No. 25-112

In the Supreme Court of the United States

OKELLO T. CHATRIE,
Petitioner
v.

UNITED STATES OF AMERICA,
Respondent

On Writ of Certiorari to the United States Court of Appeals for the Fourth Circuit

BRIEF AMICUS CURIAE OF THE AMERICAN CENTER FOR LAW AND JUSTICE IN SUPPORT OF NEITHER PARTY

JAY ALAN SEKULOW
Counsel of Record
JORDAN A. SEKULOW
STUART J. ROTH
ANDREW J. EKONOMOU
GEOFFREY R. SURTEES
NATHAN J. MOELKER
LIAM R. HARRELL
AMERICAN CENTER FOR LAW & JUSTICE
[redacted]

Counsel for Amicus Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES iii

INTEREST OF AMICUS 1

SUMMARY OF ARGUMENT 2

ARGUMENT 4

I. THE FOURTH AMENDMENT PROTECTS PROPERTY RIGHTS, NOT MERELY PRIVACY EXPECTATIONS 4

A. The "Expectation of Privacy" Framework Has Untethered Fourth Amendment Doctrine from Its Constitutional Moorings 5

B. Location History is Property of Users 10

C. A Property-Based Analysis Resolves This Case Without Recourse to Amorphous Balancing 12

D. Google's "Clickwrap" Agreements Cannot Establish the Voluntary Disclosure Required to Invoke the Third-Party Doctrine. 13

II. GEOFENCE WARRANTS PRESENT SERIOUS PARTICULARITY DANGERS THAT DEMAND A CLEAR CONSTITUTIONAL FRAMEWORK 20

A. General Warrants Were the Chief Evil the Fourth Amendment Was Designed to Prevent 20

B. Geofence Warrants Pose Serious Dangers of Becoming General Warrants in Digital Form. 22

CONCLUSION 25

TABLE OF AUTHORITIES

Cases ***Page(s)***

Airbnb, Inc. v. Doe,
336 So. 3d 698 (Fla. 2022) 16

Bazemore v. Jefferson Cap. Sys., LLC,
827 F.3d 1325 (11th Cir. 2016) 17

Berkson v. Gogo LLC, 97 F. Supp. 3d 359
(E.D.N.Y. 2015)..... 17

Berman v. Freedom Fin. Network, LLC,
30 F.4th 849 (9th Cir. 2022)..... 17

Carpenter v. United States,
585 U.S. 296 (2018) 4-11, 13, 15, 22

Coolidge v. New Hampshire,
403 U.S. 443 (1971) 22, 23

Cullinane v. Uber Techs., Inc.,
893 F.3d 53 (1st Cir. 2018)..... 17

Ex parte Jackson,
96 U.S. 727 (1878) 3, 9, 10

Hosanna-Tabor Evangelical Lutheran Church & Sch. v. EEOC, 565 U.S. 171 (2012)..... 1

In re Zappos.com, Inc.,
893 F. Supp. 2d 1058 (D. Nev. 2012) 17

Katz v. United States,
389 U.S. 347 (1967) 2, 4, 6, 13, 18

Kyllo v. United States,
533 U.S. 27 (2001) 4

Lamb's Chapel v. Center Moriches Sch. Dist., 508
U.S. 384 (1993) 1

Marron v. United States,
275 U.S. 192 (1927) 22

Marshall v. Georgetown Mem'l Hosp.,
112 F.4th 211 (4th Cir. 2024)..... 17

McConnell v. FEC,
540 U.S. 93 (2003) 1

Minnesota v. Carter,
525 U.S. 83 (1998) 6

Nieves v. Bartlett,
587 U.S. 391 (2019) 21

Pleasant Grove City v. Summum,
555 U.S. 460 (2009) 1

Riley v. California,
573 U.S. 373 (2014) 2, 21

Smith v. Maryland,
442 U.S. 735 (1979) 7, 13, 15, 18, 19

Soldal v. Cook County,
506 U.S. 56 (1992) 9

Specht v. Netscape Communs. Corp.,
306 F.3d 17 (2d Cir. 2002)..... 17

Stanford v. Texas,
379 U.S. 476 (1965) 20

State of Washington v. Kealey,
907 P.2d 319 (Wash. Ct. App. 1995) 16

Trump v. Anderson,
601 U.S. 100 (2024) 1

United States v. Graham,
824 F.3d 421 (4th Cir. 2016) 16

United States v. Jones,
565 U.S. 400 (2012) 8, 9

United States v. Miller,
425 U.S. 435 (1976) 7, 15, 19

United States v. Smith,
110 F.4th 817 (5th Cir. 2024)..... 2, 22-24

Constitutional Provisions

U.S. CONST. amend. IV.....2, 4, 8, 21, 23

Other Authorities

10 Works of John Adams (C. Adams ed. 1856)..... 21

8 C.J.S. *Bailments* § 28 (1988)..... 11

Harvey Silverglate, *Three Felonies a Day: How the Feds Target the Innocent* (2011)..... 21

