PD-0523-25
COURT OF CRIMINAL APPEALS
AUSTIN, TEXAS
Transmitted 5/13/2026 4:04 PM
Accepted 5/13/2026 4:51 PM
DEANA WILLIAMSON
CLERK

IN THE COURT OF CRIMINAL APPEALS OF TEXAS
No. PD-0523-25

De H. Nguyen,
Appellant,

v.

The State of Texas,
Appellee.

On Appeal from the Court of Appeals for the Third District of Texas at Austin
No. 03-23-00301-CR

BRIEF OF *AMICI CURIAE* THE AMERICAN CIVIL LIBERTIES UNION OF TEXAS AND AMERICAN CIVIL LIBERTIES UNION IN SUPPORT OF APPELLANT

Terry Ding*
Laura Moraff**
American Civil Liberties Union Foundation
125 Broad Street, 17th Floor
New York, NY 10004
(212) 549-2500
ttding@aclu.org
lauramoraff@aclu.org

Pro hac vice application pending
***Pro hac vice* application forthcoming

Thomas Buser-Clancy
(Texas Bar No. 24078344)
Savannah Kumar
(Texas Bar No. 24120098)
ACLU Foundation of Texas, Inc.
P.O. Box 8306,
Houston, TX 77288
(713) 942-8146
tbuser-clancy@aclutx.org
skumar@aclutx.org

Counsel For Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES iii

STATEMENT OF INTEREST 1

INTRODUCTION AND SUMMARY OF ARGUMENT 2

ARGUMENT 7

I. Geofence warrants violate the Texas Constitution because they authorize overbroad exploratory searches to which the third-party doctrine does not apply. 8

A. The government conducts a search when it executes a geofence warrant because it infringes on Texans' reasonable expectations of privacy and property interests. 9

B. Texas's third-party doctrine does not apply to Location History. 15

1. This Court should reaffirm the narrow form of the third-party doctrine articulated in *Richardson* because it effectuates the Texas Constitution's protections for private data. 16

2. The third-party doctrine does not apply to Location History. 21

C. Geofence warrants are unconstitutional because, similar to general warrants and writs of assistance, they necessarily encompass data belonging to people who could not have committed the pertinent offense. 24

II. Geofence warrants transfer judicial authority to law enforcement and private parties in violation of the separation of powers required by the Texas Constitution. 28

A. Warrants implicate acute separation-of-powers concerns under the Texas Constitution. 28

B. Geofence warrants violate the Texas Constitution's separation-of-powers commands. 30

III. At a minimum, this Court should provide guidance to limit unreasonably intrusive geofence searches. 32

CONCLUSION 36

TABLE OF AUTHORITIES

Cases

Arizona v. Hicks,
480 U.S. 321 (1987).....14

Arkansas v. Sanders,
442 U.S. 753 (1979).....29

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

Clemons v. State,
605 S.W.2d 567 (Tex. Crim. App. 1980) 29

Commonwealth v. Beauford,
327 Pa. Super. 253 (1984) 18

Crider v. State,
607 S.W.3d 305 (Tex. Crim. App. 2020) 24

Dupree v. State,
102 Tex. 455 (1909)..... 27, 33

Eggemeyer v. Eggemeyer,
554 S.W.2d 137 (Tex. 1977) 10

El-Ali v. State,
428 S.W.3d 824 (Tex. 2014) 25

Entick v. Carrington,
95 Eng. Rep. 807 (C.P. 1765).....14

Ex parte Gould,
60 Tex. Crim. 442 (1910) 2, 13, 33

Ford v. State,
477 S.W.3d 321 (Tex. Crim. App. 2015) 18, 19

Garofolo v. Ocwen Loan Servicing, L.L.C.,
497 S.W.3d 474 (Tex. 2016) 2, 21

Hankston v. State,
517 S.W.3d 112 (Tex. Crim. App. 2017), *cert. granted, judgment vacated*, 585 U.S. 1028 (2018) 19, 20

Holder v. State,
595 S.W.3d 691 (Tex. Crim. App. 2020) ..... passim

In re Sun Coast Res., Inc.,
562 S.W.3d 138 (Tex. App.—Houston [14th Dist.] 2018, *no pet.*) 11

Jim Olive Photography v. Univ. of Houston Sys.,
624 S.W.3d 764 (Tex. 2021) 10

Kopplow Dev., Inc. v. City of San Antonio,
399 S.W.3d 532 (Tex. 2013) 10

LeCroy v. Hanlon,
713 S.W.2d 335 (Tex. 1986) 16

Lightning Oil Co. v. Anadarko E&P Onshore, LLC,
520 S.W.3d 39 (Tex. 2017).....11

Lippert v. State,
664 S.W.2d 712 (Tex. Crim. App. 1984) 14

Maryland v. King,
569 U.S. 435 (2013).....24

Nguyen v. State,
722 S.W.3d 237 (Tex. App.—Austin 2025, *pet. granted*) 31

Richardson v. State,
865 S.W.2d 944 (Tex. Crim. App. 1993) ..... passim

Riley v. California,
573 U.S. 373 (2014).....10

Rodriguez v. State,
232 S.W.3d 55 (Tex. Crim. App. 2007) 28

Smith v. Maryland,
442 U.S. 735 (1979)..... passim

State v. Baldwin,
664 S.W.3d 122 (Tex. Crim. App. 2022) 35

State v. Barnett,
788 S.W.2d 572 (Tex. Crim. App. 1990) ..... passim

State v. Contreras-Sanchez,
No. A22-1579, 2026 WL 1015919 (Minn. Apr. 15, 2026) 2, 12, 23, 31

State v. Geraw,
795 A.2d 1219 (Vt. 2002) 29

State v. Granville,
423 S.W.3d 399 (Tex. Crim. App. 2014) 10

State v. Hobbs,
975 N.E.2d 965 (Ohio 2012) 29

State v. Huse,
491 S.W.3d 833 (Tex. Crim. App. 2016) 9

State v. Organ,
726 S.W.3d 346 (Tex. Crim. App. 2025) 13, 14

State v. Rhine,
297 S.W.3d 301 (Tex. Crim. App. 2009) 28

Steagald v. United States,
451 U.S. 204 (1981) 25

United States v. Chatrie,
136 F.4th 100 (4th Cir. 2025), *cert. granted in part*, 2026 WL 120676
(U.S. Jan. 16, 2026) (No. 25-112) 4, 25

United States v. Miller,
425 U.S. 435 (1976) 17, 19, 20, 23

United States v. Smith,
110 F.4th 817 (5th Cir. 2024), *cert. denied*, 146 S. Ct. 356 (2025) ..... passim

Walthall v. State,
594 S.W.2d 74 (Tex. Crim. App. 1980) 29, 31

Wells v. State,
714 S.W.3d 614 (Tex. Crim. App. 2025) 1, 4, 12

Ybarra v. Illinois,
444 U.S. 85 (1979) 26

Constitutional Provisions

Texas Const. art. I § 9 ..... passim
Texas Const. art. I § 17 ..... 8, 9, 12, 36
Texas Const. art. I § 19 ..... 8, 9, 12, 36
Texas Const. art. II § 1 ..... 28, 36
U.S. Const. amend. IV 33

