, over the information). Concerning the scope of the other investigative subpoenas in this case, as the information obtained from the subpoenas fell under the categories of subscriber information or IP address information, we need not examine the particular language of the subpoenas as Mr. Diaw had no reasonable expectation of privacy over the information voluntarily disclosed to the third-party providers. Accordingly, any potential defects in the form and scope of the other investigative subpoenas do not trigger protections under the Fourth Amendment to warrant suppress of the evidence.

D. Remaining arguments

{¶ 64} The state asserts that even if there was a Fourth Amendment violation in this instance, suppression of the evidence was improper under both the inevitability doctrine (Appellant's Brief at 29-30) and the good-faith doctrine (Appellant's Brief at 31-32). Because we find that there was no reasonable expectation of privacy concerning the evidence provided in the investigative subpoenas, we decline to address the remaining arguments. *State v. Williams,* 10th Dist. No. 06AP-842, 2007-Ohio-1015, ¶ 21, citing App.R. 12(A)(1)(c).

{¶ 65} The state's sole assignment of error is sustained.

V. Conclusion

{¶ 66} To be sure, 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. While the state's appeal is meritorious in this instance, it would be well served to cure these issues going forward. Without remedial action, the state operates at its own peril by jeopardizing lawful investigations and risking further injury to the constitutional rights of Ohioans.

{¶ 67} Based on the foregoing, the state's sole assignment of error is sustained. This matter is remanded for further proceeding consistent with this judgment.

Judgment reversed; cause remanded.

BOGGS and EDELSTEIN, JJ., concur.

DECISION AND ENTRY DENYING DEFENDANT'S MOTION TO DISMISS AND GRANTING DEFENDANT'S MOTION TO SUPPRESS EVIDENCE (OCTOBER 3, 2022)

IN THE COURT OF COMMON PLEAS
FRANKLIN COUNTY, OHIO

STATE OF OHIO,

Plaintiff,

v.

MAMADOU DIAW,

Defendant.

Case No. 21CR-379

Before: KIMBERLY COCROFT, Judge.

This matter is before the Court on Defendant's motion to dismiss or, alternatively, to suppress evidence, which was filed on June 14, 2021. Plaintiff, State of Ohio, filed its memorandum contra on June 28, 2021. The Court held an evidentiary hearing on February 24, 2022 and, thereafter, both Plaintiff and Defendant filed post-hearing briefs. This matter is now ripe for decision.

I. Factual Background

In February 2020, Kareema Wafa ("Wafa") attempted to negotiate the purchase of a computer with two men, one of whom was Defendant, through a website called LetGo. As a part of this transaction, Wafa agreed to meet Defendant and the other individual at a Kroger located in Groveport, Franklin County, Ohio so that Wafa could look at and, perhaps, purchase the computer. Wafa brought $360 and an iPhone to effectuate the computer purchase. Upon arriving at the agreed location and after speaking with Defendant, Wafa got in the passenger seat of the car in which Defendant arrived. Wafa alleges that, as he attempted to exchange the money and iPhone for the computer, Defendant pulled the computer away from Wafa and began to punch Wafa in the head and face. Wafa also alleges that the other person in the vehicle pointed a gun at him. Wafa further states the he told Defendant that he wanted out of the car and was let out of the vehicle, after which Wafa alleges Defendant pushed him to the ground and kicked Wafa repeatedly. Wafa was able to provide investigators with the last four digits of the vehicle license plate number but no registration records were found.

After the incident occurred, investigators prepared and issued numerous investigative subpoenas on various digital account providers, including but not limited to, LetGo in order to gather "any and all records" suspected to be associated with the LetGo account in issue. Although investigators obtained the signature of Franklin County Municipal Court Judges, the documents were labeled as investigative subpoenas and not search warrants. Moreover, except for one subpoena, no affidavits in support of probable cause

were attached. With the subpoenas, investigators requested and received information from several data companies. During the evidentiary hearing, Det. Sturgill, who is the lead investigator for this matter, testified that, as a part of his subpoena request for "any and all records" from LetGo, he received GPS data relating to the location of Defendant. Further, Det. Sturgill testified that the information from LetGo was the first real lead in the case and that the information gained through the LetGo subpoena allowed law enforcement to develop additional information regarding Defendant's residence, driver's license and registration records, which then led to the identification of Defendant as a suspect.