James C. Hoye, *Click—Do We Have a Deal?*, 6 SUFFOLK J. TRIAL & APP. ADVOC. 163 (2001) 14

Nancy S. Kim, *Wrap Contracts: Foundations and Ramifications* (2013) 14

Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009)..... 8, 16

William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821 (2016)..... 8

INTEREST OF AMICUS[1]

The American Center for Law and Justice ("ACLJ") is an organization dedicated to the defense of constitutional liberties secured by law. ACLJ attorneys have appeared often before this Court as counsel for parties, *e.g.*, *Trump v. Anderson*, 601 U.S. 100 (2024); *McConnell v. FEC*, 540 U.S. 93 (2003); *Pleasant Grove City v. Summum*, 555 U.S. 460 (2009); *Lamb's Chapel v. Center Moriches Sch. Dist.*, 508 U.S. 384 (1993); or for amicus, *e.g.*, *Hosanna-Tabor Evangelical Lutheran Church & Sch. v. EEOC*, 565 U.S. 171 (2012). The ACLJ has a substantial interest in this case because it presents foundational questions about the scope of constitutional protections in the digital age.

---

[1] Pursuant to Supreme Court Rule 37.6, amicus curiae states that no counsel for any party authored this brief in whole or in part, and no entity or person, aside from amicus curiae, its members, and its counsel, made any monetary contribution toward the preparation or submission of this brief.

SUMMARY OF ARGUMENT

Just over a decade ago, this Court noted that "[o]ne of the most notable distinguishing features of modern cell phones is their immense storage capacity." *Riley v. California*, 573 U.S. 373, 393 (2014). In the years since, more and more of the "digital record of nearly every aspect of [Americans'] lives," *id.*, at 395 is kept, not on the phone itself, but on remote servers, such as Google's Location Data History repository, "Sensorvault." *United States v. Smith*, 110 F.4th 817, 823 (5th Cir. 2024). The collection of so much location data opened up a novel police investigatory approach: rather than identify a suspect and search his information, search the *location* to identify those present. Such a search of Sensorvault for location data is the first step of a three-step process culminating in the identification of a particular account's owner.

This case involves that first step, asking first whether a location data search is a search, and second, whether a warrant compelling Google to complete that search is sufficient under the Fourth Amendment.

First, a search certainly occurred. The Fourth Amendment's text protects the people's right "to be secure in *their* persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. CONST. amend. IV. That language provides categorical protection for what *belongs* to a person. Yet for decades, Fourth Amendment doctrine has instead been governed by the *privacy expectations* rationale attributed (falsely, *see infra* pp. 6-7) to *Katz v. United States*, 389 U.S. 347 (1967), as well as its

progeny exempting third-party searches—a framework untethered from constitutional text and history. The solution lies in the Amendment's text. The traditional approach asked whether a house, paper, or effect was yours under law. If so, Fourth Amendment protection followed. In *Ex parte Jackson*, this Court held that sealed letters in the mail were protected "wherever they may be"—*even though entrusted to a third party*. 96 U.S. 727, 733 (1878). The same principle applies to digital records in Sensorvault. Google Location History is the user's property as explained further below. When the Government compelled Google to search this data, it searched the Petitioner's "papers" and "effects." Even applying the third-party exemption doctrine fails, since users did not voluntarily and knowingly disclose their Location History within the meaning of that doctrine.

Second, even under *Katz*, geofence warrants threaten the *particularity* requirement of the Fourth Amendment. These warrants are general warrants in digital form—the very evil the Fourth Amendment was designed to prevent. The particularity requirement serves twin purposes: ensuring neutral magistrates, not officers, control the scope of searches, and protecting the innocent from exploratory rummaging. Geofence warrants run against both objectives. They draw a virtual fence around a location and direct the service provider to search 592 million individual accounts to identify which fall within it. This sort of general warrant is precisely what the Fourth Amendment prohibits.

Location 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." *Carpenter v. United States*, 585 U.S. 296, 311 (2018) (internal citation omitted). With all this accessible at just the click of a button, meaningful limits on the discretion of law enforcement become even more essential. The Fourth Amendment provides those limits. This Court should enforce them.

