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 OF THE POLICING PROJECT AT NEW YORK UNIVERSITY SCHOOL OF LAW AS *AMICUS CURIAE* IN SUPPORT OF NEITHER PARTY

BARRY FRIEDMAN
MARIA PONOMARENKO
MAX ISAACS
KATIE KINSEY
POLICING PROJECT AT
NYU SCHOOL OF LAW
40 Washington Sq. S.
New York, NY 10012

NICHOLAS ROSELLINI
Counsel of Record
LATHAM & WATKINS LLP
500 Montgomery Street
Suite 2000
San Francisco, CA 94111
(415) 395-8165
nick.rosellini@lw.com

SUMER GHAZALA
MAHSHAD BADII
LATHAM & WATKINS LLP
555 11th Street, NW
Suite 1000
Washington, DC 20004

Counsel for Amicus Curiae

TABLE OF CONTENTS

Page

TABLE OF CONTENTS—Continued

Page

TABLE OF AUTHORITIES

Page(s)

CASES

TABLE OF AUTHORITIES—Continued

Page(s)

TABLE OF AUTHORITIES—Continued

Page(s)

STATUTES

TABLE OF AUTHORITIES—Continued

Page(s)

OTHER AUTHORITIES

TABLE OF AUTHORITIES—Continued

Page(s)

TABLE OF AUTHORITIES—Continued

Page(s)

TABLE OF AUTHORITIES—Continued

Page(s)

TABLE OF AUTHORITIES—Continued

Page(s)

TABLE OF AUTHORITIES—Continued

Page(s)

TABLE OF AUTHORITIES—Continued

Page(s)

TABLE OF AUTHORITIES—Continued

Page(s)

INTEREST OF *AMICUS CURIAE*

The Policing Project at New York University School of Law is dedicated to strengthening policing through democratic governance.[1] The Project facilitates public engagement on policing policies and practices, with the twin aims of giving communities a voice in how they are policed and developing greater mutual trust between them and law enforcement. The Project is committed to the proper governance of emerging policing technologies in ways that advance public safety while safeguarding civil liberties. The Project works with law enforcement to develop rules governing use of these technologies, promotes the adoption of legislative frameworks to govern them, and has a keen interest in their proper treatment under the Fourth Amendment. The Project has previously filed merits-stage amicus briefs addressing these issues in *United States v. Microsoft*, 584 U.S. 236 (2018), and *Barnes v. Felix*, 605 U.S. 73 (2025).

---

[1] The Policing Project is affiliated with New York University School of Law, but this brief does not purport to represent the school's official views. No counsel for any party authored this brief in whole or in part, and no party, counsel for a party, or person or entity other than *amicus curiae*, its members, and its counsel made a monetary contribution intended to fund the brief's preparation or submission.

INTRODUCTION AND SUMMARY OF ARGUMENT

By obtaining Location History data belonging to Okello Chatrie and innocent Google users while investigating a bank robbery, the Government conducted a search of their personal "papers" under the Fourth Amendment. Chatrie argues that the geofence warrant issued here is an unconstitutional "general warrant" because it required searching Google's entire Location History database. The Government takes the polar opposite view, insisting that obtaining Google users' Location History did not even implicate the Fourth Amendment.

This Court should reject both extremes. Given the availability of massive data and AI-powered analytic tools, the Government's request for carte blanche to use them with no judicial supervision or constitutional safeguards imperils all our liberties. But Chatrie's approach is flawed as well. Data-driven tools can help identify people who have done—or would do—great harm. Deeming any order authorizing use of these tools an unconstitutional general warrant, such that they cannot be used at all, would impede legitimate law enforcement activities.

Fortunately, this Court's jurisprudence compels neither extreme. Although warrants supported by probable cause make sense for traditional searches, novel investigative techniques call for novel solutions. Reverse-identification tools—i.e., methods for identifying unknown suspects, rather than obtaining evidence against known suspects—do not fit neatly within the usual Fourth Amendment framework. Nor do the many rapidly emerging technologies that soon will find their way before this Court. Given the

potential benefits to public safety from some of these tools, but also the enormous risks to personal liberties and security, the Court should decide this case narrowly, so as not to "embarrass the future." *Carpenter v. United States*, 585 U.S. 296, 316 (2018). "[T]he ultimate touchstone of the Fourth Amendment is 'reasonableness,'" after all. *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006).

The solution to the challenges posed by rapidly advancing technology is, at least in the first instance, legislative. The complex nature of data-driven investigation and surveillance methods cries out for statutory regulation. And legislative frameworks will make the Fourth Amendment analysis easier by enabling courts to determine whether the governing statute establishes a constitutionally "adequate substitute for a warrant." *New York v. Burger*, 482 U.S. 691, 702-03 (1987). A balanced decision in this case—one making clear that the Fourth Amendment applies, while inviting deference to compliance with adequate statutory safeguards—would encourage much-needed legislative action.

ARGUMENT

I. RAPIDLY ADVANCING TECHNOLOGY POSES DIFFICULT FOURTH AMENDMENT QUESTIONS THAT CALL FOR CAUTION IN DECIDING THIS CASE

This case once again requires this Court to confront the "power of technology to shrink the realm of [constitutionally] guaranteed privacy." *Kyllo v. United States*, 533 U.S. 27, 34 (2001). That crucial task requires this Court to "tread carefully." *Carpenter v. United States*, 585 U.S. 296, 316 (2018).

With that in mind, the Court should reject an all-or-nothing approach to the question presented.

A. Modern Technologies Offer Promise For Policing And Peril For Civil Liberties

Over the last half century, this Court has grappled repeatedly with Fourth Amendment questions raised by technological advances, including investigation and surveillance carried out using aircraft, thermal imagers, smartphones, and cell-site location data. *See, e.g.*, *California v. Ciraolo*, 476 U.S. 207, 209 (1986); *Kyllo*, 533 U.S. at 29; *Riley v. California*, 573 U.S. 373, 384-85 (2014); *Carpenter*, 585 U.S. at 305. The pace of innovation is increasing rapidly, with great promise for policing and grave peril for civil liberties.

1. Cutting-edge investigation methods, driven by new and powerful advances in artificial intelligence (AI), are reshaping law enforcement in ways that have assisted criminal investigations and protected public safety.

