United States Court of Appeals
For The Eighth Circuit
Thomas F. Eagleton U.S. Courthouse
111 South 10th Street, Room 24.329
St. Louis, Missouri 63102

Susan E. Bindler
Clerk of Court

VOICE (314) 244-2400
FAX (314) 244-2780
www.ca8.uscourts.gov

March 10, 2026

Rita Bettis
ACLU OF IOWA FOUNDATION
515-243-3576
Suite 808, Insurance Exchange Building
505 Fifth Avenue
Des Moines, IA 50309-2316

Thomas Dillon Story
ACLU OF IOWA FOUNDATION
Suite 808, Insurance Exchange Building
505 Fifth Avenue
Des Moines, IA 50309-2316

RE: 25-3303 Eyioma Uwazurike, et al v. Dave Jobes, et al

Dear Counsel:

The amicus curiae brief of the American Civil Liberties Union of Iowa Foundation has been filed. If you have not already done so, please complete and file an Appearance form. You can access the Appearance Form at www.ca8.uscourts.gov/all-forms.

Please note that Federal Rule of Appellate Procedure 29(g) provides that an amicus may only present oral argument by leave of court. If you wish to present oral argument, you need to submit a motion. Please note that if permission to present oral argument is granted, the court's usual practice is that the time granted to the amicus will be deducted from the time allotted to the party the amicus supports. You may wish to discuss this with the other attorneys before you submit your motion.

Susan E. Bindler
Clerk of Court

NDG

Enclosure(s)

cc: Chad Douglas Brakhahn
Grant Gerleman
Scott Howard Palmer
Ryan Pell
Van M. Plumb I

James Painter Roberts
Christopher Daniel Sandy
Michael Sandy
Patrick Cannon Valencia
Eric H. Wessan

District Court/Agency Case Number(s): 4:24-cv-00146-RGE

No. 25–3303

UNITED STATES COURT OF APPEALS
FOR THE EIGHTH CIRCUIT

EYIOMA UWAZURIKE, ET AL.,

Plaintiffs-Appellants,

v.

DAVE JOBES, ET AL.,

Defendants-Appellees.

On Appeal from the U.S. District Court for the
Southern District of Iowa
Central Division
Hon. Rebecca Goodgame Ebinger
Case No. 4:24-cv-00146-RGE-SBJ

BRIEF OF *AMICUS CURIAE* AMERICAN CIVIL LIBERTIES UNION OF IOWA FOUNDATION IN SUPPORT OF PLAINTIFFS-APPELLANTS FOR REVERSAL

Thomas D. Story
ACLU of Iowa, Inc.
505 Fifth Av., Ste. 808
Des Moines, IA 50309
Tel: (515) 207-7799
thomas.story@aclu-ia.org

Attorney for *Amicus Curiae*

Rita Bettis Austen
ACLU of Iowa, Inc.
505 Fifth Ave., Ste. 808
Des Moines, IA 50309
Tel: (515) 243-3576
rita.bettis@aclu-ia.org

Attorney for *Amicus Curiae*

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rules of Appellate Procedure 26.1 and 29(c)(1), the American Civil Liberties Union of Iowa Foundation (ACLU of Iowa) certifies it is a non-profit organization that has no parent organization and issues no stock.

STATEMENT OF COMPLIANCE WITH RULE 29(c)(5)

Pursuant to Federal Rule of Appellate Procedure 29(a)(4), the ACLU of Iowa certifies that no party's counsel authored this brief in whole or in part, no party or party's counsel contributed money that was intended to fund preparing or submitting this brief, and no person other than the ACLU of Iowa or their counsel contributed money that was intended to fund the preparing or submitting of this brief.

CONSENT OF THE PARTIES

The ACLU of Iowa obtained written consent on March 5, 2026 from both Plaintiffs-Appellants and Defendants-Appellees to file this brief.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Constitutions

Rules

Statutes

Other Authorities

STATEMENT OF IDENTITY AND INTEREST OF AMICUS

The American Civil Liberties Union of Iowa ("ACLU of Iowa") is a statewide nonprofit and nonpartisan organization with over 6,500 dues-paying Iowa members that is dedicated to the principles of liberty and equality embodied in the Constitution. Founded in 1935, the ACLU of Iowa is the fifth oldest state affiliate of the national American Civil Liberties Union. As part of its mission, the ACLU of Iowa works to protect the privacy of Iowans from intrusive government surveillance and tracking in violation of their Fourth Amendment protections from unreasonable, warrantless searches. Part of this work includes efforts to ensure Fourth Amendment protections are not outpaced by technological innovation and its reliance on the processing and transfer of digitally maintained personally identifiable information.