ARGUMENT

I. THE FOURTH AMENDMENT PROTECTS PROPERTY RIGHTS, NOT MERELY PRIVACY EXPECTATIONS.

The Fourth Amendment protects "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. CONST. amend. IV. The Constitution's language provides categorical protection for all things in which persons have a legal property interest. The "Fourth Amendment protects people, not places." *Katz*, 389 U.S. at 351. This Court in *Carpenter* confirmed precisely this point, sustaining a Fourth Amendment challenge to government seizure of digital location records and recognizing that the Court must "assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Carpenter*, 585 U.S. at 306 (quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001)). Justice Gorsuch's separate opinion (dissenting as to the judgment but more of a concurrence on the existence of a Fourth Amendment violation) elaborated the textual foundation for this

conclusion more fully: "Under its plain terms, the Amendment grants you the right to invoke its guarantees whenever one of your protected things (your person, your house, your papers, or your effects) is unreasonably searched or seized. Period." *Id.* at 391 (Gorsuch, J., dissenting).

A. The "Expectation of Privacy" Framework Has Untethered Fourth Amendment Doctrine from Its Constitutional Moorings.

The nine separate opinions filed by fourteen Fourth Circuit judges in this case powerfully demonstrate the unworkability of the "reasonable expectation of privacy" test. Some judges concluded a search occurred, others that it did not. Even among those who found no search, there was no agreement about why. This cacophony reflects an inherent flaw in the "expectation of privacy" framework. As Justice Thomas explained in *Carpenter*, the reasonable-expectation-of-privacy test "has no basis in the text or history of the Fourth Amendment." *Id.* at 343 (Thomas, J., dissenting).

The *Carpenter* Court declined to extend the third-party exemption cases of *Smith* and *Miller*, *infra* p. 7, to the digital age, recognizing that such an extension would leave individuals with no Fourth Amendment protection in "an intimate window into [their] personal li[ves]." *Carpenter*, 585 U.S. at 311, 316. The separate opinions further illuminated the "expectation of privacy" framework's structural weaknesses. As Justice Gorsuch noted, "*Katz* has yielded an often unpredictable—and sometimes unbelievable—jurisprudence." *Id.* at 394 (Gorsuch, J.,

dissenting). The test misconstrues virtually every word of the Fourth Amendment. It focuses on "privacy" when the text speaks of being "secure." It asks about "expectations" when the text protects objective things: property interests in "persons, houses, papers, and effects." And it invites judges to make *sociological* judgments about what society is prepared to recognize as reasonable—an inquiry untethered from law or history. It offers "no plausible foundation in the text of the Fourth Amendment" and provides no meaningful guidance to law enforcement, magistrates, or lower courts. *Id.* at 346 (Thomas, J., dissenting) (quoting *Minnesota v. Carter*, 525 U.S. 83, 97 (1998) (opinion of Scalia, J.)).

Curiously, *Katz* itself never said that the proper Fourth Amendment test looks to one's "reasonable expectation of privacy." To the contrary, the *Katz* Court explicitly declared that Fourth Amendment "protections go further [than intrusion on privacy], and *often have nothing to do with privacy at all*." 389 U.S. at 350 (emphasis added). The turn of phrase *Katz* is best known for actually comes, not from the majority (which, if anything, said the opposite), but from Justice Harlan's separate concurrence, 389 U.S. at 360. *Katz* itself properly held that the Fourth Amendment protects a person's private phone calls, regardless of the fact that the calls were made in a public place (a phone booth), 389 U.S. at 348, and there was no "physical penetration" of Katz's location, *id.* at 352, and, of course, Katz did not own the phone, phone lines, or receiver at the other end. His messages traversed the property of third parties. The *Katz* Court nevertheless found a Fourth Amendment violation. Thus, it is the (misbegotten) ghost of *Katz*,

and not *Katz* itself, which has spread abroad the "expectation of privacy" test.

This case illustrates one of the most glaring problems with the "ghost of *Katz*" test. This Court has held that individuals have no Fourth Amendment interests in business records that are possessed, owned, and controlled by a third party. *United States v. Miller*, 425 U.S. 435 (1976); *Smith v. Maryland*, 442 U.S. 735 (1979) (superseded by statute). These decisions were fundamentally premised on the Court's use of a "reasonable expectation of privacy" test without any application of the actual history and text of the Fourth Amendment. *Katz*, of course, itself found a Fourth Amendment violation despite the fact that the phone booth, phone lines, and receiver at the other end were all owned and controlled by third parties. The *Carpenter* majority similarly declined to extend the third-party exemption doctrine to digital location data precisely because doing so would give the government virtually unrestricted access to "a detailed chronicle of a person's physical presence compiled every day, every moment, over several years." *Carpenter*, 585 U.S. at 315. "Such a chronicle implicates privacy concerns far beyond those considered in *Smith* and *Miller*." *Id.*

As Justice Gorsuch asked,

> What's left of the Fourth Amendment? Today we use the Internet to do most everything. . . Countless Internet companies maintain records about us and, increasingly, for us. Even our most private documents—those that, in other eras, we would have locked safely in a desk drawer or destroyed—now reside on third party servers. *Smith* and *Miller*

> teach that the police can review all of this material[.]