To name just a few examples, officers deployed automated license plate readers to help identify the Brown University gunman.[2] Investigators identified the "Golden State Killer" using AI-powered genealogy tools.[3] Authorities have used AI scanning technology

---

[2] *See* Aaron Parseghian, *Controversial technology helped investigators track gunman in Brown University and MIT professor shootings*, CBS News (Dec. 19, 2025), https://www.cbsnews.com/boston/news/brown-university-mit-professor-shooting-flock-cameras-car.

[3] Tebah Browne & Barry Scheck, *Regulating Forensic Investigative Genetic Genealogy: The Case for Judicial Oversight and the Bipartisan Model Legislation Passed in Maryland,* The Judges' Journal (June 11, 2024), https://www.americanbar.org/

to identify online child grooming and sexual abuse material.[4] Sophisticated algorithms have helped detect billions of dollars' worth of financial crimes.[5] Meanwhile, face- and voice-recognition systems have facilitated the rescue of kidnapping victims and the arrest of January 6 rioters.[6]

Many of these law enforcement tools rely increasingly on anomaly detection systems, which flag deviations from expected patterns to help officers detect theft, fraud, and other illegal activities that otherwise might escape notice. *See* Andrew Guthrie Ferguson, *Video Analytics and Fourth Amendment Vision*, 103 Tex. L. Rev. 1253, 1275-76 (2025). Some AI-powered technologies even purport to forecast

---

groups/judicial/resources/judges-journal/2024-spring/regulating-forensic-investigative-genetic-genealogy (login required).

[4] Shira Ovide, *Scanning Technology is coming to Detect Child Porn. Here's what it means,* Wash. Post (June 24, 2025), https://www.washingtonpost.com/technology/2025/06/24/child-sex-abuse-crime-fighting-technology.

[5] Matt Egan, *AI helped the feds catch $1 billion of fraud in one year. And it's just getting started*, CNN (Oct. 17, 2024), https://www.cnn.com/2024/10/17/business/ai-fraud-treasury; Matt Egan, *AI is Uncle Sam's new secret weapon to fight fraud*, CNN (Feb. 28, 2024), https://www.cnn.com/2024/02/28/business/artificial-intelligence-fraud-treasury-ai/index.html.

[6] Drew Harwell & Craig Timberg, *How America's surveillance networks helped the FBI catch the Capitol mob*, Wash. Post (Apr. 2, 2021), https://www.washingtonpost.com/technology/2021/04/02/capitol-siege-arrests-technology-fbi-privacy; *AI and policing: The benefits and challenges of artificial intelligence for law enforcement* 24, Europol Innovation Lab (2024), https://www.europol.europa.eu/cms/sites/default/files/documents/AI-and-policing.pdf.

where future crimes may occur—and who will commit them.[7]

2. The very same data-driven investigative and surveillance tools can present serious threats to privacy and civil liberties. These "seismic shifts in digital technology" offer considerable promise for effective policing and public safety precisely because they have "made possible the tracking" of almost every facet of American life. *Carpenter*, 585 U.S. at 313. That unprecedented capability threatens the Fourth Amendment's dual aims of "secur[ing] 'the privacies of life' against 'arbitrary power'" and "'plac[ing] obstacles in the way of a too permeating police surveillance.'" *Id.* at 305. Those bedrock constitutional values must not be left to "'the mercy of advancing technology.'" *Id.*

These threats are not abstract—they are unfolding now. By compiling internet browsing history, purchase records, biometric data, and social media activity, today's AI-powered surveillance technology generates a "detailed, encyclopedic, and effortlessly compiled" portrait of each of us. *Id.* at 309. It allows officers to "[m]easure[] everything you eat, drink, and wear." 3 *Debates in the Several Conventions on the Adoption of the Federal Constitution* 448-49 (Jonathan Elliot ed., 1974). And it empowers them to discern a person's friends, family, colleagues, and associates with remarkable accuracy.[8]

---

[7] Tim Lau, *Predictive Policing Explained,* Brennan Ctr. for Just. (Apr. 1, 2020), https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained.

[8] *Combine knowledge graphs and large language models to speed up criminal network analysis*, GraphAware (July 28,

Such synthesis risks exposing all of our "familial, political, professional, religious, and sexual associations." *Carpenter*, 585 U.S. at 311. Extended data retention magnifies this concern: The more data sits and accumulates, the more revealing it can become. Increasingly, law enforcement agencies are aggregating data from various databases and other sources, analyzing it with AI-powered tools, and capturing "an intimate window" into our lives. *Carpenter*, 585 U.S. at 311; *see also* Bridget A. Fahey, *Data Federalism*, 135 Harv. L. Rev. 1007, 1017 (2022). New investigative platforms offered by private technology companies empower law enforcement officers to "take[] fragmented data, scattered across various agencies and stored in different formats, and transform[] it into a unified searchable web."[9] Baltimore police, for instance, recently pooled data from aerial cameras, CCTV, and license plate readers, "'mak[ing] all the systems work together'" to "glean insights from the whole of individuals' movements." *Leaders of a Beautiful Struggle v. Balt. Police Dep't*, 2 F.4th 330, 344-45 (4th Cir. 2021).

Even for one-off events, technologies like location tracking and facial recognition software pose risks. Such tools can identify people visiting sensitive locations, like private residences, healthcare

---

2025), https://graphaware.com/blog/combine-knowledge-graphs-and-llms-to-speed-up-crime-analysis.

[9] Nicole M. Bennett, *When the government can see everything: How one company – Palantir – is mapping the nation's data*, The Conversation (Aug. 27, 2025), https://theconversation.com/when-the-government-can-see-everything-how-one-company-palantir-is-mapping-the-nations-data-263178.

facilities, places of worship, and political rallies. *See United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring). Officers already have come under scrutiny for using such tools for tracking attendees at gun shows and mosques.[10] So too with their efforts to surveil and track demonstrators following George Floyd's death in 2020[11]—and, more recently, anti-ICE protesters.[12]

The geographic reach and temporal scope of modern surveillance methods—especially "persistent surveillance" techniques—are nothing short of remarkable. Baltimore's "Persistent Surveillance System" filmed 90% of the city, 40 hours a week, for six months. *See Leaders of a Beautiful Struggle*, 2 F.4th at 334. Each image taken over that period could have been "magnified to a point where people and cars [we]re individually visible," giving officers the power to track nearly every resident of Baltimore wherever they went. *Id.* It is scarcely an exaggeration to say that authorities can now conduct "twenty-four hour

---

[10] Devlin Barrett, *Gun-Show Customers' License Plates Come Under Scrutiny,* Wall St. J. (Oct. 2, 2016), https://www.wsj.com/articles/gun-show-customers-license-plates-come-under-scrutiny-1475451302 (login required); Adam Goldman & Matt Apuzzo, *With Cameras, Informants, NYPD Eyed Mosques*, Associated Press (Feb. 23, 2012), https://www.ap.org/media-center/ap-in-the-news/2012/with-cameras-informants-nypd-eyed-mosques.