Statutes

Tex. Code Crim. Proc. art. 18.01 29
Tex. Code Crim. Proc. art. 18.02 29
Tex. Penal Code § 30.05 11
Tex. Penal Code § 31.07 13
Tex. Penal Code § 33.01(16) 10
Tex. Penal Code § 33.02 ..... 11, 14

Other Authorities

Geofence Warrants and the Fourth Amendment, 134 Harv. L. Rev. 2508 (2021) 3

Herbert B. Dixon Jr., *Your Cell Phone Is A Spy!*, Judges' J., Summer 2020 ..... 15, 22

Jeffrey S. Sutton, *51 Imperfect Solutions: States and the Making of American Constitutional Law* 17 (2018) 32

Ryan Nakashima, *Google Tracks Your Movements, Like it or Not*, Associated Press (Aug. 13, 2018) 22

STATEMENT OF INTEREST[1]

The American Civil Liberties Union ("ACLU") is a nationwide, non-profit, non-partisan organization dedicated to defending the principles of liberty and equality embodied in the federal and state constitutions. The ACLU of Texas is the Texas affiliate of the national ACLU. It has thousands of members and supporters across the State and works with communities, at the State Capitol, and in the courts to fulfill the promises of the U.S. and Texas Constitutions for every Texan, with no exceptions. From Amarillo to Brownsville and Beaumont to El Paso, we believe in a Texas that works for all of us—a Texas where each person has an equal say in the decisions that shape our future and everyone can build a good life.

Amici have an interest in this case because they have long advocated for courts to uphold constitutional protections against unreasonable searches, seizures, and other intrusions on people's privacy and property rights, and to ensure that those protections are not eroded by the advance of technology. They submitted an amicus brief when this Court previously considered geofence warrants in *Wells v. State*, 714 S.W.3d 614 (Tex. Crim. App. 2025). The ACLU has also filed amicus briefs in other courts addressing the constitutionality of geofence warrants. *See, e.g.*, Br. of Amici Curiae American Civil Liberties Union et al. in Support of Petitioner, *Chatrie v. United States* (U.S. Mar. 2, 2026) (No. 25-112); Br. of Amici Curiae American Civil

[1] No party has paid a fee or otherwise compensated *amici* for this brief.

Liberties Union and American Civil Liberties Union of Minnesota, *State v. Contreras-Sanchez*, No. A22-1579, 2026 WL 1015919 (Minn. Apr. 15, 2026).

INTRODUCTION AND SUMMARY OF ARGUMENT

During the colonial era, British authorities used general warrants and writs of assistance to conduct wide-ranging searches of colonists, their homes, and their property. These warrants were not based on probable cause to believe a particular person had broken the law. Instead, they allowed officials to rummage through anyone's belongings in the hopes of turning up some evidence of wrongdoing. Colonists despised these oppressive methods as "the worst instrument of arbitrary power . . . found in an English law book." *Ex parte Gould*, 60 Tex. Crim. 442, 447 (1910) (citation omitted) (quoting James Otis).

When Texas adopted its Constitution, it sought to outlaw such methods once and for all. The Framers enshrined robust provisions barring unreasonable searches and seizures, infringements on personal property, and executive overreach in law enforcement investigations. These provisions must be read "in light of each other." *Garofolo v. Ocwen Loan Servicing, L.L.C.*, 497 S.W.3d 474, 477 (Tex. 2016) (citation omitted). And collectively, they afford Texans protections against government intrusion that are even stronger than those under federal law.

This case concerns a modern iteration of the general warrant: the geofence warrant. Like their reviled predecessors, geofence warrants do not identify a specific

suspect based on individualized probable cause. Instead, they allow the government to rummage through the private data of countless people in the hopes of dredging up one suspect. These warrants, including the one in this case, generally follow a three-step procedure:

- Step 1: Officers submit a warrant to Google specifying a geographic area (the "geofence") and a timeframe. Google produces a list of devices that were likely within those parameters by searching its Sensorvault, a database containing "Location History" data for more than 500 million users.[2] In Google's words, Location History is "a detailed diary of everywhere a person went: from her house to her gym to her place of worship." Br. of Amicus Curiae Google L.L.C. in Support of Neither Party at 10, *Chatrie v. United States* (U.S. Mar. 2, 2026) (No. 25-112), 2026 WL 624354 [hereinafter "Google Amicus"]. At this step, Google does not tell law enforcement the identity of the users associated with each device.
- Step 2: Officers ask Google for more Location History of some or all of the devices that Google disclosed at Step 1—typically for a wider time

[2] All discussion of Location History in this brief pertains to how it functioned when the geofence warrant issued in this case, in 2019. Between late 2023 and July 2025, Google transitioned to storing Location History on users' own devices instead of in the Sensorvault. Google Amicus at 1–2. This does not mean law enforcement will stop seeking geofence warrants. Google could change its policies at any time, and other companies that store their users' private location information, including Apple, Lyft, Snapchat, and Uber, "have all received these warrants." *Geofence Warrants and the Fourth Amendment*, 134 Harv. L. Rev. 2508, 2512 (2021).

window than at Step 1, and without geographic limits. The officers do not return to the magistrate to secure a new warrant at this step or explain how they determined which devices to target.

- Step 3: Officers review the additional data from Step 2 to arrive at a final list of devices of interest. Google then provides identifying information for the users of those devices. Officers may also request additional information about the identified users. Again, the officers generally do not return to the magistrate to secure a new warrant for the additional information.

Thus, geofence warrants sweep up the personal data of many people based on their mere proximity to a crime. Then, without judicial oversight, law enforcement officers—not magistrates—decide which users should be subject to broader searches, and which users' subscriber information should ultimately be disclosed.

Following its split decision in *Wells v. State*, 714 S.W.3d 614 (Tex. Crim. App. 2025), this Court now has another opportunity to examine the constitutionality of geofence warrants. And while the U.S. Supreme Court may soon rule on whether the Fourth Amendment permits geofence warrants, *see United States v. Chatrie*, 136 F.4th 100 (4th Cir. 2025), *cert. granted in part*, 2026 WL 120676 (U.S. Jan. 16, 2026) (No. 25-112), that ruling will not address the Texas Constitution. *Amici* therefore submit this brief to highlight several reasons why, properly interpreted, the Texas Constitution prohibits geofence warrants like the one at issue here.

For starters, geofence searches infringe on Texans' reasonable expectations of privacy and property interests in the Location History data they unavoidably generate while carrying their cell phones. This data is even more comprehensive and revealing than cell site location information, which this Court has recognized to be intensely private. And, by Google's own description, Location History data belongs to the user. But a geofence warrant allows the government to search these revealing records for vast numbers of people without probable cause as to any of them. The search in this case encompassed an entire apartment complex and a highway feeder road—all based on the investigating detective's boilerplate claim that criminals often carry cell phones.

Moreover, the third-party doctrine does not apply to Location History, particularly under Texas law. In *Richardson v. State*, 865 S.W.2d 944 (Tex. Crim. App. 1993), this Court adopted a narrower view of the third-party doctrine, under Article I, Section 9, than federal courts had articulated under the U.S. Constitution. Although more recent Texas cases have called *Richardson* into question, subsequent developments—both technological and societal—have shown that *Richardson* supplies the proper framework for determining whether Texans have a constitutional interest in the sensitive data they generate simply by participating in modern society. Under that framework, the question is whether a customer's limited disclosure of data to the provider of an essential service should be treated as opening the door to

government access. The answer for Location History is no. Using a cell phone does not invite the government to see everywhere we have been.