The ACLU of Iowa has long been committed to safeguarding the right of individuals to be secure in their persons and electronic data from unreasonable government intrusion. As part of these efforts, the ACLU has worked in the courts, state legislature and through policy advocacy to promote appropriate limitations on police collection and use of this data.

Because vast amounts of Iowans' information are collected every day and Iowans maintain a privacy interest in that information, the proper resolution of this case is a matter of substantial interest to the ACLU of Iowa and its members.

ARGUMENT

In 2019, the State of Iowa joined other states that have legalized sports betting. Senate File 617, 2019 Iowa Acts ch. 132. As the District Court noted, a complex regulatory scheme maintained by the Iowa Racing and Gaming Commission quickly developed to oversee this activity. App. 930–31, R.Doc. 89, at 2–3; *see generally* Iowa Code ch. 99F; Iowa Admin. Code r. 491-13.2. Within this scheme were rules intended to ensure that Iowans using mobile applications to place sports bets did so only within the borders of Iowa or another state where such gambling is legal. *See generally* Iowa Code § 99F.9 (governing "advance deposit sports wagering"); Iowa Admin. Code r. 491-13.2(2)(b) (requiring compliance with all federal, state, and local laws). To maintain compliance, sports books FanDuel and DraftKings contracted with another company, GeoComply Solutions, Inc., to track and verify their users' locations. App. 11, R.Doc. 32, at ¶¶ 39–41. This case involves Defendants-Appellees' warrantless, suspicionless, and unlimited use of this personally identifiable information—not to ensure these companies' compliance with gaming regulations, or to investigate users suspected of extraterritorial gambling, but to conduct targeted investigations into athletes and others at Iowa's collegiate institutions. App. 18–19, R.Doc. 32, at ¶¶ 97–100.

These searches were comprehensive and detailed, and they far exceeded Plaintiffs-Appellants' objectively reasonable expectation of privacy in the location

data generated by the apps. This Court should rule as such to vindicate Plaintiffs-Appellants' rights and ensure appropriate limitations are maintained on law enforcement's ability to access and use the incredibly vast amounts of personal information generated by mobile applications.

I. THE DISTRICT COURT WAS CORRECT TO CONCLUDE THE WARRANTLESS COLLECTION OF PLAINTIFFS' PERSONAL INFORMATION VIOLATED THEIR FOURTH AMENDMENT RIGHTS, BUT INCORRECT TO CONCLUDE THESE RIGHTS WERE NOT CLEARLY ESTABLISHED.

This case comes to the Court following the district court's ruling on Defendants' Motion to Dismiss for qualified immunity. App. 208–14, R.Doc. 41-1 at 67–73. While the district court conducted a thorough analysis to find Plaintiffs had adequately alleged a violation of their Fourth Amendment rights, App. 942–53, R.Doc. 89 at 14–25, it erroneously determined Plaintiffs had failed to allege these rights were clearly established. App. 953–55, R.Doc. 89 at 25–27. District courts can and should "rule promptly on the issue of qualified immunity," *Washington v. Wilson*, 46 F.3d 39, 41 (8th Cir. 1995); *see also Schatz Family ex rel. Schatz v. Gierer*, 346 F.3d 1157, 1160 (8th Cir. 2003) (encouraging district courts to "address qualified immunity at the earliest possible stage in the litigation"), but early dismissal is proper only if "immunity can be established on the face of the complaint." *Bradford v. Huckabee*, 330 F.3d 1038, 1041 (8th Cir. 2003). Reviewing this issue de novo, accepting all the Plaintiffs-Appellants' factual allegations as true,

and viewing these allegations in the light most favorable to them, *see Stodghill v. Wellston Sch. Dist.*, 512 F.3d 472, 476 (8th Cir. 2008), Plaintiffs-Appellants have sufficiently alleged Defendants-Appellees violated their constitutional rights that were clearly established under controlling precedent.

A. U.S. Supreme Court Precedent Clearly Established Plaintiffs'-Appellants' Right to be Secure from the Warrantless Collection of their Personal Information.

State actors are not entitled to qualified immunity if "at the time of alleged violation," "'every reasonable official' would have known the conduct was unlawful." *T.S.H. v. Green*, 996 F.3d 915, 918 (8th Cir. 2021) (quoting *District of Columbia v. Wesby*, 583 U.S 48, 63 (2018)). This standard may be met by "an obvious violation," or one for which "a controlling case or a robust consensus of cases or persuasive authority," even if not "directly on point," have put the "constitutional question beyond debate." *Thurmond v. Andrews*, 972 F.3d 1007, 1012 (8th Cir. 2020) (quoting *Dillard v. O'Kelley*, 961 F.3d 1048, 1052 (8th Cir. 2020)). Here, a controlling case, *Carpenter v. United States*, has clearly established that the warrantless collection of location information generated when using cell phones violates the Fourth Amendment. 585 U.S. 296, 315–16 (2018). Following the facts and reasoning of *Carpenter*, it "is sufficiently clear that every reasonable official" tempted to engage in the warrantless collection of location information "would have understood that what he is doing violates that right" as determined in

that case. *Thurmond*, 972 F.3d at 1012 (quoting *Mullenix v. Luna*, 577 U.S. 7, 11 (2015)).