[11] Zolan Kanno-Youngs, *U.S. Watched George Floyd Protests in 15 Cities Using Aerial Surveillance,* N.Y. Times (June 19, 2020), https://www.nytimes.com/2020/06/19/us/politics/george-floyd-protests-surveillance.html.

[12] Alfred Ng, *DHS accused of using surveillance tech to track legal observers in Maine,* Politico (Feb. 23, 2026), https://www.politico.com/news/2026/02/23/dhs-accused-of-using-surveillance-tech-to-track-legal-observers-in-maine-00792722.

surveillance" of not just "any citizen of this country," *United States v. Knotts*, 460 U.S. 276, 283 (1983), but all of them—all at once.

3. Modern technologies pose another kind of threat: Even the most advanced systems fail often, further jeopardizing the public's sense of safety and trust in law enforcement. For example, an AI-powered weapons-detection system deployed in New York misidentified a child's lunchbox as a bomb, while failing to detect an actual knife carried by another student.[13] And in Colorado, a woman and four children were pulled over and detained at gunpoint after a license-plate reader misidentified her SUV as a stolen motorcycle.[14] Such mistakes underscore a broader problem: "[T]he effectiveness of these surveillance technologies in achieving the government's aims is largely unstudied, as is their empirical validity and reliability." Christopher Slobogin & Sarah Brayne, *Surveillance Technologies and Constitutional Law*, 6 Ann. R. Crim. 219, 220 (2023); *see* Barry Friedman et al., *Policing Police Tech: A Soft Law Solution,* 37 Berkeley Tech. L.J. 701, 710 (2022).

The danger of data misuse compounds these concerns. Some officers have used law enforcement databases improperly to collect information on former

---

[13] *See* Georgia Gee, *Un-Alarmed: AI Tries (and Fails) to Detect Weapons in Schools,* The Intercept (May 7, 2023), https://theintercept.com/2023/05/07/ai-gun-weapons-detection-schools-evolv (login required).

[14] Vanessa Romo, *No Charges for Colorado Officers Who Held Black Children At Gunpoint,* NPR (Jan. 8, 2021), https://www.npr.org/2021/01/08/955165485/no-charges-for-colorado-officers-who-held-black-children-at-gunpoint.

romantic partners, business associates, neighbors, and journalists—all for purely private reasons.[15] And security breaches are not uncommon. In one case, hackers attacked a police software vendor and stole nearly twenty gigabytes of highly sensitive data.[16] Numerous police departments themselves have been the target of ransomware attacks.[17]

B. A Rigid All-Or-Nothing Approach To These Critical Issues Is Undesirable

To assess law enforcement activities, this Court's Fourth Amendment precedents require answering two main questions: (1) "whether or not a Fourth Amendment 'search' [or seizure] has occurred" and, if so, (2) whether that search or seizure was "unreasonable." *Kyllo*, 533 U.S. at 31-33. Searches and seizures are usually "per se unreasonable" without a warrant supported by probable cause. *Katz v. United States*, 389 U.S. 347, 357 (1967). That

---

[15] *See, e.g.*, State of Minn. Off. of the Legis. Auditor, Law Enforcement's Use Of State Databases 26 (2013), https://www.auditor.leg.state.mn.us/ped/pedrep/ledatabase.pdf; *Police chief gets caught*, WKRC (Aug. 18, 2024), https://local12.com/news/nation-world/police-chief-gets-caught-using-license-plate-cameras-to-track-his-ex-girlfriend-228-times-arrests-charges-probation-flock-safety-follow-stalk-new-boyfriend-broke-up-out-of-town-misuse.

[16] Zach Whittaker, *A hack at ODIN Intelligence exposes a huge trove of police raid files*, TechCrunch (Jan. 21, 2023), https://techcrunch.com/2023/01/21/odin-intelligence-breach-police-surveillance/.

[17] *See, e.g.*, Jonathan Dienst, *Ransomware Attack at NJ County Police Department Locks Up Criminal Investigative Files,* NBC New York (Apr. 7, 2023), https://www.nbcnewyork.com/investigations/ransomware-attack-at-nj-county-police-department-locks-up-criminal-investigative-files/4219341.

general rule creates an all-or-nothing problem: On the one hand, "[t]o label any police activity a 'search' or 'seizure' is to" require probable cause and a warrant. Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 Minn L Rev 349, 388 (1974). Given how these new technologies operate, that may disable their use altogether. On the other hand, if use of a new technology is deemed neither a search nor a seizure, "it is subject to no significant restrictions of any kind." *Id.*; *see* Barry Friedman, *The Constitutionality of Indiscriminate Data Surveillance*, 174 U. Pa. L. Rev. 293, 347 (2026). This doctrinal dynamic poses dilemmas at both steps of the Fourth Amendment analysis.

1. In recent cases involving data-driven policing, the threshold question whether the Government has conducted a search or seizure has required assessing, in effect, how much is too much. *See Carpenter*, 585 U.S. at 310 n.3 (declining to decide "how long" location data must be tracked to become a search). This mode of analysis poses "vexing problems." *Jones*, 565 U.S. at 412. Courts are struggling to apply it, often reaching contradictory results.[18] The task will

---

[18] *Compare People v. Harris*, 92 N.Y.S.3d 863, 866-67 (N.Y. Sup. Ct. 2019) (three days of cell site location information (CSLI) was a search), *with People v. Jiles*, 68 N.Y.S.3d 787, 791 (N.Y. App. Div. 2017) (four days of CSLI was not a search); *compare Commonwealth v. Wilkerson,* 156 N.E.3d 754, 765-66 (Mass. 2020) (six hours of CSLI was a search), *with United States v. Jackson*, No. 21-CR-331, 2022 WL 1498191, at *4 (M.D. Ala. Mar. 15, 2022) (six hours of GPS tracking was not a search); *compare Commonwealth v. Almonor,* 120 N.E.3d 1183, 1197 (Mass. 2019) (single ping of cell phone was a search), *with United States v. Riley*, 858 F.3d 1012, 1018 (6th Cir. 2017) (single ping was not a search).

become only more difficult as digital tools diversify in kind and advance in scale and precision.