Finally, geofence warrants violate the Texas Constitution's strict separation-of-powers safeguards. Magistrates have a constitutional duty to ensure that a warrant is both supported by a showing of probable cause and identifies, with particularity, what can be searched and seized. Geofence warrants do neither. They allow law enforcement and private parties (here, Google employees) to decide, without judicial oversight, whose data to corral and de-anonymize. For example, in this case, when Google returned an initial list of 18 responsive devices, the detective did not narrow the list. Instead, he requested more Location History for every user, and he expanded the time window for the search beyond what the magistrate had authorized. As is typical of geofence warrants, the magistrate played no role in reviewing that expansion of the search. This delegation of judicial powers to executive officers is impermissible.

Accordingly, this Court should hold that the Texas Constitution categorically prohibits geofence warrants. At a minimum, the Court should issue guidance to mitigate the constitutional harms these warrants inflict on innocent Texans, including that (1) the temporal and geographic parameters articulated in the initial geofence warrant must be as narrow as practicable to minimize the intrusion into

innocent people's data; and (2) law enforcement agents must obtain a new warrant when they request additional information following the initial geofence search.

ARGUMENT

When interpreting the Texas Constitution's search-and-seizure protections, instead of departing from Fourth Amendment case law "just for the sake of being different," this Court asks whether that case law is "persuasive." *Holder v. State*, 595 S.W.3d 691, 701–02 & n.18 (Tex. Crim. App. 2020). Here, regardless of how the U.S. Supreme Court rules in *Chatrie*, there are three persuasive reasons to hold that Texas law limits the government's use of geofence warrants. First, the Texas Constitution and Texas statutes fiercely protect not only personal privacy, but also personal property. Those protections support reading the Texas Constitution more broadly than the U.S. Constitution where, as with geofence warrants, the government invades the privacy and digital property interests of countless innocent people. *See* Argument I.A., *infra*. Second, geofence warrants implicate the Texas Constitution's explicit separation-of-powers command, which is not at issue in *Chatrie*. *See* Argument II, *infra*. And third, unlike a federal court having to craft a constitutional rule that works for the whole country, this Court can provide this state's courts with much-needed guidance on geofence warrants tailored to this state's concerns and fulsome constitutional protections. *See* Argument III, *infra*.

I. Geofence warrants violate the Texas Constitution because they authorize overbroad exploratory searches to which the third-party doctrine does not apply.

The government's acquisition of geofence data constitutes a search under the Texas Constitution because it sweeps up profoundly revealing personal data implicating privacy and property interests not just for one potentially guilty person, but for countless innocent people. The geofence warrants that purport to authorize such searches are neither supported by probable cause nor sufficiently particularized. Like the general warrants the Texas Framers abhorred, geofence warrants authorize wide-ranging, exploratory rummaging without probable cause as to every person—and sometimes *any* person—whose data is searched. They therefore implicate three provisions of the Texas Constitution: Article I, Section 9, which prohibits "all unreasonable seizures or searches" and requires warrants to "describ[e]" what is to be searched or seized "as near as may be"; Article I, Section 17, which provides that "[n]o person's property shall be taken, damaged, or destroyed for or applied to public use without adequate compensation"; and Article I, Section 19, which commands that "[n]o citizen of this State shall be deprived of . . . property . . . except by the due course of the law of the land."

A. The government conducts a search when it executes a geofence warrant because it infringes on Texans' reasonable expectations of privacy and property interests.

Executing a geofence warrant constitutes a search. A search occurs under the Texas Constitution when the government breaches a person's reasonable expectation of privacy or intrudes upon their property. *Richardson*, 865 S.W.2d at 949; *State v. Huse*, 491 S.W.3d 833, 840 (Tex. Crim. App. 2016). A geofence warrant allows the government to do both, and this dual intrusion—in the aggregate—supplies a persuasive reason to hold that geofence warrants trigger the protections of Article I, Sections 9, 17, and 19. *See Holder*, 595 S.W.3d at 701–02 & n.18.

First, people have a reasonable expectation of privacy in their Location History. This Court already recognized in *Holder* that there is a reasonable expectation of privacy in cell site location information (CSLI). 595 S.W.3d at 703. CSLI is "a time-stamped record" of a cell phone's location generated when it "connect[s] to a set of radio antennas called 'cell sites.'" *Id.* at 699 (quoting *Carpenter v. United States*, 585 U.S. 296, 300 (2018)). In *Holder*, this Court expressed "grave concerns" about the government's use of CSLI to track people retrospectively. *Id.* at 703. Those concerns are graver still with Location History. Whereas CSLI "narrow[s] location to dozens or hundreds of city blocks," Location History can "pinpoint a device's location within twenty meters." Google Amicus at 29 (citations omitted). Location History is also logged more frequently—"on

average, every two minutes." *United States v. Smith*, 110 F.4th 817, 823 (5th Cir. 2024), *cert. denied*, 146 S. Ct. 356 (2025) (citation omitted). And while CSLI is collected "only when a cell phone user places or receives a call," Location History records the user's whereabouts "on an ongoing basis, including when the device [is] not in active use." Google Amicus at 29 (citations omitted). Thus, Location History allows the government to achieve "near perfect surveillance" over our "privacies of life." *Holder*, 595 S.W.3d at 701 (quoting *Carpenter*, 585 U.S. at 311–12); *see also State v. Granville*, 423 S.W.3d 399, 408–09, 417 (Tex. Crim. App. 2014) (holding, even before *Riley v. California*, 573 U.S. 373 (2014), that a person has a "reasonable expectation of privacy in the contents of his cell phone").

Second, Texans have a property interest in their Location History. Property is "a bundle of rights" that includes "the right to possess, use and dispose of" a thing. *Jim Olive Photography v. Univ. of Houston Sys.*, 624 S.W.3d 764, 773 (Tex. 2021) (citations omitted). Texas law guards property rights with exceptional fervor: "One of the most important purposes of our government is to protect private property rights," which are "fundamental, natural, inherent, inalienable," and "preexist[] even constitutions." *Kopplow Dev., Inc. v. City of San Antonio*, 399 S.W.3d 532, 535 (Tex. 2013) (quoting *Eggemeyer v. Eggemeyer*, 554 S.W.2d 137, 140 (Tex. 1977)). And Texas law treats computer data as property. *See, e.g.*, Tex. Penal Code § 33.01(16) (defining "property" to include "[electronic] data"). Accessing such

property "without the effective consent of the owner" is a crime, just like any other trespass. *See* Tex. Penal Code §§ 33.02 ("Breach of Computer Security"), 30.05 ("Criminal Trespass").

Location History has all the hallmarks of property. Users can review, edit, or delete their Location History from Google's servers. Google Amicus at 10. Users can also exclude others from their Location History—"one of the most essential sticks in the bundle of [property] rights." *Lightning Oil Co. v. Anadarko E&P Onshore, LLC*, 520 S.W.3d 39, 48 (Tex. 2017) (citation and internal quotation marks omitted); *see In re Sun Coast Res., Inc.*, 562 S.W.3d 138, 158 (Tex. App.—Houston [14th Dist.] 2018, *no pet.*) ("Consistent with long-standing Texas property law and the exclusionary interest inherent in property ownership," cell phone owners "generally have the right . . . to exclude others from the content of text messages stored on the device."). Location History is stored in users' accounts, "protected with passwords," and "inaccessible to the public." Google Amicus at 32, 37. That is why Google describes Location History as "the user's *personal* records." *Id.* at 3.