Carpenter, 585 U.S. at 387 (Gorsuch, J., dissenting).

Justice Gorsuch has thoroughly unpacked the deep-rooted problems with the third-party doctrine: "countless scholars, too, have come to conclude that the 'third-party doctrine is not only wrong, but horribly wrong.'" *Carpenter*, 585 U.S. at 388-389 (quoting Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563, n. 5, 564 (2009)). It is "quite dubious." *Id.* at 389 (quoting William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821, 1872 (2016)). Justice Gorsuch highlights how broadly the third-party doctrine sweeps and the practical implications of the doctrine: "In the end, what do *Smith* and *Miller* add up to? A doubtful application of *Katz* that lets the government search almost whatever it wants whenever it wants." *Id.* at 391.

The solution to this overbreadth lies in returning to a more plain and direct understanding of the Fourth Amendment. The text of the Fourth Amendment protects "[t]he right of the people to be secure in ***their*** persons, houses, papers, and effects," U.S. CONST. amend. IV (emphasis added), not abstract protections of "expectations." And when intrusion becomes normalized or expected, and surveillance becomes common, then that should not justify further intrusions on protected constitutional rights. The *Carpenter* majority confirmed that *Katz* did not replace the common-law property framework but rather added to it. *Carpenter*, 585 U.S. at 304 (citing *United States v. Jones*, 565 U.S. 400, 405, 406-07

(2012)). "[T]he traditional approach asked if a house, paper, or effect was *yours* under law. No more was needed to trigger the Fourth Amendment." *Carpenter*, 585 U.S. at 397-98 (Gorsuch, J., dissenting); *Soldal v. Cook County*, 506 U.S. 56, 64 (1992) (*Katz* did not "snuf[f] out the previously recognized protection for property under the Fourth Amendment").

When this Court applied the traditional understanding of the Fourth Amendment before *Katz*, the results in "third party" cases were far different. "*Miller* and *Smith* may not apply when the Government obtains the modern-day equivalents of an individual's own 'papers' or 'effects,' even when those papers or effects are held by a third party." *Carpenter*, 585 U.S. at 332. In *Ex parte Jackson*, 96 U.S. 727 (1878), this Court held that sealed letters placed in the mail were protected because "[t]he constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to *their papers*, thus closed against inspection, *wherever they may be*." *Id.* at 732 (emphasis added). It did not matter that letters were entrusted to the government via a bailment. The sender enjoyed the same Fourth Amendment protection as he does "when papers are subjected to search in one's own household." *Id.* This Court's conclusion was clear and emphatic:

> No law of Congress can place in the hands of officials connected with the postal service any authority to invade the secrecy of letters and such sealed packages in the mail; and all regulations adopted as to mail matter of this kind must be in

> subordination to the great principle embodied in the fourth amendment of the Constitution."

Id.

As this Court held in *Carpenter*, digital sharing does not automatically forfeit Fourth Amendment rights — the fact that "information is gathered by a third party does not make it any less deserving of Fourth Amendment protection." *Carpenter*, 585 U.S. at 320. No one forfeits property interests or Fourth Amendment rights simply by entrusting their property to a third party.

B. Location History is Property of Users.

Unlike the cell-site location information at issue in *Carpenter*, location history is not a business record created and maintained by Google for its own purposes. It is user-generated data that Google collects and stores on behalf of users, subject to the users' control. The legal relationship is one of bailment, not ownership.

Google's privacy policy confirms this point. The policy consistently refers to Location History as "your information" and "your data." Users can enable or disable Location History at will. They can delete their Location History at any time. They can export it. They control it. The individualized Location History associated with a particular user's account is that user's property, held by Google as a bailee.