The first fault line, one this Court already has confronted, concerns duration. *Carpenter* addressed CSLI obtained from wireless providers, which enables officers to reconstruct an individual cell phone user's movements over time. 585 U.S. at 300-01. The Court held that "accessing seven days of CSLI constitutes a Fourth Amendment search," while leaving open the possibility that accessing CSLI for a "more limited" period would not. *Id.* at 310 n.3; *see Jones*, 565 U.S. at 430 (Alito, J., concurring) (concluding that "the point at which the tracking of this vehicle became a search" was "surely crossed before the 4-week mark").

Courts also are grappling with the "how much is too much" question in the context of non-continuous data collection. Baltimore's persistent surveillance program, for instance, was limited to daylight hours. *Leaders of a Beautiful Struggle*, 2 F.4th at 342-43. And as discussed, even one-off snapshots can disclose sensitive details. *Supra* at 7-8.

Technological advancement also raises new questions about what kind of data is constitutionally protected. Case in point: *Carpenter* acknowledged the traditional rule that "an individual has no reasonable expectation of privacy in [his] public movements," but recognized that "pervasive tracking" made effortless by CSLI required a different result. 585 U.S. at 314-15. Similarly, while the Fourth Amendment has generally been understood not to shield a person's "facial characteristics" or "voice," *United States v. Dionisio*, 410 U.S. 1, 14 (1973), widespread use of face- and voice-recognition technology still might invite constitutional scrutiny. So too for social media: Viewing one public Facebook post might warrant

different legal treatment than mining years of online activity to build a comprehensive dossier of a person's belief system. Tonja Jacobi & Dustin Stonecipher, *A Solution for the Third-Party Doctrine in A Time of Data Sharing, Contact Tracing, and Mass Surveillance*, 97 Notre Dame L. Rev 823, 825-26, 880 (2022).

The realities of modern technology also are making application of the third-party doctrine more problematic. *Carpenter* recognized that people do not "voluntarily" share CSLI in any meaningful sense, because carrying a phone is such a "pervasive and insistent part of daily life." 585 U.S. at 315. And countless people download apps to store and use personal data to improve their health, deepen relationships, and ease their lives—while reasonably expecting that their data will not be shared with the Government. *See* Friedman, *Constitutionality*, *supra*, at 300, 309-11; *infra* at 18-19.

Still more difficult questions arise when, rather than collecting data themselves, officers buy location data, browsing histories, and consumer profiles on the open market.[19] The scale of data available for officers to purchase is staggering: As of 2020, more than 4,000 data brokers had dossiers on 98% of Americans.[20] And some vendors advertise "billions" of location data points going back 180-plus days, far

---

[19] Off. of the Dir. of Nat'l Intel., Senior Advisory Grp., Panel on Commercially Available Info., Report to the Director of National Intelligence 19-20 (2022), https://perma.cc/BE3L-8A5L.

[20] Danielle Keats Citron, *The Fight for Privacy* 11 (2022); *see* Carey Shenkman et al., *Legal Loopholes and Data for Dollars* 10, 22 (2021), https://perma.cc/4DJA-93GD.

exceeding *Carpenter*'s seven-day threshold.[21] Some agencies have even purchased stolen data.[22] If subpoenaing certain data constitutes a search, what about simply buying and holding it indefinitely?

Courts also are grappling with how even lawfully obtained data can be used later on. Some already have held that the initial collection and subsequent use of data are distinct Fourth Amendment events, each of which demands constitutional scrutiny. *See Olson v. County of Grant*, 127 F.4th 1193, 1199 (9th Cir. 2025) (holding that examining cell phone data beyond the scope of the original consent violated the Fourth Amendment); *Commonwealth v. Yusuf*, 173 N.E.3d 378, 395-97 (Mass. 2021) (same for reviewing lawfully recorded body-camera footage of a residence in connection with an unrelated investigation). Whether these courts' analysis is correct holds significant consequences for both policing and personal privacy.

2. Assessing the "reasonableness" of modern data-driven investigation and surveillance techniques presents its own difficulties.

If a warrant supported by probable cause is required for all indiscriminately collected data, critical investigations may never get off the ground. Traditional investigations generally proceed from a

---

[21] *See* Garance Burke & Jason Dearen, *How an obscure cellphone tracking tool provides police 'mass surveillance on a budget'*, PBS News (Sept. 1, 2022), https://www.pbs.org/newshour/politics/how-an-obscure-cellphone-tracking-tool-provides-police-mass-surveillance-on-a-budget.

[22] Joseph Cox, *Police Are Buying Access to Hacked Website Data,* Vice (July 8, 2020), https://www.vice.com/en/article/police-buying-hacked-data-spycloud.

known suspect to incriminating evidence. But digital investigations often proceed in reverse—from masses of data to a previously unknown perpetrator. An officer might trawl through a biometric database, deploy algorithms to crawl social media posts, or conduct persistent aerial surveillance to discern individuals traveling to and from a crime scene. But because the perpetrator's identity is precisely what the officer seeks, requiring probable cause before these identification methods may be used can impose an impossible prerequisite. Forbidding these kinds of searches would result in a Fourth Amendment that permits far more invasive techniques without a warrant—stakeouts, pat-downs, covert recording—while barring preliminary digital queries that represent a far "less intrusive step." *California v. Acevedo*, 500 U.S. 565, 584 (1991) (Scalia, J., concurring in the judgment).

Even more elusive—but increasingly common—are data uses based on no particularized suspicion whatsoever. These include efforts to detect anomalies or make predictions, both of which can involve intrusive investigations into personal data. *See* Ferguson, *supra*, at 1308-10, 1318.

Situations where useful data is found on third-party servers pose even more difficulty. *Supra* at 13-14. Officers often rely on various kinds of third-party data early in an investigation—before probable cause exists—to develop leads and identify suspects. Some private companies holding such data will happily comply with government requests, without regard for privacy interests—a problem in its own right. *See* Friedman, *Constitutionality*, *supra*, at 312-13. But many others will not comply absent a court order, on the theory that "[p]rotecting customer

privacy is good for business." Orin Kerr, *The Case for the Third-Party Doctrine*, 107 Mich. L. Rev. 561, 598 (2009). Imposing a blanket warrant-supported-by-probable-cause requirement—as opposed to some other sort of predicate, *see infra* at 30-31—would hamstring legitimate law enforcement attempts to obtain evidence from third parties.