1. A person's detailed location information is protected from warrantless search.

The opinion in *Carpenter* involved the government's warrantless access to cell-site location information ("CSLI"), which it compelled from wireless carriers under a provision of the Stored Communications Act. 585 U.S. at 301–02 (citing 18 U.S.C. § 2703(d)). As described by the Court, CSLI are time-stamped records automatically generated when cell phones continuously scan for the best signal and are used by wireless carriers to find weak spots in their network, impose "roaming charges," and sell the anonymized and aggregated data to brokers. *Id.* at 300. While "the ability to chronicle a person's past movements through the record of his cell phone signals" was a "new phenomenon" for the Court to confront, it fit, if not "neatly," then easily, into the Court's long-existing precedent acknowledging "a person's expectation of privacy in their physical location and movements." *Id.* at 306, 310–13; *see also U.S. v. Jones*, 565 U.S. 400, 430 (2012) (Alito, J., concurring in judgment) (recognizing long-term monitoring of location "impinges on expectations of privacy"); *id.* at 415 (Sotomayor, J., concurring) (agreeing); *U.S. v. Knotts*, 460 U.S. 276, 283–84 (1983) (declining to find use of rudimentary "beeper" a search, but noting potential for constitutional protection if "twenty-four hour surveillance of any citizen of this country" became possible with new technology).

Following the reasoning of these cases, the Court held the government's access of the CSLI was a search that invaded the defendant's "reasonable expectation of privacy in the whole of his physical movements." *Carpenter*, 585 U.S. at 313.

This holding was based on four features of CSLI data: (1) it is comprehensive; (2) it is retrospective; (3) it has the capacity to reveal intimate information about the subject; and (4) it is alarmingly easy and efficient to use when compared to traditional investigative techniques. *Carpenter*, 585 U.S. at 311–12. Each of these features are present in the location data maintained by GeoComply and searched by Defendants–Appellees, as explained below. Accordingly, though CSLI is generated by different technology and for different purposes than the location data at issue here, a person's expectation of privacy in it is no different. If not "directly on point," *Thurmond*, 972 F.3d at 1012, the Court's decision in *Carpenter* gave Defendants-Appellees more than "fair warning" their conduct was unconstitutional. *Quraishi v. St. Charles Cty., Mo.*, 986 F.3d 831, 835 (8th Cir. 2021) (quoting *Sisney v. Reisch*, 674 F.3d 839, 845 (8th Cir. 2012)).

First, in *Carpenter*, the Court was disturbed by the fact that CSLI data provided "an all-encompassing record of the holder's whereabouts." 585 U.S. at 311. There, law enforcement requested and obtained nearly 13,000 individual location data points tracking users' movements over more than 130 days. *Id.* at 302. The Court held the government's use of such quantities of data contravenes the

reasonable expectation that law enforcement will not secretly monitor a person's every move. *Id.* at 310–11. The same is true here, as GeoComply maintains a vast database of location information, which law enforcement used to identify users in an area over the course of several months and track them over longer periods of time accordingly. App. 19, R.Doc. 32 at ¶¶ 102–104. Indeed, given they possessed login credentials—unlike the government in *Carpenter*, which was forced to ask for a discrete subset of data, 585 U.S. at 302—Defendants-Appellees had full access to the GeoComply dataset. App. 16–17, R.Doc. 32 at ¶ 82. Defendants-Appellees used this access to compile *years* of historic location information for each Plaintiff-Appellant. App. 19, R.Doc. 32 at ¶ 103. The quantity of data available to them allowed them to create, just as the subset of CSLI in *Carpenter*, "an all-encompassing record of the holder's whereabouts." *Carpenter*, 585 U.S. at 311.