The *Carpenter* majority drew this line itself, distinguishing *Miller* and *Smith*—which involved records created by institutions for their own business purposes—from location data generated incidentally in the course of using a device. 585 U.S. at 314. Justice

Gorsuch's dissent translated this same distinction into common-law property terms, recognizing that entrusted data is held by a bailee, not surrendered to an owner. He noted that when records are "entrusted" to a third party, the Fourth Amendment's protection does not necessarily lapse. 585 U.S. at 399 (Gorsuch, J., dissenting). "Entrusting your stuff to others is a bailment" under common law, and a "bailee normally owes a legal duty to keep the item safe" according to the terms of the parties' agreement. *Id.* These "ancient principles" protect individuals' interests even in records held by a third party. *Id.* at 400.

Location History fits comfortably within this framework. When people enable Location History, they do not surrender ownership of the data to Google. They authorize Google to collect and store it on their behalf, subject to their continuing control. The relationship is analogous to storing personal papers in a safe deposit box or personal files on a cloud server. The bank or service provider may physically possess the items, but they remain the customer's property. A warrant to search those items is a search of the customer's effects, not the service provider's business records.

This analysis finds strong support in the common law of bailment. *See id.* At common law, the bailee holds the goods on behalf of the bailor and owes the bailor duties of care and return. Critically, the bailor retains ownership of the bailed property. 8 C.J.S. *Bailments* § 28 (1988). The bailee's possession is derivative and limited by the terms of the bailment. *See Carpenter,* 585 U.S. at 399 (Gorsuch, J., dissenting) (quoting 8 C.J.S., *Bailments* § 36, pp. 468-

469 (2017)).

That is precisely the relationship between users and Google with respect to Location History. Users retain ownership of their location data. Google's possession is derivative—it exists only because users have authorized Google to collect and store the data. And Google's rights to use that data are limited by the terms of service, which give users the power to disable collection, delete stored data, and export their information. Granting Google limited usage of the data cannot be understood as a wholesale waiver of one's constitutional right against an unreasonable search.

C. A Property-Based Analysis Resolves This Case Without Recourse to Amorphous Balancing.

Once Location History is recognized as belonging to the user, the constitutional analysis becomes straightforward. When the Government compels Google to search a user's Location History, it searches the user's "papers" and "effects" within the meaning of the Fourth Amendment. A property-based approach provides clear guidance to law enforcement, magistrates, and courts. There is no need to engage in multi-factor balancing or to make sociological predictions about societal expectations. The question is simply whether the item searched belongs to the person claiming Fourth Amendment protection. If it does, the search requires a warrant supported by probable cause, subject to established exceptions.

Moreover, a property-based approach avoids the third-party doctrine's most troubling implications.

Under the *Smith* and *Miller* framework, sharing information with anyone—even for limited purposes and subject to contractual restrictions—can result in forfeiture of Fourth Amendment protection. This creates perverse incentives: it discourages beneficial data-sharing and forces individuals to choose between using modern technology and preserving their constitutional rights.

A property-based approach eliminates this dilemma. "When confronting new concerns wrought by digital technology, this Court has been careful not to uncritically extend existing precedents." *Carpenter*, 585 U.S. at 318. Sharing property with a bailee does not forfeit ownership. Storing papers in a bank vault does not make them the bank's papers. Uploading files to a cloud server does not transfer ownership to the server operator. The same should be true for Location History: entrusting it to Google for safekeeping does not strip people of their Fourth Amendment protection in that data.

D. Google's "Clickwrap" Agreements Cannot Establish the Voluntary Disclosure Required to Invoke the Third-Party Doctrine.

Moreover, the third-party doctrine forfeits Fourth Amendment protection only where an individual *knowingly* and *voluntarily* exposes information to a third party, thereby assuming the risk of government access. *Smith*, 442 U.S. at 743-44 ("[A] person has no legitimate expectation of privacy in information he *voluntarily* turns over to third parties.") (emphasis added). *See also Katz*, 389 U.S. at 351 ("What a person

knowingly exposes to the public . . . is not a subject of Fourth Amendment protection") (emphasis added). The government's theory depends entirely on the premise that users who click through Google's setup screens have voluntarily disclosed and forfeited their location data within the meaning of that doctrine. But that premise fails at every level. Google's "clickwrap"[2] agreements neither satisfy the contractual requirements courts demand for genuine assent nor establish the informed, purposeful exposure that *Katz* and its progeny require before a constitutional privacy interest may be deemed surrendered. Where consent is illusory as a matter of contract law, it cannot carry the far heavier constitutional burden the government asks this Court to place upon it.