Defendant argues that he had a genuine expectation of privacy regarding his online accounts and the information included therein and, as such, a search warrant would be necessary to access and review the accounts. Additionally, Defendant argues that evidence gathered through the investigative subpoenas was the result of the illegal search of Defendant's GPS/location data, digital data and account information and relied improperly on R.C. 2935.23 which authorizes the issuance of a subpoena to obtain witness testimony in a felony investigation but not the collection of data or documents. Conversely, Plaintiff contends a search warrant was unnecessary to access Defendant's online accounts and data and that investigators relied correctly on the authority of R.C. 2953.23 in issuing the investigative subpoenas, since the plain language of the statute does not require an affidavit in support of probable cause.

II. Argument and Analysis

R.C. 2935.23, which governs the issuance of investigative subpoenas states:

> After a felony has been committed, and before any arrest has been made, the prosecuting attorney of the county, or any judge or magistrate, may cause subpoenas to issue, returnable before any court or magistrate, for any person to give information concerning such felony. The subpoenas shall require the witness to appear forthwith. Before such witness is required to give any information. he must be informed of the purpose of the inquiry, and that he is required to tell the truth concerning the same. He shall then be sworn and be examined under oath by the prosecuting attorney, or the court or magistrate, subject to the constitutional rights of the witness. Such examination shall be taken in writing in any form, and shall be filed with the court or magistrate taking the testimony. Witness fees shall be paid to such persons as in other cases.

(Emphasis added.) While the investigative subpoenas issued in this case state that an entity "can comply with this Investigative Subpoena without the court appearance scheduled below (***)", the plain language of the statutory provision contemplates that a witness "shall" appear. In this instance, no witness appeared. In that regard, there is no compliance with mandated statutory requirements for the issuance of investigative subpoenas. Moreover, this provision does not cover a subpoena duces tecum by which documents could be submitted without testimony under oath. While Plain-

tiff argues that this provision should be read in concert with Crim R. 17, there is no such requirement contemplated in the plain language of the statute. On this basis, alone, the Court could find and does find that any information derived from the investigative subpoenas should be suppressed. Since, however, both Plaintiff and Defendant focus their arguments primarily on Fourth Amendment considerations, the Court will evaluate whether there was conformance with constitutional mandates regarding this investigation.

The Fourth Amendment provides protection against a subpoena too sweeping in its terms "to be regarded as reasonable." *Hale v. Henkel,* 201 U.S. 43, 76, 26 S.Ct. 370, 380 (1906). In the present case, seven investigative subpoenas were issued to various providers, seeking "any and all records" pertaining to a customer with certain identifying information. The "any and all records" and information included, but was not limited to "names, phone numbers, Facebook account names, email addresses, incoming and outgoing calls and I.P. addresses." Further, Det. Sturgill testified, "[I]n a way, it's like if I don't put any and all, they'll give me — they'll only give me just what I specifically spell out. So if — any information they give me, absolutely, I'll take it", and confirmed that he did not want to limit the records that would be sent through investigative subpoenas.

In the *Henkel* case, however, the Court found the investigative subpoena far too sweeping to be regarded as reasonable and noted, "It does not require the production of a single contract, or of contracts with a particular corporation, or a limited number of documents, but all understandings, contracts, or correspondence between the MacAndrews & Forbes Company,

and no less than six different companies, as well as all reports made and accounts rendered by such companies from the date of the organization of the MacAndrews & Forbes Company." *Id.* At 76. In the present case, the lead investigator issued seven investigative subpoenas to six different companies and requested "any and all records" pertaining to a certain customer and admits that he did not want to put parameters on his request so that he would obtain as much information as the entities subject to subpoena were willing to provide voluntarily. Given the conclusion reached in *Henkel,* this Court also finds the expanse of the companies subpoenaed and the scope of information requested too sweeping to be reasonable.