As a doctrinal matter, then, "rigid adherence" to the traditional warrant requirement places enormous pressure on judges deciding the threshold question whether a search occurred in the first place. Christopher Slobogin, *The Liberal Assault on the Fourth Amendment*, 4 Ohio St. J. Crim. L. 603, 607 (2007). Under that regime, "the only way" for courts to preserve vital investigative tools is "to deny that what the police or prosecutors are doing constitutes a 'search.'" Friedman, *Constitutionality*, *supra*, at 319. Invasive law enforcement activities could thus go completely unregulated. *See* Slobogin, *Liberal Assault*, *supra*, at 607. An absolutist approach risks giving us a Fourth Amendment that either becomes less protective as modern investigation and surveillance techniques grow more sophisticated, or becomes a straightjacket prohibiting the use of valuable investigative tools. Either path is intolerable, but there is another way.

II. THIS CASE SHOULD BE RESOLVED NARROWLY SO AS NOT TO EMBARRASS THE FUTURE

In this case, the parties stake out diametrically opposed positions. The Government argues that obtaining geofence data was no search at all because users "voluntarily" disclosed their Location History to Google, and the Government sought only two hours'

worth of location data within a confined perimeter. BIO.10. Chatrie's top-line position, by contrast, is that Location History can never be constitutionally obtained because any warrant authorizing such a search is a per se unconstitutional "general warrant" authorizing "the search of millions of separate accounts." Pet'r.Br.42-43.

This Court should chart a middle course. Geofence warrants like this one are neither totally immune from Fourth Amendment scrutiny nor irredeemably unconstitutional. The Court should hold that, at every step, obtaining Google users' Location History constituted a search. But the Court then should evaluate the search's reasonableness under something other than the requirement for a traditional warrant based on probable cause. This approach accounts for both the promise and peril of modern investigative techniques. *See* Friedman, *Constitutionality*, *supra*. A narrow decision along these lines will avoid "embarrass[ing] the future" as technology continues to advance. *Carpenter*, 585 U.S. at 316.

A. Obtaining Users' Location History Was A Fourth Amendment "Search"

When the Government obtained users' Location History from Google, it conducted a search under the Fourth Amendment.

1. The Fourth Amendment protects people from government searches of their "papers." Google users' Location History fits comfortably within that text. Today, mobile apps and online platforms serve as digital substitutes for the journaling and correspondence that historically was done on physical "papers." Apps let us interact with loved ones, store

photographs, track our reading and listening habits, and organize ideas for professional and creative projects. While some apps require that we enter information manually, many now collect personal data automatically through various sensors. Fitness apps record our step counts, running routes, and sleep patterns; navigation apps log our driving routes and daily routines; and health apps track our heart rates and other medical data. And they do so automatically without further action.

That is precisely what Google users do with their Location History. This detailed compilation of personal movements, though "acquire[d] and store[d]" on Google's services, is created for users' personal benefit. Pet.App.270a. A user's Location History "is off by default," but users can opt in, manage retention, and export or delete records as they see fit. Pet.App.273a, 281a-84a. When users opt in, Location History chronicles their movements in a "sweeping, granular, and comprehensive" way. Pet.App.270a.

Google users accordingly have both a property interest and a reasonable expectation of privacy in their Location History. *See Jones*, 565 U.S. at 409. They possess core property rights in their Location History, including the right to use, enjoy, dispose, and exclude—and their contractual relationship with Google made clear that Google was just a bailee. *See* Pet'r.Br.15-22. Google users also reasonably expect that this detailed log of their precise movements—pinpointed to within three meters and collected every two minutes—would remain protected from prying eyes, especially the Government's. *Id.* at 22-25.

It should be of no consequence that this personal recordkeeping is accomplished through modern mobile devices, rather than ballpoint pens and paper

(or quill and parchment, for that matter). Though virtual, they are "papers" nonetheless—and as such are entitled to Fourth Amendment protection. Any other conclusion would fall short of protecting the "degree of privacy" that "existed when the Fourth Amendment was adopted." *Kyllo*, 533 U.S. at 34.

In this regard, Location History differs materially from the CSLI considered in *Carpenter*. CSLI is a "species of business record." *Carpenter*, 585 U.S. at 318. "Wireless carriers collect and store [it] for their own business purposes, including finding weak spots in their network and applying 'roaming' charges when another carrier routes data through their cell sites." *Id.* at 301.

Location History, by contrast, "is not a business record, but a journal of a user's location and travels that is created, edited, and stored by and for the benefit of Google users." JA15 (capitalization normalized); *see* Pet.App.268a n.5. As explained, it is a digitized personal record stored in the user's password-protected account, at the user's behest, analogous to "emails on Google's Gmail service" and "documents on Google Drive." JA20. The user maintains full control and can "review, edit, or delete" their data as they please. Pet.App.281a, 283a. If that does not qualify as someone's personal "papers," nothing does.

2. It also makes no difference that users' Location History was stored on Google's servers. "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." *Carpenter*, 585 U.S. at 387 (Gorsuch, J., dissenting). Location History fits that description: It is a comprehensive "digital record" of users' physical

movements. *Riley*, 573 U.S. at 395. The subset of Location History data obtained in this case could have swept in users' journeys to private residences, hospitals, houses of worship, or political rallies. Pet.App.296a; *see* Pet.App.299a-300a. And for those users whose data was de-anonymized, the Government could have connected them to all of these sensitive places. *See* Pet.App.296a, 300a-01a.

Nor does it matter that Google may have used users' Location History for limited and consented-to purposes. Smartphones "are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society." *Carpenter*, 585 U.S. at 315. Today, people should have the "ability to use such services *and* the right to maintain their privacy when they do so." *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies* 111-12 (Dec. 12, 2013), https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf. A contractual bargain with private companies to perform the necessary functions of modern life in exchange for allowing the provider some use of the data cannot defensibly be deemed a wholesale waiver of Fourth Amendment protection in a modern "free society." *Id.* Now more than ever, "[c]onsenting to give a third party access to private papers is not the same thing as consenting to a search of those papers by the government." *Carpenter*, 585 U.S. at 390 (Gorsuch, J., dissenting) (emphasis omitted).