As articulated by this Court, the third-party disclosure doctrine holds that individuals forfeit their reasonable expectation of privacy in information they voluntarily convey or knowingly expose to third parties, thereby allowing government access without a warrant; but this exception applies only when the

---

[2] "Clickwrap" agreements are a form of adhesion agreements in which "the adhering party does not have to use a pen," but rather clicks on some electronic icon. Nancy S. Kim, *Wrap Contracts: Foundations and Ramifications* 3 (2013) (There are other "wrap" agreements, like "browsewrap," "scrollwrap," etc., named from the action required.) The unusual names stem from "shrinkwrap" agreements, in which physically packaged software contained agreements to which an offeree supposedly agreed by merely tearing the cellophane packaging. James C. Hoye, *Click—Do We Have a Deal?*, 6 SUFFOLK J. TRIAL & APP. ADVOC. 163, 165 n.16 (2001).

disclosure is purposeful and informed, not compelled by necessity or inadvertent. *See Miller*, 425 U.S. at 442-43 (no Fourth Amendment protection for bank records because defendant "voluntarily conveyed" financial information to the bank and "exposed" it to employees in the ordinary course of business, assuming the risk of further disclosure); *Smith*, 442 U.S. at 743-44 (no privacy expectation in dialed phone numbers as petitioner "voluntarily conveyed numerical information to the telephone company" via automated systems, knowingly exposing it despite subjective beliefs in confidentiality).

Recent decisions have narrowed the doctrine's scope, further underscoring that it does not apply absent true voluntariness, particularly in digital contexts where data sharing is often compelled by modern life. Most importantly, this Court held in *Carpenter* that the third-party doctrine does not apply to digital location records. The Court rejected the government's third-party doctrine argument because cell-site location information is not "truly 'shared' as one normally understands the term," 585 U.S. at 315, and is instead generated automatically "without any affirmative act on the part of the user" beyond simply carrying a phone. The Court distinguished this from the "purposeful disclosures" in *Miller* and *Smith*.

Lower courts, state courts, and scholars have reinforced that the doctrine demands purposeful cession of privacy, invalidating its application to involuntary or unknowing disclosures, such as

automated metadata generation. *See, e.g.*, *State of Washington v. Kealey*, 907 P.2d 319 (Wash. Ct. App. 1995) (holding that defendant maintained a privacy interest, albeit diminished, in forgotten, zipped purse); *United States v. Graham*, 824 F.3d 421, 430 (4th Cir. 2016) (*en banc*) (pre-*Carpenter* CSLI case focusing on how defendant "thus voluntarily conveys the information necessary" to create CSLI); Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 575 (2009) (emphasizing "voluntary" exposure as doctrinal core, excluding compelled or unwitting transfers). Thus, the third-party doctrine applies solely when an individual *knowingly* and *purposefully* cedes control over private information to a third party, assuming the risk of government access, and does not extend to incidental, automatic, or coerced conveyances that lack such intent.

Clickwrap agreements, a form of electronic adhesion contract where users manifest assent by clicking a button or checkbox (*e.g.*, "I agree") after being presented with terms, *can* be enforceable when they provide reasonable notice of the terms and require affirmative user consent, as courts evaluate them based on traditional principles of offer, acceptance, and mutual assent. *See, e.g.*, *Airbnb, Inc. v. Doe*, 336 So. 3d 698 (Fla. 2022). However, when "consumers are urged to download free software at the immediate click of a button," courts give more scrutiny to whether an offeree has actually manifested any assent to the contract, usually by

focusing on the user experience leading up to the "click" at issue. *Specht v. Netscape Communs. Corp.*, 306 F.3d 17, 31 (2d Cir. 2002) (Sotomayor, J.). Courts have repeatedly refused to enforce clickwrap agreements where the terms are not conspicuously presented, lack meaningful opportunity for review, or fail to secure genuine consent. *Cullinane v. Uber Techs., Inc.*, 893 F.3d 53 (1st Cir. 2018) (holding that offerees were not reasonably notified of an arbitration agreement in clickwrap); *Marshall v. Georgetown Mem'l Hosp.*, 112 F.4th 211 (4th Cir. 2024); *Berman v. Freedom Fin. Network, LLC*, 30 F.4th 849 (9th Cir. 2022); *Bazemore v. Jefferson Cap. Sys., LLC*, 827 F.3d 1325 (11th Cir. 2016). Buried hyperlinks, small font, or confusing interfaces all weigh against a clickwrap's enforceability. *See, e.g.*, *Berkson v. Gogo LLC*, 97 F. Supp. 3d 359, 397-401 (E.D.N.Y. 2015) (refusing enforcement when hyperlinks to terms were inconspicuous compared to "sign-in" button); *In re Zappos.com, Inc.*, 893 F. Supp. 2d 1058, 1064 (D. Nev. 2012) (terms unenforceable when placed inconspicuously at bottom of page). As adhesion contracts (at best), courts similarly are quick to strike unconscionable portions, particularly when presented during mandatory device setup, or when an app presents persistent prompts, creating illusory choice rather than informed consent.