Second, the *Carpenter* Court found "the retrospective quality of the data here gives police access to a category of information otherwise unknowable." 585 U.S. at 312. CSLI is historic location data, and "subject only to the retention policies of the wireless carriers," law enforcement can use this to retrace a person's whereabouts over years of time. *Id.* Effectively, the use of such data means that everyone, "not just those who . . . might happen to come under investigation," are under police surveillance at "every moment of every day" for as far back as the data goes, which contravenes any reasonable person's expectation of privacy in their

movements. *See id.* Again, the same is true for the historic location data searched here. App. 19, R.Doc. 32 at ¶ 103. Worse, as in contrast to the "seven days of CSLI" the Court ruled was a search in *Carpenter*, 585 U.S. at 310 n. 3, Defendants used GeoComply to recreate years of Plaintiffs-Appellants' movements. App. 19, R.Doc. 32 at ¶ 103.

Third, CSLI, in its specificity, is highly intrusive. *Carpenter*, 585 U.S. at 311. "As with GPS information, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'" *Id.* (quoting *Jones*, 565 U.S. at 415 (opinion of Sotomayor, J.)); *see also U.S. v. Karo*, 468 U.S. 705, 715 (1984) (reasoning that using an electronic device to obtain information from within the home is as presumptively unreasonable as a physical search). Here, Plaintiffs-Appellants' locations were verified every time they opened a contracting sports book, and the tracking continued at regular intervals while the app ran. App. 935, R.Doc. 89 at 7; App. 11, R.Doc. 32 at ¶ 41; App. 229–30, 271, R.Doc. 42 at 007 ¶ b, 049 ¶ 21.2; App. 479, R.Doc. 42 at 257. This allowed Defendants to produce "reports detailing the exact dates, times, and precise locations—including the users' homes and specific areas within other States that allowed online sports betting." App. 19, R.Doc. 32 at ¶ 103. Using the detailed location data at their fingertips, Defendants-Appellees had insight into Plaintiffs-Appellants' every move, and would

have been able to determine whether they skipped class, stayed overnight with someone, or went to the bar.

Fourth, CSLI, in its relative ease and efficiency, presents an unacceptable temptation for misuse. *See Carpenter*, 585 U.S. at 311. In *Carpenter*, the Court compared CSLI to GPS monitoring, noting that "cell phone tracking is remarkably easy, cheap, and efficient compared to traditional investigative tools," adding that, "With just the click of a button, the Government can access each carrier's deep repository of historical location information at practically no expense." *Id.* In *Carpenter*, that statement, while true in principle, had a touch of the dramatic, as the Government had to do much more than just "push a button": it only obtained the location data after offering to a magistrate "'specific and articulable facts showing that there are reasonable grounds to believe' that the records sought 'are relevant and material to an ongoing criminal investigation.'" *Id.* at 326 (quoting 18 U.S.C. § 2703(d)). But here, the "push-of-a-button" claim is literally descriptive. With log-in credentials and special software allowing them to interface more easily with the raw data, Defendants-Appellees had a virtual map with which they could push a few buttons, maybe drag a mouse pointer, and quickly and easily locate, identify, and track users across time. App. 935, R.Doc. 89 at 7; App. 19, R.Doc. 32 ¶¶ 98–100; App. 471, R.Doc. 42 at 249.

As in *Carpenter*, this case "is not about 'using a phone' or a person's movement at a particular time," 585 U.S. at 315; it is about the warrantless collection of expansive, retrospective, intrusive, and cheaply available location data. Though this case concerns location data generated by an app and not a cell phone tower, these crucial characteristics persist. Given this, it is highly unlikely that Defendants-Appellees did not understand they were violating Plaintiffs-Appellants' rights. Indeed, Plaintiffs-Appellants have supported their allegations with emails between Defendants indicating they knew just that. App. 13–19, R.Doc. 32 at ¶¶ 57–100.

2. The third-party doctrine does not apply.

It was these same characteristics of CLSI data that led the *Carpenter* Court to reject application of the third-party doctrine. 585 U.S. at 315–16. Under the third-party doctrine, there are times when a person that "voluntarily turns over [information] to third parties" cannot maintain an expectation of privacy in that information. *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979). The rationale of this doctrine is that a person who knowingly reveals certain information is "assum[ing] the risk" that it could be then redisclosed to others. *Id.* at 744; *see also U.S. v. Miller*, 425 U.S. 435, 443 (1976). The *Carpenter* Court reasoned that the third-party doctrine depends heavily on the facts and circumstances of information disclosed and is generally inconsistent with society's expectations regarding their personal information generated by using mobile phones. 585 U.S. at 314–15 (noting

considerable differences between information accessible under third-party doctrine and location data, holding that users of mobile phones do not voluntarily assume the risk that the government will obtain "a comprehensive dossier" of their movements). Contrary to the D.C. District Court's decision in *U.S. v. Bledsoe*, which is likely to be heavily cited by Defendants–Appellees, the *Carpenter* Court's rejection of the third-party doctrine was not simply because generating CSLI is "automatic," "inescapable," or "essential to modern life." 630 F. Supp. 3d 1, 13 (D.C. Dist. Ct. 2022). Though it may be those things, the third-party doctrine does not apply because the information at issue is incomparable to the limited records redisclosed to law enforcement in past third-party doctrine cases. *See Carpenter*, 585 U.S. at 314.