B. The Ultimate Touchstone Of The Fourth Amendment Is Reasonableness

Because collecting Google users' Location History was a search of their "papers," the Court must grapple with whether that search was "reasonable." U.S. Const. amend. IV. While this Court's precedents have required a warrant supported by probable cause for traditional searches, they also recognize that "the ultimate touchstone of the Fourth Amendment is 'reasonableness.'" *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006). That flexibility leaves room for carefully tailored, context-specific rules for modern, data-driven investigation and surveillance methods.

1. Precedent Permits Departures From The Usual Requirement Of A Warrant Supported By Probable Cause

Time and again, this Court has recognized that certain investigative techniques do not fit the traditional warrant-supported-by-probable-cause model. But rather than declare such techniques categorically unconstitutional, the Court has adopted alternative doctrinal frameworks to assess their reasonableness under the Fourth Amendment.

Start with *Camara v. Municipal Court of the City & County of San Francisco*, 387 U.S. 523 (1967). There, a housing inspector attempted to conduct a "routine annual inspection" of an apartment building without a warrant. *Id.* at 526-27. Such inspections were essential to prevent the "unintentional development of conditions which are hazardous to public health and safety"—but also posed "significant intrusions upon the interests protected by the Fourth Amendment." *Id.* at 533-35. To accommodate both

concerns, the Court held that a neutral authority could issue "area" warrants based not on individualized suspicion, but on generalized criteria designed by "reasonable legislative or administrative standards"—such as "the passage of time, the nature of the building, or the condition of the area." *Id.* at 538-39; *accord New York v. Burger*, 482 U.S. 691, 702-03 (1987) (upholding warrantless searches for "closely regulated" businesses so long as "inspection program" provides "a constitutionally adequate substitute for a warrant").

This Court also has upheld many programmatic checkpoint searches. In *Michigan Department of State Police v. Sitz*, the Court upheld a drunk-driving prevention program where "[a]ll vehicles passing through a checkpoint would be stopped and their drivers briefly examined for signs of intoxication." 496 U.S. 444, 447 (1990). The Court reached that conclusion by balancing "the State's interest in preventing drunken driving, the extent to which this system can reasonably be said to advance that interest, and the degree of intrusion upon individual motorists who are briefly stopped." *Id.* at 455. It emphasized that "checkpoints are selected pursuant to [state] guidelines," thus constraining individual officer discretion. *Id.* at 453. And in *Illinois v. Lidster*, the Court upheld a police checkpoint seeking help identifying the perpetrator of a fatal hit-and-run accident that occurred nearby. 540 U.S. 419, 422 (2004). Thus, "the stop's objective was to help find the perpetrator of a specific and known crime, not of unknown crimes of a general sort." *Id.* at 427.

More recently, in *Maryland v. King*, the Court upheld the collection and analysis of DNA samples from detainees via buccal swab, conducted pursuant

to a state statute. 569 U.S. 435, 440-41 (2013). The Court emphasized that "the touchstone of the Fourth Amendment is reasonableness, not individualized suspicion." *Id*. at 448. After weighing the "minor intrusion" of the buccal swab against the "significant state interests" in identifying arrestees, the Court concluded that "DNA identification of arrestees is a reasonable search that can be considered part of a routine booking procedure." *Id*. at 465.

These cases underscore the ability of the Fourth Amendment's reasonableness requirement to accommodate novel measures to ensure public safety, while still guarding against "arbitrary invasions by governmental officials." *Carpenter*, 585 U.S. at 303.

2. The Court Should Conduct A Reasonableness Analysis Informed By The Unique Nature Of These Investigative Tools

The Government obtained Location History for several Google users (including Chatrie) by following a three-step process designed by Google for handling law enforcement requests for user data. Pet.App.286a-91a. At Step One, a magistrate issued a geofence warrant directing Google to disclose anonymized Location History data for "every device" within a 150-meter radius of the crime scene during a one-hour window. Pet.App.294a-95a. At Step Two, Google provided expanded data for nine users covering two hours and removing all geographic limits, without further judicial approval. Pet.App.296a, 299a-300a. At Step Three, again without consulting a judge, Google gave the Government identifying information for three likely suspects. Pet.App.290a-91a, 300a-01a. Rather than

being constrained by the traditional warrant approach, this Court should assess the search's reasonableness in keeping with the Fourth Amendment's core purpose of protecting people from "officers' whim or caprice." *Brinegar v. United States*, 338 U.S. 160, 176 (1949).

1. Chatrie argues that the geofence warrant issued at Step One was a per se unconstitutional "general warrant" because it "did not identify the 'place to be searched' with particularity but instead authorized the search of millions of distinct 'places.'" Pet'r.Br.32. But on that understanding, location data maintained in a database like Google's can *never* be constitutionally obtained, even with a warrant. *Id.* "The sheer breadth" of that position "is disquieting." Pet.App.30a (Wilkinson, J., concurring). And it is wrong: The targeted geofence warrant here was not a "general warrant."

During the Founding Era, general warrants granted officers unfettered discretion to "rummage through homes in an unrestrained search for evidence of criminal activity." *Riley*, 573 U.S. at 403. By contrast, the geofence warrant here was tied to a specific crime that occurred at a particular time and place. Pet.App.291a-92a. The warrant also specified with precision the items to be seized: anonymous location data associated with devices within 150 meters of the bank when the robbery was committed. Pet.App.294a-95a. And Google, not the Government, accessed the database where the data was kept. That targeted procedure is a far cry from the "blanket authority to search where [officers] pleased" that "had so bedeviled the colonists" during the Founding Era. *Stanford v. Texas*, 379 U.S. 476, 481 (1965); *see* Pet.App.18a.

2. The question remains whether obtaining users' Location History in this case was "reasonable." This Court could sensibly resolve the question either way. However the Court resolves the issue, though, it should structure the analysis in a way that encourages sorely needed legislative direction.

For several reasons, the search arguably was reasonable. A neutral magistrate approved a staged process where the "objective was to help find the perpetrator of a specific and known crime." *Lidster*, 540 U.S. at 427. That process swept in relatively few users (nineteen) in the initial geofence warrant, while imposing a relatively "minor intrusion" given the steps taken to preserve their anonymity. *King*, 569 U.S. at 465. Additional Location History data was disclosed for only a subset of those potential suspects. And data was ultimately de-anonymized only for the three users whose movements suggested involvement in the robbery.

At the same time, a "neutral magistrate" did not conduct an "individualized review" of the Government's expanded requests at Steps Two and Three. *Camara*, 387 U.S. at 532-33. Crucial stages of the investigatory process were left to ad hoc negotiations between the Government and Google, with no legally established rules and procedures for them to resolve disputes. No "statutory safeguards" were placed on the Government's ability to use or retain the data it received. *King*, 569 U.S. at 465.