Here, Google's Location History clickwrap fails on precisely the grounds courts have found dispositive. Like the buried hyperlinks condemned in *Berkson* and the inconspicuous footer terms struck in *In re*

Zappos.com, Google's privacy disclosures are embedded within layered, dense terms of service that no reasonable user meaningfully reviews before clicking through. The "affirmative" act of enabling Location History—whether during initial device setup or through persistent app prompts—mirrors the coercive dynamic courts have identified as producing illusory rather than genuine consent. Where the user experience fails to secure reasonable notice and genuine assent, the clickwrap cannot be said to reflect voluntary disclosure, a prerequisite assumed in *Smith v. Maryland*.

Even a user who reads and understands that Google collects location data for purposes of navigation, personalization, or targeted advertising has not thereby consented to the creation and indefinite retention of a granular, retrospective record precise enough to place them at a specific location at a specific moment in time—the sort of record at issue here and necessary for a geofence warrant. There is a profound difference of degree between knowing that a tech company "uses your location" and understanding that it is silently building a permanent, timestamped archive of your movements that law enforcement may later subpoena to reconstruct your whereabouts on any given day. No reasonable reading of Google's clickwrap disclosures (assuming they are read at all) would put an ordinary user on notice of that latter reality.

Under *Katz*, only what a person "knowingly

exposes" falls outside constitutional protection. A user who clicks through a setup screen to enable maps and weather notifications has not knowingly exposed a detailed location history suitable for forensic use by the government. The fiction of consent manufactured by an adhesion contract presented during mandatory device setup cannot bear the constitutional weight the government asks this Court to place upon it.

And if the clickwrap cannot establish voluntary disclosure as a matter of contract law, it certainly cannot establish the knowing, voluntary exposure required to forfeit Fourth Amendment rights under *Smith* and *Miller*. The government cannot simultaneously argue that Google's terms are enforceable enough to eliminate a privacy interest while the very courts tasked with enforcing those terms would find them wanting.

Accordingly, even if this Court were to apply the third-party doctrine, it could not find that individuals voluntarily relinquished their Fourth Amendment interest in their Location History data. The clickwrap mechanism through which Google purports to obtain user consent fails to satisfy the knowing, voluntary exposure required under *Katz* and *Smith* to forfeit constitutional protection. A user who clicks through device setup screens may understand, at most, that Google will use their location for everyday app functions, not that Google is constructing a permanent, forensic-grade archive of their movements available to law enforcement on demand.

Individuals have never *meaningfully* consented to share data in that form or for that purpose.

II. GEOFENCE WARRANTS PRESENT SERIOUS PARTICULARITY DANGERS THAT DEMAND A CLEAR CONSTITUTIONAL FRAMEWORK.

The government's use of geofence warrants is a recent and rapidly spreading investigative technique. Lower courts have divided sharply on its constitutionality, and the absence of clear guidance from this Court has left magistrates without meaningful standards for evaluating warrant applications. It has left law enforcement without reliable guidance about what will pass constitutional muster, and ordinary citizens without effective protection against sweeping digital dragnets. This Court should carefully scrutinize such warrants.

A. General Warrants Were the Chief Evil the Fourth Amendment Was Designed to Prevent.

The Fourth Amendment's particularity requirement has deep historical roots. This Court has emphasized that "it would be a needless exercise in pedantry to review again the detailed history of the use of general warrants as instruments of oppression from the time of the Tudors, through the Star Chamber, the Long Parliament, the Restoration, and beyond." *Stanford v. Texas*, 379 U.S. 476, 482 (1965). As John Adams recalled, James Otis's 1761 speech condemning writs of assistance, which are broad and generic warrants, "was the first act of opposition to the arbitrary claims of Great Britain" and "[t]hen and

there the child Independence was born." *Riley v. California*, 573 U.S. 373, 403 (2014) (quoting 10 Works of John Adams 247-248 (C. Adams ed. 1856)).

In fact, general warrants were particularly pernicious because they specified an offense but allowed officers discretion to determine which persons to search and which places to examine. They lacked the particularity that the Fourth Amendment now demands: warrants must "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV.