The third-party doctrine initially appears inconsistent with the reasonable expectation of privacy standard developed in *Katz v. U.S.*, 389 U.S. 347, 351 (1967), as it defies societal expectations informed by property law and even other U.S. Supreme Court Fourth Amendment cases. *See Carpenter*, 585 U.S. at 399–400 (Gorsuch, J., dissenting) (noting that in a bailment, a third party using another's property in a way inconsistent with the bailor's instructions has breached the contract and is liable for conversion); *Terrace Hill Society Found. v. Terrace Hill Comm'n*, 6 N.W.3d 290, 296 (Iowa 2024) (noting specific duties imposed on bailees to care for bailor's property when voluntary bailment has been established); *see also*

Minnesota v. Olson, 495 U.S. 91, 99 (1990) (recognizing a guest's reasonable expectation of privacy in a home under the ultimate control of the host); *Stoner v. California*, 376 U.S. 483, 489–90 (1964) (recognizing a hotel guest's reasonable expectation of privacy in a hotel room that could not be waived by hotel or its employees); *Ex parte Jackson*, 96 U.S. 727, 733 (1878) (recognizing constitutional protection in person's mail, even when given to mail carriers). However, the third-party doctrine only applies to those special circumstances when "the nature of the particular documents sought" and the scope of the voluntary disclosure create an implied assumption of potential redisclosure to the government—the assumption of risk. *Miller*, 425 U.S. at 442 (no reasonable expectation of privacy in checks, financial statements, and deposit slips given to commercial institutions); *see also Smith*, 442 U.S. at 735 (no reasonable expectation of privacy in numbers dialed and therefore conveyed to phone company). The Fourth Amendment's goals are "to secure 'the privacies of life' against 'arbitrary power'" and "'place obstacles in the way of a too permeating police surveillance.'" *Carpenter*, 585 U.S. at 305 (first quoting *Boyd v. U.S.*, 116 U.S. 616, 630 (1886), then quoting *U.S. v. Di Re*, 332 U.S. 581, 595 (1948)). If the third-party doctrine were applied blanketly to every transfer of any information to another, including those where it cannot be said the transferor assumed the risk of redisclosure, it would quickly deny these goals and become an outright exception to the reasonable expectation of privacy standard.

Recognizing this, the Eighth Circuit has been limited in its own extension of the third-party doctrine, and, except in the pen register context squarely governed by *Smith*, applies it only to specific circumstances in which the quality and quantity of the information disclosed was inherently limited. *See, e.g.*, *U.S. v. Sesay*, 937 F.3d 1146, 1152 (8th Cir. 2019) (identification cards provided when registering at a motel); *U.S. v. McIntyre*, 646 F.3d 1107, 1111–12 (8th Cir. 2011) (building's electricity usage records gathered by utility). In other cases, this Court has declined invitations to expand the third-party doctrine unnecessarily. *See, e.g.*, *Wabun-Inini v. Sessions*, 900 F.2d 1234, 1243 (8th Cir. 1990) (limiting decision on film provided to photo processors to specific facts of case and declining to hold more generally that such customers lose expectations of privacy). The facts of this case do not justify a different approach.

The question is not merely whether Plaintiffs–Appellants shared their location with GeoComply. Under *Katz*, 389 U.S. at 351, and still under the third-party doctrine of *Miller*, 425 U.S. at 442, it is whether they maintained a reasonable expectation of privacy in that information. Even if Plaintiff-Appellants provided their location "voluntarily" and "knowingly" according to a click-through privacy policy, it is their and society's expectations that govern. *See U.S. v. Warshak*, 631 F.3d 266, 286–87 (6th Cir. 2010) (holding an email subscriber agreement does not generally defeat a reasonable expectation of privacy); *see also In re Search of Info.*

Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 737 (N.D. Ill. 2020) (finding it "difficult to imagine" that mobile phone users realize their detailed location data may be revealed to the government); Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 Harv. L. Rev. 1880, 1884–88 (2013). Like a hotel guest allowing a maid in to clean, or a tenant allowing a plumber in to fix a leaky faucet, *see id.*; *see also Stoner*, 376 U.S. at 490; *Chapman v. U.S.*, 365 U.S. 610, 616–17 (1961), allowing a third party access to property for one purpose does not mean welcoming all others to access the property for their own uses, including, without a warrant, the government.