Whatever the Court concludes, its holding should be framed narrowly. Not all geofence warrants are as limited as this one. Some demands for Location History data have been extremely broad, threatening to sweep in thousands of users had Google not refused to comply. *See* Google Amicus Br. 22-26 (compiling

examples). And not every company is Google. Many will lack the gumption or resources to resist demands for sensitive data—and some, like data brokers, have a profit motive to give the Government whatever it wants. Accordingly, the Court should keep in mind the broader landscape of bulk-data surveillance, much of which lacks a close nexus to a specific crime. *Supra* at 14-15.

Ultimately, it will fall on this Court to determine whether and how these tools can be lawfully used. But the Court need not go it alone. Legislative bodies can establish a constitutionally "adequate substitute for a warrant" by fashioning detailed rules and procedures to govern the use of cutting-edge investigation and surveillance techniques. *Burger*, 482 U.S. at 702-03. Looking to such legislative guidance to assess Fourth Amendment reasonableness would permit effective policing, while guarding against the kind of "standardless and unconstrained discretion" deplored by the Framers. *Delaware v. Prouse*, 440 U.S. 648, 661 (1979).

III. THE COURT'S ANALYSIS CAN AND SHOULD BE STRUCTURED TO ENCOURAGE LEGISLATION

Regulating privacy in the twenty-first century "is simply too complex" to leave to one branch alone. Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions*, 111 Mich. L. Rev. 485, 537-38 (2013). Fortunately, this Court can decide this case—and others still to come—in a way that helps push Congress and other legislative bodies to assume their share of the regulatory burden.

A. This Court Has Tools To Promote Urgently Needed Legislative Action

"In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative." *Jones*, 565 U.S. at 429 (Alito, J., concurring in the judgment). "A legislative body," after all, "is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way." *Id.* at 429-30. It is "positive law," not "judicial intuition," that can provide the most nuanced and "detailed guidance on evolving technologies." *Carpenter*, 585 U.S. at 394, 402 (Gorsuch, J., dissenting); *see id.* at 338 (Kennedy, J., dissenting) (urging deference to legislative judgments).

Legislation is essential for data-driven investigation and surveillance methods. Such methods increasingly involve obtaining the data of individuals for whom there is no suspicion. *See supra* at 14-15. Data is collected and held, often for long periods of time, and then analyzed using tools that themselves involve varying degrees of intrusiveness. *See id.* And the utility of these tools often depends on private entities' business decisions about what data to collect—and whether to disclose it. *See id.* What is needed are clear rules that set appropriate bounds for law enforcement when using personal data and new analytic capabilities.

Legislation can address the myriad issues arising in technology-driven policing in detailed and comprehensive ways that case-by-case judicial analysis cannot. But this Court can encourage solutions. In *Berger v. New York*, for example, the Court considered a New York eavesdropping statute,

which permitted ex parte orders authorizing electronic surveillance where there was "reasonable ground to believe that evidence of crime may be thus obtained." 388 U.S. 41, 54 (1967). The Court invalidated that statute under the Fourth Amendment, reasoning that the law established "no requirement for particularity in the warrant as to what specific crime has been or is being committed, nor 'the place to be searched,' or 'the persons or things to be seized.'" *Id.* at 56. Congress responded with Title III, which regulates wiretapping through calibrated predicates, minimization requirements, time limits, and judicial oversight. *See* Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197, 211 (codified as amended at 18 U.S.C. §§ 2510-2522).

Other Fourth Amendment decisions from this Court have not sparked similarly comprehensive legislation—but there is a reason. *Jones* and *Carpenter* held that the usual warrant-supported-by-probable-cause rule applied to certain GPS tracking and CSLI, respectively. *See Carpenter*, 585 U.S. at 316; *Jones*, 565 U.S. at 404-05. Although several Justices emphasized the need for legislation, the Court's decision to resolve both cases under the traditional Fourth Amendment rules—while appropriate on those specific facts—may have dulled the urgency for broader legislative action. The result is a statutory void for many modern investigation and surveillance tools that do not fit comfortably within the usual Fourth Amendment framework.

This Court can encourage much-needed legislation in this area by holding that law enforcement's use of such tools: (1) often constitutes a Fourth Amendment search or seizure; and (2) does

not necessarily require application of traditional warrant principles; but (3) can survive constitutional scrutiny only with sufficient safeguards in place, such as a statute that provides a constitutionally adequate substitute for a warrant.

B. Tying The Fourth Amendment Analysis To Compliance With A Constitutionally Adequate Statutory Scheme Would Encourage Legislation

For data-driven investigation and surveillance techniques, this Court can and should hold that compliance with an adequate statutory scheme provides a sufficient alternative to a traditional warrant supported by probable cause.

In determining what is adequate, courts must bear in mind the Fourth Amendment's central purpose: combatting "arbitrary invasions by governmental officials." *Camara*, 387 U.S. at 528. Searches conducted pursuant to statutory standards and procedures enacted by the People's representatives naturally pose a lesser danger of arbitrary authority, as this Court's precedents recognize. In *Camara*, for example, the Court held that administrative inspection programs may be constitutionally reasonable when conducted pursuant to neutral "legislative or administrative standards," despite the lack of a traditional warrant supported by probable cause. *Id.* at 538. And several times since, the Court has upheld searches conducted pursuant to statutory schemes that "provide[] a constitutionally adequate substitute for a warrant." *Donovan v. Dewey*, 452 U.S. 594, 603 (1981) (mine inspections under federal statute); *see, e.g.*, *Burger*, 482 U.S. at 702-03 (junkyard inspections under state statute).

Of course, mere compliance with—or a violation of—a statutory scheme cannot dictate the Fourth Amendment analysis entirely. *See Virginia v. Moore*, 553 U.S. 164, 168-76 (2008). This Court has not hesitated to invalidate deficient legislative schemes and prescribe their constitutional cures. *See, e.g.*, *City of Los Angeles v. Patel*, 576 U.S. 409, 420-21 (2015) (invalidating hotel registry inspection ordinance). But by inviting deference to law enforcement activities that comply with a duly enacted statutory scheme—so long as the scheme establishes appropriate safeguards—this Court can help "break the public-choice logjam that has kept legislatures from acting" on data-driven investigation and surveillance. Barry Friedman, *Lawless Surveillance*, 97 N.Y.U. L. Rev. 1143, 1199 (2022).