A geofence search infringes on both privacy and property interests. At Step 1, the search sifts through the "comprehensive, precise, and revealing" data of *every* user in Google's Sensorvault—an estimated 592 million people as of 2018—to determine whether they fall within the warrant's parameters. *Id.* at 27; *Smith*, 110 F.4th at 823. A single geofence may sweep up the Location History of potentially

"hundreds or thousands" of people, without any individualized suspicion. Google Amicus at 30. At Step 2, law enforcement expands the timeframe for which Location History is sought and dispenses with geographic parameters. At Step 3, not only is the data de-anonymized, but law enforcement may also seek even more information of an even more intimate nature about the identified users. *See, e.g.*, *Wells*, 714 S.W.3d at 634 (Newell, J., concurring and dissenting) ("[T]he third step of the geofence warrant sought six months of prior IP history[3] in addition to identifying subscriber information.").

Thus, across the three Steps, geofence searches unreasonably invade privacy and defeat the property right to exclude others from private data—all in violation of Article I, Sections 9, 17 and 19. Interpreting its own state constitution, the Minnesota Supreme Court recently reached a similar conclusion. *See State v. Contreras-Sanchez*, No. A22-1579, 2026 WL 1015919, at *1 (Minn. Apr. 15, 2026) (holding that executing a geofence warrant was "a search under the Minnesota Constitution").

The State characterizes these geofence intrusions as "limited" in "quality and quantity." State's Cross-Pet. Br. 42–43. That is not accurate. With geofence searches, even a brief window of time can expose the presence of hundreds of people in "private residences, doctor's offices, political headquarters, and other potentially

[3] IP history is a "record . . . of websites visited or services accessed on a cellphone." *Wells*, 714 S.W.3d at 634 (Newell, J., concurring and dissenting). "[T]here is no 'opt-in'" for these records; "[c]ellphones log IP history whenever the user accesses the internet." *Id.*

revealing locales." *Holder*, 595 S.W.3d at 700 (quoting *Carpenter*, 585 U.S. at 311). And "[e]ven a small geographic area for a short period of time" can encompass "hundreds or thousands of people." Google Amicus at 12. In any event, the geofence can also be expansive. Law enforcement officers often draw broad geofence parameters, sometimes spanning "several square miles" and "several days." *Id.* One such warrant, for example, covered "a combined 2.5 square miles of San Francisco for a cumulative period of two-and-a-half days," and another covered nearly all of Aspen and Vail, Colorado, for multiple hours. *Id.* at 13–26. Such dragnets are not "limited."

Beyond being inaccurate, the State's attempt to downplay the intrusiveness of geofence searches fails to account for Texas's protections for private property. The government is not free to engage in a "limited" trampling of innocent people's data, for much the same reason as an individual cannot take someone else's car for a "limited" joyride. *Cf.* Tex. Penal Code § 31.07. Under Texas law, "every invasion of private property, be it ever so minute, is a trespass." *Gould*, 60 Tex. Crim. at 447–48. Understandably so. As this Court recently explained, under the "property-based trespassory test," a search occurs whenever "law enforcement physically intrude[s] into a constitutionally protected area to obtain information." *State v. Organ*, 726 S.W.3d 346, 356, 360 (Tex. Crim. App. 2025). "This is consistent with English common-law's understanding that the 'law holds the property of every man so

sacred, that no man can set foot upon his neighbour's close without his leave; if he does he is a trespasser, though he does no damage at all.'" *Id.* at 355–56 (quoting *Entick v. Carrington*, 95 Eng. Rep. 807 (C.P. 1765)). Thus, *Organ* held that "a search undoubtedly occurred" when a drug-detection "dog's nose entered [a] vehicle's interior several times through the open passenger side window." *Id.* at 360–61 (cleaned up). It did not matter that the intrusion was brief.[4]

The State also suggests that no search occurs at Steps 1 and 2, when the government obtains Location History from all cell phones within the geofence, because that data is anonymized. State's Cross-Pet. Br. 50 n.34. This argument does not hold up either. "A search is a search, even if it happens to disclose nothing but the bottom of a turntable," *Arizona v. Hicks*, 480 U.S. 321, 325 (1987), and even if the government does not initially know who was searched, *see, e.g.*, *Lippert v. State*, 664 S.W.2d 712, 715–16 (Tex. Crim. App. 1984) (en banc) (frisk of initially unidentified individual was a search). Again, this is particularly true under Texas law. The prohibition against accessing someone's data contains no anonymization defense, *see* Tex. Penal Code § 33.02; in Texas, intruding into someone's phone or data and perusing their private pictures or diary does not become lawful just because the intruder claims not to know the identity of the owner.

[4] Here, the intrusions may be long-lasting, as the geofence warrant did not require the government to destroy data that turned out to be irrelevant to the investigation.

In fact, the data anonymization at Steps 1 and 2 does not necessarily prevent the government from connecting the data to a person. In *Chatrie*, an expert witness showed that, at Step 2, the identities of several people "could be discerned by combining the information on their movements with public information like tax records and social media postings." Petitioner's Opening Br. at 44, *Chatrie v. United States* (U.S. Feb. 23, 2026) (No. 25-112), 2026 WL 561004; *see also* Herbert B. Dixon Jr., *Your Cell Phone Is A Spy!*, Judges' J., Summer 2020, at 34–36 (noting that "deanonymizing . . . [CSLI] data was a straightforward task" for researchers, who were "able to track federal employees," including "judicial staff").[5]

Consequently, when the State obtains individuals' private Location History, it conducts a search.

B. Texas's third-party doctrine does not apply to Location History.

The State argues that it does not even need a warrant to acquire the Location History of any law-abiding Texan—or *every* Texan—because cell phone users have supposedly disclosed their locations voluntarily to a third party (Google). *See* State's Cross-Pet. Br. 26–27. As Mr. Nguyen details, the State's argument cannot be squared with the Fourth Amendment. *See* Appellant's Br. on Merits 35–41. It is even less tenable under Article I, Section 9. Although this Court has taken different

[5] *Available at* https://www.americanbar.org/content/dam/aba/publications/judges_journal/vol59no3-jj2020-tech.pdf.

approaches to applying the third-party doctrine over the years, the version it first articulated in *Richardson v. State* was narrower than the federal doctrine. 865 S.W.2d 944. Subsequent developments—including this Court's recent decision in *Holder*—have shown that the *Richardson* framework is well-suited to determining whether the third-party doctrine should apply to digital data. Accordingly, this Court should reaffirm the *Richardson* framework and hold that the third-party doctrine does not apply to Location History under the Texas Constitution.

1. This Court should reaffirm the narrow form of the third-party doctrine articulated in *Richardson* because it effectuates the Texas Constitution's protections for private data.

