No. 22-4489

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

OKELLO T. CHATRIE,

Defendant-Appellant,

On Remand from the
United States Supreme Court

BRIEF OF *AMICI CURIAE* SIX LAW PROFESSORS IN SUPPORT OF DEFENDANT-APPELLANT

Megan Graham
Clinical Law Programs
University of Iowa College of Law
380 Boyd Law Building
Iowa City, IA 52242
(319) 335-9023

Counsel for Amici Curiae

TABLE OF CONTENTS

TABLE OF CONTENTS ..... **i**

TABLE OF AUTHORITIES ..... **ii**

INTEREST OF *AMICI CURIAE* **1**

INTRODUCTION AND SUMMARY OF ARGUMENT **2**

ARGUMENT **4**

I. Reverse Warrants Gratuitously Empower the Government Without Appropriate Fourth Amendment Checks. 4

II. There Are Many Other Data Sources that May Lead to Invasive Reverse Searches If the Geofence Warrant in This Case Is Found Constitutional. 8

A. The Critical Characteristics of Geofence and Other Reverse Searches Raise Significant Constitutional Concerns. 9

B. Reverse Keyword Searches 11

C. AI Chatbots 13

D. Cloud Searches 16

E. People and Object Recognition in Video and Image Surveillance 19

F. What Comes Next: Capturing and Commodifying Human Experience 22

III. Implications 25

CONCLUSION **29**

CERTIFICATE OF COMPLIANCE **30**

TABLE OF AUTHORITIES

CASES

Berger v. New York,
388 U.S. 41 (1967) 6, 27

Boyd v. United States,
116 U.S. 616 (1886) 7

Camara v. Mun. Ct.,
387 U.S. 523 (1967) 4

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

Carroll v. United States,
267 U.S. 132 (1925) 4

Chatrie v. United States,
146 S. Ct. 2193 (2026) 4, 5, 7, 25

Coolidge v. New Hampshire,
403 U.S. 443 (1971) 12

Groh v. Ramirez,
540 U.S. 551 (2004) 6

In re Four Appls. for Search Warrants Seeking Info. Associated with Particular Cellular Towers,
No. 3:25-CR-38, 2026 WL 2260371 (S.D. Miss. Aug. 5, 2026) 9

In re Search of Info. Stored at Premises Controlled by Google, as Further Described in Attachment A,
No. 20-mc-297, 2020 WL 5491763 (N.D. Ill. July 8, 2020).....28

In re Search of Info. that Is Stored at Premises Controlled by Google LLC,
579 F. Supp. 3d 62 (D.D.C. 2021).....26

Leaders of a Beautiful Struggle v. Balt. Police Dep't,
2 F.4th 330 (4th Cir. 2021) (en banc) 20

Osborn v. United States,
385 U.S. 323 (1966) 27

People v. Seymour,
536 P.3d 1260 (Colo. 2023) 11

Riley v. California,
573 U.S. 373 (2014) 5, 7

United States v. Brown,
No. 1:16-cr-427-AT-JKL-31, 2025 WL 1674283 (N.D. Ga. June 13, 2025) 25

United States v. Chatrie,
590 F. Supp. 3d 901, 937 (E.D. Va. 2022), *aff'd*, 107 F.4th 319 (4th Cir. 2024), *on reh'g en banc*, 136 F.4th 100 (4th Cir. 2025), *vacated and remanded*, 146 S. Ct. 2193 (2026) 28

United States v. Di Re,
332 U.S. 581 (1948) 7, 8

United States v. Dickerson,
No. 24-cr-83-BHL, 2025 WL 2779095 (E.D. Wis. Sept. 30, 2025) 8

United States v. Heppner,
No. 25-CR-503-JSR, 2026 WL 436479 (S.D.N.Y. Feb. 17, 2026) 15

United States v. McCracken,
No. 24-cr-3-JFM, 2025 WL 3034953 (E.D. Pa. Oct. 30, 2025) 8

United States v. McLamb,
880 F.3d 685 (4th Cir. 2018).....28

United States v. Pilling,
721 F. Supp. 3d 1113 (D. Idaho 2024) 18

United States v. Ray,
541 F. Supp. 3d 355 (S.D.N.Y. 2021).....18

United States v. Smith,
110 F.4th 817 (5th Cir. 2024), *cert. denied*, 146 S. Ct. 356 (2025).....28