Even assuming this Court found the scope and breadth of the investigative subpoenas to be reasonable for purposes of analysis under either the U.S. or Ohio Constitution, which it does not, the Court still finds that the investigative subpoenas do not satisfy the requirements of the Fourth Amendment to the U.S. Constitution or Art. 1, Sec. 14 of the Ohio Constitution.

In *State v. Moore* 90 Ohio St.3d 47, 48-49 (2000), the Ohio Supreme Court wrote:

> The Fourth Amendment to the United States Constitution, as applied to the states through the Fourteenth Amendment, provides, "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 place to be searched, and the persons or things to be seized." Section 14,

> Article I of the Ohio Constitution, nearly identical to its federal counterpart, likewise prohibits unreasonable searches. *State v. Kinney* (1998), 83 Ohio St.3d 85, 87, 698 N.E.2d 49, 51.
>
> For a search or seizure to be reasonable under the Fourth Amendment, it must be based upon probable cause and executed pursuant to a warrant. *Katz v. United States* (1967), 389 U.S. 347, 357, 88 S.Ct. 507, 514, 19 L.Ed.2d 576, 585; *State v. Brown* (1992), 63 Ohio St.3d 349, 350, 588 N.E.2d 113, 114. This requires a two-step analysis. First, there must be probable cause. If probable cause exists, then a search warrant must be obtained unless an exception to the warrant requirement applies. If the state fails to satisfy either step, the evidence seized in the unreasonable search must be suppressed. *Mapp v. Ohio* (1961), 367 U.S. 643, 81 S.Ct. 1684, 6 L.Ed.2d 1081; *AL Post 763 v. Ohio Liquor Control Comm.* (1998), 82 Ohio St.3d 108, 111, 694 N.E.2d 905, 908.

In *Carpenter v. United States* 138 U.S. 2206 (2018), the Supreme Court of the United States considered the evolution of digital data and information stored and maintained by a third party and its intersection with the mandates of the Fourth Amendment to the U.S. Constitution. Specifically, the Court noted:

> For much of our history, Fourth Amendment search doctrine was "tied to common-law trespass" and focused on whether the Government "obtains information by physically intruding on a constitutionally

protected area." *United States v. Jones,* 565 U.S. 400, 405, 406, n. 3, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012). More recently, the Court has recognized that "property rights are not the sole measure of Fourth Amendment violations." *Soldal v. Cook County,* 506 U.S. 56, 64, 113 S.Ct. 538, 121 L.Ed.2d 450 (1992). In *Katz v. United States,* 389 U.S. 347, 351, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967), we established that "the Fourth Amendment protects people, not places," and expanded our conception of the Amendment to protect certain expectations of privacy as well. When an individual "seeks to preserve something as private," and his expectation of privacy is "one that society is prepared to recognize as reasonable," we have held that official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause. *Smith,* 442 U.S., at 740, 99 S.Ct. 2577 (internal quotation marks and alterations omitted).

Although no single rubric definitively resolves which expectations of privacy are entitled to protection, the analysis is informed by historical understandings "of what was deemed an unreasonable search and seizure when [the Fourth Amendment] was adopted." *Carroll v. United States,* 267 U.S. 132, 149, 45 S.Ct. 280, 69 L.Ed. 543 (1925). On this score, our cases have recognized some basic guideposts. First, that the Amendment seeks to secure "the privacies of life" against "arbitrary power." *Boyd v. United States,* 116 U.S.

616, 630, 6 S.Ct. 524, 29 L.Ed. 746 (1886). Second, and relatedly, that a central aim of the Framers was "to place obstacles in the way of a too permeating police surveillance." *United States v. Di Re,* 332 U.S. 581, 595, 68 S.Ct. 222, 92 L.Ed. 210 (1948).