This particularity requirement serves two critical functions. First, it ensures that magistrates, not officers, determine the scope of a search. The point of the Fourth Amendment is to interpose a magistrate between the police and the people. Second, particularity protects the innocent. By requiring the government to describe with particularity what it seeks, the Amendment prevents officers from conducting exploratory rummaging in a person's belongings in hopes of finding evidence of some crime. (And, given the extreme proliferation of new crimes, who could hope not to be found guilty of something? *See* Harvey Silverglate, *Three Felonies a Day: How the Feds Target the Innocent* (2011); *Nieves v. Bartlett*, 587 U.S. 391, 412 (2019) (Gorsuch, J., dissenting) ("In our own time and place, criminal laws have grown so exuberantly and come to cover so much previously innocent conduct that almost anyone can be arrested for something.")).

These principles apply with full force in the digital age. As the Fifth Circuit recognized, the fact that modern general warrants are executed via digital

search of a database rather than physical search of a home does not change their character. *Smith*, 110 F.4th at 837. If anything, the ease and efficiency of digital searches make the particularity requirement more important, not less. When officers can search hundreds of millions of records "with just the click of a button," *Carpenter*, 585 U.S. at 311, the need for meaningful limits on their discretion becomes acute.

B. Geofence Warrants Pose Serious Dangers of Becoming General Warrants in Digital Form.

The standard of particularity regarding *the items to be seized* requires that the description leave nothing to the discretion of the officers. *See Marron v. United States*, 275 U.S. 192, 196 (1927). The particularity requirement exists to ensure that a neutral magistrate—not the investigating officer—defines the scope of a search before it occurs. *See Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971). Geofence warrants create structural pressures against both of those purposes.

Geofence warrants direct a service provider to search through hundreds of millions of user accounts to identify those whose devices were in a particular geographic area at a particular time. They do not identify any particular suspect. They simply draw a virtual fence around a location and direct the service provider to report back which accounts fall within it.

As the Fifth Circuit explained, this process requires the service provider to "search through the entirety of its Sensorvault—all 592 million individual accounts—for all of their locations at a given point in

time." *Smith*, 110 F.4th at 837. "Moreover, this search is occurring while law enforcement officials have no idea who they are looking for, or whether the search will even turn up a result." *Id.* "Indeed, the quintessential problem with these warrants is that they never include a specific user to be identified, only a temporal and geographic location where any given user may turn up post-search." *Id.* Every American with a Google Account is searched every time such a warrant is issued. One can imagine John Adams's reaction to a warrant including millions. When a geofence warrant is issued, the *place* actually searched is Google's entire Sensorvault: millions of accounts on Google's servers, wherever those servers sit.

Just as colonial general warrants authorized officers to search any home where evidence might be found, geofence warrants authorize service providers to search any account that might contain relevant information. The only limit is geographic and temporal—not based on individualized suspicion of any particular person. This reflects "the exact sort of 'general, exploratory rummaging' that the Fourth Amendment was designed to prevent." *Smith*, 110 F.4th at 837 (quoting *Coolidge*, 403 U.S. at 467).

The Fourth Amendment requires particularity as to "the persons or things to be seized," not merely the place to be searched. U.S. CONST. amend. IV. A warrant that authorizes searching every house on a city block for evidence of a crime would violate the particularity requirement, even if the geographic area is precisely described, because it fails to define any particular criminal individual or object. The same is

true for digital searches. A warrant that instructs a service provider to search hundreds of millions of accounts and report back merely which ones fall within a geographic fence does not describe the things to be seized—it defines the things to be seized as the output of a general search. That inverts the constitutional requirement. At minimum, a valid geofence warrant would describe the category of data to be produced, the time window with specificity sufficient to limit the search, and the criteria—beyond mere geographic presence—that would establish relevance to the alleged offense.

Without careful and defined limits, geofence warrants do not describe with particularity what is to be seized. Instead, they authorize a fishing (or trawling) expedition: search all the accounts and report back which ones contain potentially relevant information. That is not a thing described with particularity; it is the definition of an exploratory rummaging. "These geofence warrants fail at Step 1—they allow law enforcement to rummage through troves of location data from hundreds of millions of Google users without any description of the particular suspect or suspects to be found." *Smith*, 110 F.4th at 837-838. This is the very definition of a general warrant. Carefully defined guardrails are necessary to hold geofence warrants to the specificity standard.

CONCLUSION

This Court should reverse the decision below.

Respectfully submitted,

JAY ALAN SEKULOW
Counsel of Record
JORDAN A. SEKULOW
STUART J. ROTH
ANDREW J. EKONOMOU
GEOFFREY R. SURTEES
NATHAN J. MOELKER
LIAM R. HARRELL
AMERICAN CENTER FOR
LAW & JUSTICE