Texas courts have long stressed that "[o]ur constitution has independent vitality," and "court[s] ha[ve] the power and duty to protect the additional state guaranteed rights of all Texans." *LeCroy v. Hanlon*, 713 S.W.2d 335, 339 (Tex. 1986). In the search-and-seizure context, this Court "interprets the Texas Constitution by '[its] own lights.'" *Holder*, 595 S.W.3d at 697–98 (citation omitted). To be sure, this Court "will not read Article I, [Section] 9 differently than the Fourth Amendment in a particular context simply because [it] can." *Id.* at 701–02 (alteration in original). But nor will the Court reflexively tether Article I, Section 9 to federal doctrine. *See id.* at 703 & n.18. The ultimate question is "whether the [U.S.] Supreme Court's reasoning makes more sense than the alternatives." *Id.* at 697–98.

In *Richardson*, this Court concluded that it did not make sense to follow the U.S. Supreme Court's construction of the third-party doctrine. 865 S.W.2d at 951–53. That doctrine originated with *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979). *Miller* held that the government needed no warrant to obtain a customer's bank records, including canceled checks and monthly statements, because they were "the business records of the banks" rather than the customer's "private papers." 425 U.S. at 440, 442. Similarly, *Smith* held that the government's use of a pen register was not a search because a person lacks a reasonable expectation of privacy over telephone numbers they "voluntarily" transmitted to the telephone company by dialing. 442 U.S. at 743.

Richardson determined that the third-party doctrine has a narrower scope under the Texas Constitution and declined to apply it to pen registers. 865 S.W.2d at 953. Its reasoning, moreover, has proven to be prescient. *Richardson* identified three key questions to consider when assessing whether to apply the third-party doctrine:

(1) *How sensitive is the information?* With respect to pen registers, this Court noted that "an individual's personal contacts reveal[] an enormous amount of information," so the "unrestricted use of pen registers by the police would have a substantial and deleterious effect on privacy." *Id.* at 950 (citations and internal quotation marks omitted).

(2) *Was the customer's disclosure truly voluntary, given the demands of modern society?* This Court reasoned that telephone usage is "pervasive in our society," so it makes little sense to say "a telephone user assum[es] the risk of pen register surveillance, since the user has no practical alternative but to forego the use of the telephone altogether." *Id.* (citation and internal quotation marks omitted).

(3) *Is it "reasonable[]" to treat a customer's "limited disclosure" to the service provider as "open[ing] the door to public disclosure"? Id.* at 952. For pen registers, this Court answered no, because "society recognizes as objectively reasonable the expectation" that "the numbers [a customer] dials as a necessary incident of his use of the telephone will not be published to the rest of the world." *Id.* at 953. Indeed, this Court cautioned that the notion "that information provided to the telephone company for a limited record-keeping purpose automatically becomes available to the police for criminal investigative purposes[] should have no foundation in a free society." *Id.* at 951 (quoting *Commonwealth v. Beauford*, 327 Pa. Super. 253, 264 (1984)).

Two decades after *Richardson*, this Court hewed more closely to the federal third-party doctrine when, in *Ford v. State*, it held that the Fourth Amendment does not prohibit warrantless CSLI collection. 477 S.W.3d 321, 322 (Tex. Crim. App.

2015). Since *Ford* presented only a federal constitutional claim, *see id.* at 322 n.1, the Court looked to federal doctrine for guidance. But because the U.S. Supreme Court had not yet addressed CSLI, this Court could only rely on precedent from a different technological era. It opined that, "like the bank customer in *Miller* and the phone customer in *Smith*," a cell phone user "voluntarily availed himself of [the service provider's] cellular service." *Id.* at 331 (citation omitted). And the Court was not convinced that several days of "location data" would "reveal a comprehensive view of the specific details of [the user's] daily life." *Id.* at 335. The Court later extended its Fourth Amendment ruling to Article I, Section 9, "simply because it ma[de] more sense." *Hankston v. State*, 517 S.W.3d 112, 120 (Tex. Crim. App. 2017), *cert. granted, judgment vacated*, 585 U.S. 1028 (2018) (citation and internal quotation marks omitted).

But a year later, in *Carpenter*, the U.S. Supreme Court declined to apply the third-party doctrine to CSLI. 585 U.S. at 315–16. The Supreme Court's reasoning tracked the same three considerations this Court articulated in *Richardson*. It recognized that (1) location data is "an all-encompassing record of the holder's whereabouts" that "provides an intimate window into a person's life," *id.* at 311; (2) "in no meaningful sense does the user voluntarily assume the risk of turning over a comprehensive dossier of his physical movements" merely by using a cell phone, *id.* at 315 (cleaned up); and (3) "an individual maintains a legitimate expectation of

privacy in the record of his physical movements as captured through CSLI," even if that record is conveyed to the service provider, *id.* at 309–10. In sum, the Supreme Court explained, "mechanically applying" the logic of *Smith* and *Miller* to "the exhaustive chronicle of location information casually collected by wireless carriers today" would constitute "a significant extension of [the third-party doctrine] to a distinct category of information." *Id.* at 314.

This Court then reconsidered its prior cases "[i]n light of" *Carpenter* and held that, under Article I, Section 9, the third-party doctrine "cannot defeat a person's expectation of privacy" in historical CSLI. *Holder*, 595 S.W.3d at 698, 704. The Court acknowledged that its "reasoning [in *Ford* and *Hankston*] was expressly rejected in *Carpenter*," because "[c]ell phone location information is not truly 'shared.'" *Id.* at 703 & n.22 (quoting *Carpenter*, 585 U.S. at 315). Moreover, "[t]he Supreme Court exhaustively analyzed the privacy issues implicated by CSLI, which [*Hankston*] did not do." *Id.* at 703. And this Court took note of "society's expectation 'that law enforcement agents and others would not . . . secretly monitor and catalogue [a person's] every single movement," even if that person allows their wireless provider to collect their location data. *Id.* at 701 (quoting *Carpenter*, 585 U.S. at 310). In other words, *Holder* considered the same three questions this Court had asked in *Richardson*.

This Court should now reaffirm that, for Location History, the *Richardson* framework "makes more sense." *Holder*, 595 S.W.3d at 697–98. That framework carefully assesses the privacy implications of allowing the government to access personal data without a warrant—and may give more weight to those privacy interests than federal doctrine does. *Compare Richardson*, 865 S.W.2d at 953 (requiring a warrant for the use of pen registers), *with Smith*, 442 U.S. at 743 (not requiring a warrant for the use of pen registers). This more protective approach gives meaning to the complementary Texas constitutional protections for privacy rights, property interests, and the judicial role in reining in executive overreach. *See Garofolo*, 497 S.W.3d at 477. And the framework's grounding in *Texans'* expectations for what would be a reasonable degree of government intrusion into their digital lives spares this Court from having to predict what the U.S. Supreme Court might consider reasonable under a different constitution.

2. The third-party doctrine does not apply to Location History.

Under the three factors that *Richardson* identified and *Holder* reiterated, this Court should hold that the third-party doctrine does not apply to Location History as a matter of Texas constitutional law.

First, as detailed above, Location History reveals the "privacies of life" to an even greater degree than the CSLI at issue in *Holder*. *See* Argument I.A., *supra*.