Here, the Court should hold that compliance with appropriate legislation would satisfy the Fourth Amendment. *See* Friedman, *Constitutionality*, *supra*, at 338-41; Friedman, *Lawless Surveillance*, *supra*, at 1169-71. Such legislation could take the following shape:

Predicates. A statute could establish calibrated predicates matched to the degree of intrusiveness of particular types of data searches. *See* Christopher Slobogin, *Virtual Searches: Regulating the Covert World of Technological Policing* 41, 61-67 (2022) (suggesting four levels of predicates proportional to intrusiveness). Not every step in a multi-stage process necessarily requires probable cause. *See, e.g.*, 18 U.S.C. § 2703(a)-(d) (Stored Communications Act) (establishing different predicates for obtaining certain "content" and "noncontent" information). Predicates should progress "from the lowest, such as relevant to an ongoing investigation, to the more

traditional probable cause[] depending on the nature and quantity of the information being accessed." Friedman, *Lawless Surveillance*, *supra*, at 1197.

Proportionality. Legislation could establish rules around the types of crimes for which officers may employ data surveillance. *See* Murphy, *supra*, at 541. Some states have set such limits for the use of certain technologies, such as facial recognition technology, permitting its use only for serious offenses like a "crime of violence" or a "human trafficking offense." Md. Code Ann., Crim. Proc. § 2-503(a)(i); *see, e.g.*, Mont. Code Ann. § 44-15-106(2)(a); Utah Code Ann. § 77-23e-103(2)(c)(i).

Distinctions among kinds of data. Legislation could draw categorical distinctions among types of data. Location data, browsing history, and the like may warrant protection not presently afforded to bank records, pen registers, or IP addresses. Other limits or stronger predicates could be required when requested data risks exposing movements into residences, medical facilities, schools, houses of worship, or other core protected spaces. *See* Murphy, *supra*, at 544.

Safeguards for data accuracy. Another component could be data accuracy and integrity measures to help prevent "all too frequent" errors that can "lead to encounters with the police." Friedman, *Constitutionality*, *supra*, at 313. Data providers could be required to disclose known accuracy limitations and mandate corroboration before any data unmasking or attempts at arrest. *See* Friedman, *Lawless Surveillance*, *supra*, at 1193-97.

Limits on data storage, security, and retention. In scrutinizing CSLI, *Carpenter*

emphasized the danger in "the retrospective quality of the data" that is subject only to the "retention polic[i]es of the wireless carriers," and allows "the Government [to] travel back in time to retrace a person's whereabouts." 585 U.S. at 312. Legislation could require use restrictions, retention limits, encryption, detailed audit logs, and data breach notifications. *See* Friedman, *Lawless Surveillance*, *supra*, at 1193-97; *see, e.g.*, Tenn. Code Ann. § 55-10-302(b) (generally requiring data deletion after 90 days); Utah Code Ann. § 41-6a-2004 (nine months).

Accountability and oversight. To ensure accountability and oversight, legislation also could require a neutral magistrate to authorize each stage of a graduated warrant process, require warrant returns, and establish periodic compliance audits. *See* Murphy, *supra*, at 541-42; Friedman, *Constitutionality*, *supra*, at 342; Friedman, *Lawless Surveillance*, *supra*, at 1180, 1197-98.

Courts ultimately will need to determine whether any such statutory scheme is constitutionally adequate. Yet with proper guidance, such frameworks will emerge, as they did with Title III. *Supra* at 27-28. This Court should foster them.

C. Unresolved Statutory Questions Could Impact The Constitutional Analysis In This Case

The irony in this case is that the search at issue *did* implicate two existing statutes—the Stored Communications Act ("SCA"), 18 U.S.C. § 2703, and a recently amended state law analog, Va. Code Ann. § 19.2-70.3. *See* JA129 (warrant application invoking latter statute). But the parties have not addressed, and the lower courts did not decide, whether those

statutes were complied with—much less whether compliance would satisfy the Fourth Amendment.

Both the SCA and Virginia's analog require a warrant based on probable cause to compel the disclosure of the "contents" of certain electronic communications. *See* 18 U.S.C. § 2703(a); Va. Code Ann. § 19.2-70.3(C). Throughout this case, Google has argued that Location History—unlike the CSLI at issue in *Carpenter*—is "substantive information." JA28-31. For that reason, it might qualify as "contents" under these laws, subjecting geofence warrants to the highest tier of statutory protection. *Id.* If that's correct, the lack of individualized suspicion at Step One and the magistrate's absence at Steps Two and Three of the warrant process likely violated both statutes, which in turn cuts against Fourth Amendment reasonableness. Even if it is not correct and Location History does *not* qualify as "contents," the question still remains whether the magistrate's degree of involvement satisfied both laws. Answers to those threshold statutory compliance questions could inform whether either legislative scheme provided a "constitutionally adequate substitute for a warrant" in this case. *Patel*, 576 U.S. at 426. At a minimum, they would help inform resolution of the Fourth Amendment question.

However the Court rules, it should leave room for compliance with an appropriate statutory scheme to inform the Fourth Amendment analysis in this rapidly evolving context. Encouraging legislation in this way could help stave off the "very unfortunate" status quo, where "privacy protection in the 21st century" has been "left primarily to the federal courts using the blunt instrument of the Fourth Amendment." *Riley*, 573 U.S. at 408 (Alito, J.,

concurring in part and concurring in the judgment). And it would serve the Fourth Amendment's core purpose of preventing arbitrary governmental intrusions, while preserving space for legislative action and effective policing.

CONCLUSION

For the foregoing reasons, this Court should hold that a search occurred and that compliance with an adequate statutory scheme may render it reasonable.

Respectfully submitted,

BARRY FRIEDMAN
MARIA PONOMARENKO
MAX ISAACS
KATIE KINSEY
POLICING PROJECT AT
NYU SCHOOL OF LAW
40 Washington Sq. S.
New York, NY 10012

NICHOLAS ROSELLINI
Counsel of Record
LATHAM & WATKINS LLP
500 Montgomery Street
Suite 2000
San Francisco, CA 94111
(415) 395-8165
nick.rosellini@lw.com

SUMER GHAZALA
MAHSHAD BADII
LATHAM & WATKINS LLP
555 11th Street, NW
Suite 1000
Washington, DC 20004

Counsel for Amicus Curiae

March 9, 2026