To illustrate: when a person visits jimmyjohns.com and clicks the button to authorize the collection of their personal information, including their location, they do not do so expecting law enforcement to access Jimmy Johns' database to track their movements; they do it expecting a quick sandwich from a nearby franchise, and maybe with the understanding they will receive some targeted marketing for the new Greek & Chicken Gyro. *See* Jimmy John's, *Privacy Policy*, https://www.jimmyjohns.com/privacy-policy (accessed March 3, 2026). Providing location data is not "automatic," *Bledsoe*, 630 F. Supp. 3d at 13, as one could pick up their own sandwich, nor is it "inescapable" or "essential to modern life," *id.*, as surely one could do without. Yet most must agree that some expectation of privacy in the location data is reasonable. *See, e.g.*, Cal. Civ. Code § 1798.100(c) ("A

business's collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected . . . , and not further processed in a manner that is incompatible with those purposes."); General Data Protection Regulation, Ch. 2, Art. 5, § 1(b) (similarly describing "purpose limitation" in processing of personal data, that it be collected and used for only purposes specified and necessary). Therefore, when Plaintiffs–Appellees opened up their FanDuel or DraftKings app, they may reasonably have expected their location in a legal state would be confirmed so they could place a bet; but they would not have anticipated their movements would continuously be logged or later accessed by Defendants-Appellees.

B. The District Court Erred in Construing the Warrantless Collection of Location Data Here as Akin to the Geofence Warrants at Issue in other Circuit Court Decisions.

After examining this authority, rejecting the third-party doctrine, and correctly concluding Defendants-Appellees violated the Fourth Amendment rights of Plaintiffs-Appellants, the District Court too easily determined the novelty of Defendants-Appellees' investigative methods took them outside of clearly established law. App. 954–55, R.Doc. 89 at 26–27. The District Court described its opinion as "follow[ing] the path the Supreme Court articulated in *Carpenter*," App. 955, R.Doc. 89 at 27, when it was already on well-trodden ground. The District

Court's mistake was in analogizing the case before it to a current post-*Carpenter* Circuit Court split between *U.S. v. Smith*, 110 F.4th 817 (5th Cir. 2024), and *U.S. v. Chatrie*, 107 F.4th 319 (4th Cir. 2024), *aff'd on rehearing en banc*, 136 F.4th 100 (2026), *cert. granted in part*, 2026 WL 120676 (Jan. 16, 2026). In short, the Circuit Court split over the extension of *Carpenter*'s reasoning to geofence warrants does not undermine the clear application of *Carpenter* itself to Defendants-Appellees' warrantless collection of location data. The constitutional question of geofence warrants remains, but the unconstitutionality of warrantlessly searching location data generated by mobile phone use should be "beyond debate." *Thurmond*, 972 F.3d at 1012.

The issue in *Chatrie* and *Smith* is narrow and focused specifically on the constitutionality of a "geofence warrant." *See Smith*, 110 F.4th at 830 ("The threshold question posed by this case is whether geofencing is a search under the Fourth Amendment."); *Chatrie*, 136 F.4th at 101–02 ("Today we consider the constitutionality of geofence warrants, a novel and powerful technology that law enforcement has increasingly used to investigate crime."). Defendants-Appellees' use of location data may resemble what occurs in a geofence warrant, but it was not a geofence warrant as that term is defined. Defendants-Appellees themselves did not consider their actions a "typical geofence search," App. 183, R.Doc. 41-1 at 42, and, albeit for the wrong reasons, they are correct.

"In simple terms, a geofence warrant requires a service provider to produce location data from cell phone users who were near the scene when a crime occurred." *Chatrie*, 136 F.4th at 102. A considerable amount of writing exists on the many problems of geofence warrants, including law enforcement's growing reliance on them, *see* Brian L. Owsley, *The Best Offense Is a Good Defense: Fourth Amendment Implications of GeoFence Warrants*, 50 Hofstra L. Rev. 829, 834 (2022) (noting Google received about 20,000 geofence warrant requests between 2018 and 2020, over half in 2020 alone), their access to a mind-bogglingly large yet particular volume of data, *see* Haley Amster, Brett Diehl, *Against GeoFences*, 74 Stan. L. Rev. 385, 389 (2022) (noting one geofence warrant unearthed location data for 1,494 cell phones in a 7.4-acre area over just nine hours), or their lack of oversight, Note, *GeoFence Warrants and the Fourth Amendment*, 134 Harv. L. Rev. 2508, 2513–14 (2021) (noting judges approving geofence warrants are often not provided detailed information regarding the search, and that public insight is limited by the sealing of warrants). These issues are important, and present here, but magnified such that they are not part of the *Chatrie–Smith* split and are returned to the core of *Carpenter*.