Second, as a practical matter, it is not accurate to say that "a [cell phone] user assum[es] the risk of [Location History] surveillance." *Richardson*, 865 S.W.2d at 950. Although, in theory, users could avoid generating Location History, the realities of both daily life and cell-phone technology—especially for people who are *not* committing crimes—dictate otherwise. At all times relevant to this case, Google was telling users that their devices and core applications would not "work correctly" without Location History, Petitioner's Opening Br. at 30, *Chatrie v. United States* (U.S. Feb. 23, 2026) (No. 25-112), 2026 WL 561004; multiple apps repeatedly prompted users to enable Location History, *id.* at 29–31; and users were not informed that their phone sometimes tracked their location even when Location History was turned off, such as when they opened Google Maps or ran a Google search.[6] *See* Dixon, *supra*, at 34–36 (cautioning judges that "[e]very place judges visit could be tracked" by their cell phones, and that "many apps . . . share [location] data beyond what users have consented to under the permission requests and privacy policies"). Users were not making a conscious decision to expose their Location History to widespread collection by law enforcement. *See Holder*, 595 S.W.3d at 703 & n.22 ("Cell phone location information is not truly 'shared.'").

[6] Ryan Nakashima, *Google Tracks Your Movements, Like it or Not*, Associated Press (Aug. 13, 2018), https://www.apnews.com/828aefab64d4411bac257a07c1af0ecb.

Third, and most important, it is fundamentally reasonable for a cell phone user to expect that "the [comprehensive location data he generates] as a necessary incident of his use of the telephone will not be published to the rest of the world." *Richardson*, 865 S.W.2d at 953. Indeed, although private contracts are not dispositive of constitutional rights, Google treats location data as the user's own private data. Its "Privacy Policy specifically says that Google will not share users' personal information except in specific circumstances, like complying with lawful and enforceable warrants." Google Amicus at 41. Moreover, Google disclaims that Location History data are its business records. *Id.* at 3. That is unlike the situations in *Miller* and *Smith*, where the U.S. Supreme Court viewed the records as the *service provider's* business records, not the *customer's* "private papers." *See Miller*, 425 U.S. at 440, 442 (documents were "the business records of the banks" that were "voluntarily conveyed to the banks"); *Smith*, 442 U.S. at 743 (similar). When a third party tells users that certain data is *theirs*, users can reasonably expect that the "limited disclosure" of that data to the third party will not "open the door to public disclosure." *Richardson*, 865 S.W.2d at 952; *see Contreras-Sanchez*, 2026 WL 1015919, at *10–11 (holding that "the third-party doctrine does not apply to the location data Google stores" because "users do not assume the full risk of permanently disclosing the entirety of their location history when they use Google's products or even opt in to Google's location requests").

The notion that, simply by moving around with their belongings, people invite the government to engage in "continuous, surreptitious, precise, and permeating . . . surveillance" of their location—without a warrant—would have been unthinkable to the Framers of the Texas Constitution. *Holder*, 595 S.W.3d at 703. Yet that is exactly the power the State is claiming when it urges the Court to apply the third-party doctrine here. That claim should be rejected.

C. Geofence warrants are unconstitutional because, similar to general warrants and writs of assistance, they necessarily encompass data belonging to people who could not have committed the pertinent offense.

The fact that the government obtains geofence warrants before undertaking searches that return troves of sensitive data does not make those searches constitutional. To the contrary, geofence warrants are offensive to the Texas Constitution because, like general warrants and writs of assistance, they give the government broad discretion to conduct dragnet searches without individualized probable cause.

At the Founding, "Americans despised the British use of so-called 'general warrants'—warrants not grounded upon a sworn oath of a specific infraction by a particular individual, and thus not limited in scope and application." *Crider v. State*, 607 S.W.3d 305, 310 n.6 (Tex. Crim. App. 2020) (Newell, J., concurring) (quoting *Maryland v. King*, 569 U.S. 435, 466 (2013) (Scalia, J., dissenting)). Americans also loathed the British "writs of assistance," which "noted only the object of the

search—any uncustomed goods—and thus left customs officials completely free to search any place where they believed such goods might be." *Steagald v. United States*, 451 U.S. 204, 220 (1981). These writs were "among the key grievances that triggered the American Revolution." *El-Ali v. State*, 428 S.W.3d 824, 827 (Tex. 2014) (Willett, J., dissenting to denial of petition for review) (citation omitted). The "Texas Framers . . . were gravely concerned about general warrants"—perhaps even more so than the federal Framers, seeing as "the first Texas prohibition on unreasonable searches and seizures, unlike the Fourth Amendment, specifically cited general warrants." *Holder*, 595 S.W.3d at 702–03 & n.20.

Geofence warrants operate in much the same way as general warrants and writs of assistance. Instead of identifying a person suspected of committing the crime under investigation and authorizing a search based on individualized probable cause, geofence warrants permit the government to rummage through the private data of potentially hundreds of millions of people in the hopes of dredging up a single suspect. *See United States v. Chatrie*, 136 F.4th 100, 122 (4th Cir. 2025) (en banc) (Wynn, J., concurring in the judgment) ("[T]he very point of a geofence is to generate leads where none exist."). For every geofence warrant Google responds to, it "must search each account in its entire Sensorvault—all 592 million—to" determine which users were within the geofence. *Smith*, 110 F.4th at 824. Each of those 592 million users has a reasonable expectation of privacy and a property

interest in their Location History, *see* Argument I.A., *supra*, and the government does not have probable cause as to any of them. The search therefore violates every user's rights.

Geofence warrants like the one in this case are wholly devoid of probable cause. Although many innocent people carry cell phones, many perpetrators either do not carry cell phones during their offense or, if they do, disable Location History. *See* Google Amicus at 30–31. Thus, geofence warrants "sometimes cover *only* unrelated users." *Id.* at 30. But even when there is probable cause to believe that *one* suspect carried a Location-History-enabled phone during the offense, that probable cause does not extend to *everyone* swept up in the geofence.

Under Texas law, that hoovering up of data belonging to innocent people matters. For purposes of Article I, Section 9, a "person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person." *State v. Barnett*, 788 S.W.2d 572, 575 (Tex. Crim. App. 1990) (quoting *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979)). Rather, "a search . . . of a person must be supported by probable cause particularized with respect to that person." *Id.* (alteration in original) (quoting *Ybarra*, 444 U.S. at 91). Thus, this Court held in *Barnett* that even if officers had a warrant to search a home, they could not search "all vehicles on the premises" unless they "explain under oath to a magistrate what probable cause exists to search [each of] those vehicles." *Id.* at

576. Similarly, the Texas Supreme Court invalidated warrants authorizing "officer[s] to seize all intoxicating liquors found in" places where they were being illegally sold or kept for sale. *Dupree v. State*, 102 Tex. 455, 468–69 (1909). Because the warrants were not confined to liquors that were actually being unlawfully sold or kept, the Court decried them as, "in . . . effect," "a general warrant[]." *Id.*

Likewise with geofence warrants. By definition, a geofence targets people based on their "mere propinquity" to an alleged crime. *Barnett*, 788 S.W.2d at 575. But the geofence warrant is not supported by "probable cause particularized with respect to" each person. *Id.* It therefore does not justify the search of their private data. *See Smith*, 110 F.4th at 837 n.11 (holding that "probable cause is required for each person's obtained records," *i.e.*, each "Google account[] containing Location History data" (cleaned up)). The non-digital analogue—a government agent searching every person and home within a certain distance from a crime scene merely because they are close to the scene—would not have been accepted when Article I, Section 9 was adopted and remains plainly unlawful today. *See* Tr. of Oral Argument at 99:19–103:25, *Chatrie v. United States* (No. 25-112) (counsel for the government conceding that a warrant would not be valid if it purported to authorize a search of all rooms in a hotel based on the premise that there is a gun in one of the rooms, and "very likely not" valid if it purported to authorize a search of all units in a storage facility to look for contraband in one unit).