We have kept this attention to Founding-era understandings in mind when applying the Fourth Amendment to innovations in surveillance tools. As technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to "assure [] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo v. United States,* 533 U.S. 27, 34, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001). For that reason, we rejected in *Kyllo* a "mechanical interpretation" of the Fourth Amendment and held that use of a thermal imager to detect heat radiating from the side of the defendant's home was a search. *Id.,* at 35, 121 S.Ct. 2038. Because any other conclusion would leave homeowners "at the mercy of advancing technology," we determined that the Government—absent a warrant—could not capitalize on such new sense-enhancing technology to explore what was happening within the home. *Ibid.*

Likewise in *Riley,* the Court recognized the "immense storage capacity" of modern cell phones in holding that police officers must generally obtain a warrant before searching the contents of a phone. 573 U.S., at ___, 134

> S.Ct., at 2489. We explained that while the general rule allowing warrantless searches incident to arrest "strikes the appropriate balance in the context of physical objects, neither of its rationales has much force with respect to" the vast store of sensitive information on a cell phone. *Id.,* at ___, 134 S.Ct., at 2484.

Id. at 2213, 2214. While the *Carpenter* court acknowledged it had previously held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties" *(Smith,* 442 U.S., at 743-744, 99 S.Ct. 2577), it reasoned it was not clear that the same logic would apply to cell site location information. More specifically, the Court said: "When *Smith* was decided in 1979, few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements." *Id.* at 2317. Thus, in holding that information regarding cell site location information was subject to Fourth Amendment considerations, the Court articulated,

> Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection. Whether the Government employs its own surveillance technology * * * or leverages the technology of a wireless carrier, we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through [cell site location information]. The

> location information obtained from Carpenter's wireless carriers was the product of a search.

Id. at 2217.

In the present case, Det. Sturgill stated that he requested a search warrant for Sprint Corporation because he understood that he needed a warrant to assess, use and gather GPS data. He also testified that investigators sought "any and all records" to identify a suspect about whom investigators had no reliable information, other than the fact that Wafa had contacted an individual through the LetGo platform. Indeed, during the evidentiary hearing, Det, Sturgill testified that LetGo was the only avenue for developing a suspect. To that end, Det. Sturgill testified that his request through the investigative subpoenas was "unlimited" and that he wanted as much evidence as possible. Moreover, Det. Sturgill testified that the information gathered from the investigative subpoena to LetGo had a cumulative effect, in that the information provided therefrom, including Defendant's location data, allowed him to issue additional subpoenas that were based and built on the LetGo subpoena. In other words, Det. Sturgill admitted through his testimony that, were it not for the information provided based on the LetGo subpoena, he would not have issue subpoenas to Gmail, Charter Communications, OfferUp or the other entities. In fact, Det. Sturgill testified that, while he issued a search warrant to Sprint in order to obtain GPS location data, IP address information and cell tower location, which he understood was required for compliance with constitutional guarantees, he never in fact received any information from Sprint as a result of the warrant. To that end, Det. Sturgill

testified, "This particular situation, I didn't get the records back, but I wasn't too concerned with the records once I found them because I found them in [Defendant's] car at Cedar Drive. Once I found that, I didn't really care about this, so I never went to Sprint and was like where's the stuff at because I already got him (***)." Case law makes clear that such data must be secured consistent with constitutional requirements and that did not occur in the present case.

III. Conclusion

While the Court understands and is sensitive to the gravity and seriousness of the allegations involved in this case, it cannot consider them to the detriment of the constitutional protections to which Defendant is entitled. As such, the Court finds Defendant's motion well-taken and the motion to suppress evidence is hereby GRANTED.

IT IS SO ORDERED.

Copies to all parties.

Franklin County Court of Common Pleas

Date: 10-03-2022

Case Title: STATE OF OHIO-VS-MAMADOU DIAW

Case Number: 21CR000379

Type: ENTRY/ORDER

It Is So Ordered.

/s/ Judge Kimberly Cocroft