It is firstly in the name: a geofence warrant requires a warrant, and none was sought here. App. 18, R.Doc. 32 at ¶ 90. As a warrant, a geofence warrant can only be obtained after a judge has determined both that probable cause exists and that the warrant meets the particularity requirement in its scope. *See In re Search of Info.*

Stored, 481 F. Supp. 3d at 740–41. Here, Defendants-Appellees did not have probable cause and it is unclear whether they even had a hunch of wrongdoing. App. 18–19, 21, R.Doc. 32 at ¶¶ 97, 101, 111, 113, 120. Whatever cause they might once have possessed had dissipated by then, App. 13, R.Doc. 32 at ¶¶ 58–59, and it appears much of the impetus for the search was simply Defendants-Appellees' excitement to use their new tool. App. 13–14, 18, 20, R.Doc. 32 at ¶¶ 57, 65, 96, 110. As for particularity, unlike the circumscribed area and time frame of a geofence warrant, Defendants-Appellees were bound by no such requirement and, due to their log-in credentials and access via their own laptops, were permitted full access to scour GeoComply's location data as their own time and interest allowed. App. 16–17, R.Doc. 32 at ¶¶ 81, 85.

This case differs in process from geofence warrants as well. For example, a geofence warrant requires a private company to conduct a search of its own data in response to government demand. *See Smith*, 110 F.4th at 824–25 (describing "step 1" of a geofence warrant requiring Google to search its "Sensorvault" "to find responsive user records"). Here, GeoComply simply gave Defendants-Appellees log in credentials and taught them how the user interface works, allowing Defendants-Appellees to conduct the searches themselves. App. 16–17, R.Doc. 32 at ¶¶ 81, 85. Relatedly, a geofence warrant involves a back-and-forth between the company and law enforcement, first providing anonymized data, then narrowing down to relevant

user IDs, before finally being compelled to provide full account-identifying information. *See Smith*, 110 F.4th at 824–25 (describes steps 2 and 3 of a geofence warrant). Defendants-Appellees were able to skip all of this process due to their plenary access to GeoComply's database and the use of software that simultaneously found and identified users within the particular search area. App. 19, R.Doc. 32 at ¶¶ 98–100, 103–104. If a regular warrant proceeds from suspect to surveillance, and a geofence warrant from surveillance to suspect, *see Smith*, 110 F.4th at 822, then Defendants-Appellees here had a tool giving them all at once.

Again, assessing the constitutionality of geofence warrants requires the application of Fourth Amendment principles common to this case: privacy, and an obstacle in the way of police surveillance that is comprehensive, retrospective, intrusive, and easy. *See Carpenter*, 585 U.S. at 311–12. But that does not make the application of those principles to the facts of this case any less clear.

II. REGARDLESS, BECAUSE THIS IS A MATTER OF GREAT IMPORTANCE, THIS COURT SHOULD AFFIRMATIVELY ESTABLISH CLEAR PRECEDENT NOW.

In the alternative, if Defendants-Appellees' warrantless collection of location data generated by Plaintiffs-Appellants' sports betting apps did not violate clearly established law at the time, *but see Thompson v. City of Monticello*, 894 F.3d 993, 999 (8th Cir. 2018) ("While clearly established law should not be defined at a high level of generality it is not necessary, of course, the very action in question has

previously been held unlawful." (cleaned up)), this is the case in which to establish that law in the Eighth Circuit.

Though discretionary, it is "often beneficial" to address whether a constitutional right has been violated before determining whether that right was clearly established at the time. *Pearson v. Callahan*, 555 U.S. 223, 236 (2009); *Ross v. City of Jackson, Mo.*, 897 F.3d 916, 920 (8th Cir. 2018) ("While we are not required to apply the steps sequentially, 'it is often beneficial' to do so."). While there may be an expectation that companies will generally require the government to obtain a warrant before accessing user data, *see* Rainey Reitman, *Who Has Your Back? Government Data Requests 2017*, https://www.eff.org/who-has-your-back-2017#best-practices (surveying major tech companies' policies on law enforcement requests for data), this case shows that expectation may be defied, and there must—if there is not already—be a rule to govern such cases. *See Pearson*, 555 U.S. at 236 (noting "the two-step procedure promotes the development of constitutional precedent"). Moreover, given the apparent availability of law enforcement's warrantless access to location data maintained by any number of companies, this issue may frequently rearise, but in each case will be subject to a claim of qualified immunity. *See Pearson*, 555 U.S. at 236 (noting the development of constitutional precedent is "especially valuable" in cases that will not arise without a qualified immunity defense).