II. Geofence warrants transfer judicial authority to law enforcement and private parties in violation of the separation of powers required by the Texas Constitution.

Geofence warrants also violate the robust separation-of-powers principles enshrined in Article II, Section 1, of the Texas Constitution. They do so by impermissibly delegating to law enforcement the magistrate's power to decide whose data will be hoovered up and de-anonymized.

A. Warrants implicate acute separation-of-powers concerns under the Texas Constitution.

The Texas Constitution expressly divides state government into three branches and instructs that, except in rare circumstances, none "shall exercise any power properly attached to either of the others." Tex. Const. art. II, § 1. Because this text appears nowhere in the U.S. Constitution, it suggests that "Texas would more aggressively enforce separation of powers" than the federal government. *State v. Rhine*, 297 S.W.3d 301, 315 (Tex. Crim. App. 2009) (Keller, P.J., concurring).

Such enforcement is necessary in the warrant context because issuing warrants is a power that the Texas Constitution expressly attaches to the judiciary. It commands that a neutral magistrate must determine whether there is probable cause to issue a warrant, Tex. Const. art. I, § 9, and separation-of-powers principles prohibit the outsourcing of that duty to another branch, *see Rodriguez v. State*, 232 S.W. 3d 55, 59–60 (Tex. Crim. App. 2007) (explaining that this requirement is to ensure that probable cause determinations are made by a neutral magistrate rather

than a police officer). This strict delineation of roles "substitutes the detached and neutral judgment of a magistrate in the place of the suspicions and intuitions of law enforcement officers." *Barnett*, 788 S.W.2d at 576. It also embodies the "basic constitutional doctrine that individual freedoms will best be preserved through a separation of powers," and "minimize[s] the risk of unreasonable assertions of executive authority." *Arkansas v. Sanders*, 442 U.S. 753, 759 (1979) (citations omitted).[7]

Texas statutory law also channels this doctrine by requiring that search warrants be issued by judicial officers, not police officers. *See* Tex. Code Crim. Proc. art. 18.01, art. 18.02. Together, these constitutional and statutory provisions ensure that warrants are "drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime." *Clemons v. State*, 605 S.W.2d 567, 570 n.7 (Tex. Crim. App. 1980).

These provisions strictly prohibit delegating judicial determinations to law enforcement. "The requirement that warrants shall particularly describe the things to be seized" means "*nothing* is left to the discretion of the officer executing the warrant." *Walthall v. State*, 594 S.W.2d 74, 78 (Tex. Crim. App. 1980) (emphasis

[7] *See also State v. Geraw*, 795 A.2d 1219, 1221 (Vt. 2002) (explaining that the warrant requirement "operates as a potent and immutable check on the power of the executive branch"); *State v. Hobbs*, 975 N.E.2d 965, 971 (Ohio 2012) (issuance of warrant by a dual judicial and executive actor "blurs the separation and threatens the independence of the executive and judicial functions").

added) (citation omitted). Further, magistrates cannot sidestep their duty by determining probable cause *ex ante*, in anticipation that certain facts *will* exist when police execute the warrant. *See Barnett*, 788 S.W.2d at 577. In *Barnett*, while executing a search warrant at someone's home, police searched the car of another person who drove up to the home. *See id.* at 573–74. Although that search arguably fell within the text of the warrant, because the warrant affidavit described the object of the search as the home and "all vehicles . . . on the premises," this Court ruled the search unlawful. *Id.* at 575. It reasoned that no "probable cause [was] expressed in the warrant affidavit" as to the car that drove up during the search. *Id.* at 577. It did not matter that the officers claimed to know facts that would have supported a warrant at the time of the search, because "[n]one of the facts" had been "conveyed to the magistrate." *Id.*

B. Geofence warrants violate the Texas Constitution's separation-of-powers commands.

Geofence warrants run afoul of Texas's separation-of-powers safeguards because they delegate, to police officers and Google employees, crucial decisions about what to search and seize.

This delegation unfolds at Steps 2 and 3, when law enforcement decides whether to obtain additional information about each device that was disclosed at Step 1 while the magistrate remains sidelined. At Steps 2 and 3, officers do not inform a magistrate whether they have narrowed the list of devices, what reasoning

guided any narrowing, which facts justify obtaining additional data on particular devices, and which specific data there is probable cause to obtain. There is no judge to ensure that these additional searches and seizures are grounded in probable cause or that police do not unreasonably invade the privacy of innocent Texans. In this case, Detective Mahoney, not a magistrate, decided at Step 2 to obtain Location History for all 18 devices disclosed at Step 1. *Nguyen v. State*, 722 S.W.3d 237, 241–42 (Tex. App.—Austin 2025, *pet. granted*). Seventeen of those devices had no connection to the offense. *See id.* at 242. In short, far from leaving "nothing . . . to the discretion of the officer executing the warrant," *Walthall*, 594 S.W.2d at 78, geofence warrants leave officers with expansive discretion to determine the scope and objects of the search, *see Contreras-Sanchez*, 2026 WL 1015919, at *16 (concluding that the geofence warrant at issue "did not effectively limit police discretion and authorized impermissible exploratory rummaging" at Step 2).

Moreover, geofence warrants delegate these crucial decisions *ex ante*, at Step 1, based on the mere hope that probable cause *may be developed* about an unknown person at some point in the future. A geofence warrant thus allows officers to acquire additional information without demonstrating to the magistrate that the facts disclosed at Step 1 actually constituted probable cause justifying the greater intrusion. This problem cannot be cured by specifying parameters for the later steps in the warrant—for example, an expanded time window that begins an hour earlier

and ends an hour later than the initial window. It must be the magistrate—not the executing officer—who determines whether there is probable cause to obtain that additional information the officer desires. The warrant in *Barnett* purported to cover "all vehicles . . . on the premises," but that did not validate the search of a car as to which the warrant application supplied no probable cause. 788 S.W.2d at 575, 577. In the same way, a geofence warrant cannot validate a search pertaining to devices, as yet unknown to the magistrate, that an officer will decide to target following the initial dragnet search. Indeed, there may be no such device at all, given that the culprit may not even have been carrying a phone that was transmitting their location information at the time of the offense.

III. At a minimum, this Court should provide guidance to limit unreasonably intrusive geofence searches.

Even if this Court concludes that some geofence warrants may be permissible, it should issue guidance to mitigate the constitutional harms they inflict on innocent Texans. In enforcing state constitutional safeguards, state courts are free to tailor rules to state-specific conditions, such as "differences in culture, geography, and history." Jeffrey S. Sutton, *51 Imperfect Solutions: States and the Making of American Constitutional Law* 17 (2018). By contrast, "[f]ederalism considerations may lead the U.S. Supreme Court to underenforce (or at least not to overenforce) constitutional guarantees in view of the number of people affected and the range of jurisdictions implicated." *Id.* at 175. Thus, no matter how the U.S. Supreme Court

resolves *Chatrie*, this Court should, at a minimum, articulate the following constraints on geofence warrants as a matter of Texas constitutional law.