If not already resolved by *Carpenter*, a decision on the merits will set the standard for future litigation and would not at all represent a decision where the "constitutional question is so factbound that [it] provides little guidance for future cases." *Pearson*, 555 U.S. at 237. This case is eye-catching for the substantial media coverage Defendants-Appellees' actions generated and the fallout,[1] but its focus—the security of personal information—is a common subject for concern.[2] Though early in process, Plaintiffs-Appellants' factual allegations are well-investigated and the basis for their claim easy to identify. *See Pearson*, 555 U.S. at 238–39. This case thus presents an ideal opportunity to decide a matter of great importance.

CONCLUSION

For these reasons, the ACLU of Iowa supports the position of Plaintiffs-Appellants and respectfully encourages this Court to reverse the district court's grant of dismissal in favor of Defendants-Appellees. However, though the district court erred in granting qualified immunity to Defendants-Appellees, its analysis and

---

[1] *See, e.g.*, Tyler Jett, *Stress from sports bet probe killed investigator, DCI agent alleges in court document*, Des Moines Register, Sept. 11, 2024, https://tinyurl.com/6az2ynbt; Tyler Jett, *How a tech company encouraged Iowa's sports gambling investigation, then walked away*, Des Moines Register, April 10, 2024, https://tinyurl.com/4rt84aau; Jared Diamond, *The Sweeping, and Puzzling, Crackdown on College Athletes' Betting in Iowa*, The Wall Street Journal, Sept. 15, 2023, https://tinyurl.com/3dz5s4wx.

[2] *See, e.g.*, Electronic Frontier Foundation, *Surveillance Self-Defense: Tips, Tools, and How-Tos for Safer Online Communications*, https://ssd.eff.org/ (accessed March 5, 2026).

affirmation of Plaintiffs-Appellants' reasonable expectation of privacy in their location data was sound. This Court should affirm this right through, as argued by Plaintiffs-Appellants, the straightforward application of existing U.S. Supreme Court precedent or, alternatively, through the development of this precedent in the Eighth Circuit.

Dated: March 9, 2026

Respectfully submitted:

/s/ Thomas D. Story
Thomas D. Story

/s/Rita Bettis Austen
Rita Bettis Austen

ACLU of Iowa, Inc.
505 Fifth Ave., Ste. 808
Des Moines, IA 50309
(515) 243-3576
thomas.story@aclu-ia.org
rita.bettis@aclu-ia.org

Attorneys for *Amicus Curiae* ACLU of Iowa

CERTIFICATE OF COMPLIANCE

This document complies with the type-volume limit of Fed. R. App. P. 29(a)(5) and 32(a)(7)(B)(i) because, excluding the parts of the document exempted by Fed. R. App. P. 32(f), this document contains 5,221 words. Further, this document complies with the typeface and type-style requirements of Fed. R. App. P. 32(a)(5) and the type-style requirements of Fed. R. App. P. 32(a)(6) because this document has been prepared in a proportionately-spaced typeface using Microsoft Word in 14-point Times New Roman font.

This document has been scanned for viruses and is virus free in compliance with 8th Cir. R. 28A(h).

Dated: March 9, 2026

Respectfully submitted:

/s/Rita Bettis Austen
Rita Bettis Austen
ACLU of Iowa, Inc.
505 Fifth Ave., Ste. 808
Des Moines, IA 50309
(515) 243-3576
rita.bettis@aclu-ia.org

Attorney for *Amicus Curiae* ACLU of Iowa

/s/ Thomas D. Story
Thomas D. Story
ACLU of Iowa, Inc.
505 Fifth Ave., Ste. 808
Des Moines, IA 50309
Tel: (515) 207-7799
thomas.story@aclu-ia.org

Attorney for *Amicus Curiae* ACLU of Iowa

CERTIFICATE OF SERVICE

I hereby certify that on March 9, 2026, I caused the foregoing to be electronically filed with the Clerk of the Court for the United States Court of Appeals for the Eighth Circuit by using the CM/ECF system. Participants in the case who are registered CM/ECF users will be served by the CM/ECF system.

I further certify that pursuant to Circuit Rule 28A(d) and within five days of receipt of the notice of this Court's acceptance of the brief for filing, I will cause ten (10) copies of the brief to be transmitted to the Court via overnight delivery, delivery charge prepaid.

Dated: March 9, 2026

Respectfully submitted:

/s/Rita Bettis Austen
Rita Bettis Austen
ACLU of Iowa, Inc.
505 Fifth Ave., Ste. 808
Des Moines, IA 50309
(515) 243-3576
rita.bettis@aclu-ia.org

Attorney for *Amicus Curiae* ACLU of Iowa