First, this Court should instruct magistrates and lower courts that the geographic and temporal parameters given in a geofence warrant must be as narrow as practicable to minimize sweeping up the information of innocent people. This follows from the text of Article I, Section 9. Whereas the Fourth Amendment requires a warrant to "particularly describ[e] the place to be searched, and the persons or things to be seized," U.S. Const. amend. IV, "the imperative demand of the [Texas] Constitution is that no warrant shall issue without first describing them '*as near as may be*,'" *Gould*, 60 Tex. Crim. at 446 (emphasis added) (quoting Tex. Const. art. I, § 9). "The purpose of this [language] is to define and limit 'as near as may be' the power of officers to invade the premises of the citizen." *Dupree*, 102 Tex. at 468. Accordingly, geofences that encompass busy commercial properties, large residential buildings, or high-traffic stretches of road should not be permitted. Geofences with extended timeframes—certainly those that span multiple hours—should likewise be prohibited.

Second, this Court should instruct magistrates and lower courts that, when law enforcement agents seek additional information that was not particularly described in the original geofence warrant, they must obtain a new warrant. For instance, when officers seek additional Location History for certain users at Step 2, or when they

seek subscriber information at Step 3 for devices that were not specifically identified in the initial warrant, they must inform the magistrate of the facts that gave rise to probable cause to believe that such information would constitute evidence of the alleged crime. This multi-warrant procedure will allow a magistrate to ensure that the list of devices for which expanded Location History is sought at Step 2 is appropriately narrowed, and that the disclosure of any additional information at Step 3 is supported by probable cause.

Notably, the federal government acknowledged in *Chatrie* that a multi-warrant process is practicable. It said that officers could obtain "a separate warrant at steps 2 and 3 and a total of three warrants." Tr. of Oral Argument at 120:3–121:19, *Chatrie v. United States* (No. 25-112).

Third, this Court should require law enforcement, when applying for a geofence warrant, to explain to the magistrate exactly how the technology works and how the search will be conducted. Without a thorough understanding of, among other things, the accuracy and reliability of the location data at issue, magistrates cannot make informed probable cause determinations. Notably, when Google has provided Location History in response to geofence warrants, it has included "a 'confidence interval' indicating Google's confidence in that estimated location." *Smith*, 110 F.4th at 824. "According to Google, it aims to accurately capture roughly 68 percent of users within its confidence intervals. In other words, there is a 68

percent likelihood that a user is somewhere inside the confidence interval." *Id.* (cleaned up). If law enforcement officers candidly inform magistrate judges that they are applying for warrants to obtain a list of devices that have just a 68% chance of being in or around the geofenced area, magistrates may ask more probing questions and require additional safeguards to limit intrusion on innocent third parties.

Fourth, courts should require a demonstrable nexus between the crime and the data sought, instead of assuming that a geofence search will be fruitful merely because cell phone use is widespread. *See State v. Baldwin*, 664 S.W.3d 122, 123 (Tex. Crim. App. 2022) (holding that "boilerplate language may be used in an affidavit for the search of a cell phone" only if it is "coupled with other facts and reasonable inferences that establish a nexus between the device and the offense"). Suspects may not carry phones or may have shut off location services. In these situations, *all* data swept up in a geofence search will be irrelevant to the investigation.

Fifth, courts should minimize the impact of a geofence warrant on uninvolved third parties. Unless they are prosecuted, third parties will likely not receive notice of the search. And even if they learn of it, they may have no legal recourse after the search has occurred. It is thus all the more important for magistrates to assess and mitigate intrusions on the front end. Further, mitigation efforts should include

ordering the government to segregate and destroy information about people who were not involved in the alleged crime identified in the geofence warrant.

CONCLUSION

This Court should hold that geofence warrants per se violate Article I, Sections 9, 17, and 19 and Article II, Section 1 of the Texas Constitution. In the alternative, if the Court concludes that geofence warrants may be permissible in some instances, it should provide much-needed guidance to law enforcement and magistrates to minimize unconstitutional intrusions into the private data of innocent third parties.

Dated this 13th day of May, 2026

/s/ Thomas Buser-Clancy
Thomas Buser-Clancy
(Texas Bar No. 24078344)
Savannah Kumar
(Texas Bar No. 24120098)
ACLU Foundation of Texas, Inc.
P.O. Box 8306,
Houston, TX 77288
(713) 942-8146
tbuser-clancy@aclutx.org
skumar@aclutx.org

Terry Ding*
Laura Moraff**
American Civil Liberties Union Foundation
125 Broad Street, 17th Floor
New York, NY 10004
(212) 549-2500
ttding@aclu.org
lauramoraff@aclu.org

*_Pro hac vice_ application pending
**_Pro hac vice_ application forthcoming

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE

I hereby certify that the word count in this document, which is prepared in Microsoft Word, is 8,618 in relevant part. *See* Tex. R. App. P. 9.4.

Dated this 13th day of May, 2026

/s/ Thomas Buser-Clancy
Thomas Buser-Clancy

Counsel For Amici Curiae

CERTIFICATE OF SERVICE

I hereby certify that on the 13th day of May, 2026, a true copy of the foregoing petition was served by this Court's e-filing system on the following counsel:

- Kurt S. Hopke at kurthopke@gmail.com;
- Mark W. Bennett, Patrick F. McCann, and Alex Macias at mb@iacls.org;
- Joshua D. Presley at preslj@co.comal.tx.us; and
- Stacey Soule at information@spa.texas.gov.

Dated this 13th day of May, 2026

/s/ Thomas Buser-Clancy
Thomas Buser-Clancy

Counsel For Amici Curiae

Automated Certificate of eService

This automated certificate of service was created by the efiling system. The filer served this document via email generated by the efiling system on the date and to the persons listed below. The rules governing certificates of service have not changed. Filers must still provide a certificate of service that complies with all applicable rules.

Christopher Clay on behalf of Thomas Buser-Clancy
Bar No. 24078344
cclay@aclutx.org
Envelope ID: 114862676
Filing Code Description: Brief
Filing Description: Brief of Amici Curiae In Support of Appellant
Status as of 5/13/2026 4:51 PM CST

Case Contacts

Name	BarNumber	Email	TimestampSubmitted	Status
Joshua Presley	24088254	preslj@co.comal.tx.us	5/13/2026 4:04:45 PM	SENT
Stacey Soule	24031632	information@spa.texas.gov	5/13/2026 4:04:45 PM	SENT
Patrick McCann	792680	writlawyer@outlook.com	5/13/2026 4:04:45 PM	SENT
Kurt Hopke	24039931	kurthopke@gmail.com	5/13/2026 4:04:45 PM	SENT
Mark Bennett		mb@iacls.org	5/13/2026 4:04:45 PM	SENT
Mark Bennett		mb@ivi3.com	5/13/2026 4:04:45 PM	SENT
Jacqueline HaganDoyer		jdoyer@comalcounty.gov	5/13/2026 4:04:45 PM	SENT
Laura Moraff		lauramoraff@aclu.org	5/13/2026 4:04:45 PM	SENT
Savannah Kumar		skumar@aclutx.org	5/13/2026 4:04:45 PM	SENT
Terry Ding		ttding@aclu.org	5/13/2026 4:04:45 PM	SENT