United States v. Torres,
751 F.2d 875 (7th Cir. 1984).....27

United States v. Warshak,
631 F.3d 266 (6th Cir. 2010).....18

Ybarra v. Illinois,
444 U.S. 85 (1979) 6, 12, 25

Zurcher v. Stanford Daily,
436 U.S. 547 (1978) 26

CONSTITUTIONAL PROVISIONS

U.S. Const. amend. IV 6, 8

STATUTES

18 U.S.C. § 2518(3)(c).....27

OTHER AUTHORITIES

Aff., Compl., *United States v. Rinderknect*,
No. 2:25-mj-06103 (C.D. Cal. Oct. 2, 2025),
https://perma.cc/HB5U-YHSA.....14

Aisha Malik, *ChatGPT Reaches 900M Weekly Active Users*,
TechCrunch (Feb. 27, 2026), https://perma.cc/AMQ6-A6Z4 14

Alicia Solow-Niederman, *Information Privacy and the Inference Economy*,
117 Nw. U. L. Rev. 357 (2022).....21

Andrew Guthrie Ferguson, *Digital Rummaging*,
101 Wash. U. L. Rev. 1473 (2024) 5

Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*,
105 Minn. L. Rev. 1105 (2021) 22

Apple, *Introduction to iCloud*, *in* iCloud User Guide,
https://perma.cc/K89C-YS2C (last visited Sept. 7, 2026).....17

Brian L. Owsley, *Searching a Person's Thoughts: Keyword Search Warrants and Fourth Amendment Concerns*,
28 Stan. Tech. L. Rev. 66 (2025) 12

Brian L. Owsley, *The Best Offense Is a Good Defense: Fourth Amendment Implications of Geofence Warrants*,
50 Hofstra L. Rev. 829 (2022).....5, 13

Clare Garvie & Laura Moy, *America Under Watch: Face Surveillance in the United States*, Geo. Ctr. on Priv. & Tech. (May 16, 2019),
https://perma.cc/DG38-HV7A.....22

Deven R. Desai, *Constitutional Limits on Surveillance: Associational Freedom in the Age of Data Hoarding*,
90 Notre Dame L. Rev. 579 (2014) 21

Dropbox, Inc., Annual Report (Form 10-K) (Feb. 20, 2026) 16

Emmelyn A. J. Croes et al., *Digital Confessions: The Willingness to Disclose Intimate Information to a Chatbot and Its Impact on Emotional Well-Being*,
36 Interacting with Comput. 279 (2024) 15

Gina Kolata, *A.I. Is Making Doctors Answer a Question: What Are They Really Good For?*, N.Y. Times (Feb. 9, 2026),
https://perma.cc/VN8B-CFMB 15

Google Cloud Blog, *Building the Industry's Best Agentic AI Ecosystem with Partners* (Apr. 9, 2025), https://perma.cc/V42B-5BUJ.....16

Jason Koebler, *Leaked Email Suggests Ring Plans to Expand "Search Party" Surveillance Beyond Dogs*, 404 Media (Feb. 18, 2026), https://perma.cc/KH2P-SXKG 20

Jean Tirole, *Digital Dystopia*, 111 Am. Econ. Rev. 2007 (2021) 21

Jennifer King et al., *User Privacy and Large Language Models: An Analysis of Frontier Developers' Privacy Policies*, 8 Ass'n for Advancement of A.I./Ass'n for Computing Machinery Conf. on AI, Ethics & Soc. 1465 (2025) 14

Jennifer Pattison Tuohy, *Ring Cancels Its Partnership with Flock Safety After Surveillance Backlash*, The Verge (Feb. 12, 2026), https://perma.cc/Q25P-YCCC 20

Jill Cowan & Valerie B. Ramsey, *Who Is Jonathan Rinderknecht? What We Know About the Palisades Fire*, N.Y. Times (Oct. 8, 2025), https://perma.cc/EK4D-FG8U 14

Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 Mach. Learning Rsch. 87 (2018).....22

Junfeng Jiao et al., *LLMs and Childhood Safety: Identifying Risks and Proposing a Protection Framework for Safe Child-LLM Interaction* (Urb. Info. Lab, Univ. of Tex., Working Paper DOI: 10.48550, 2025).....14

Kavous Salehzadeh Niksirat et al., *Wearable Activity Trackers: A Survey on Utility, Privacy, and Security*, 56 ACM Comput. Surv. 1 (2024) 24

Lauren Jackson, *Finding God in the App Store*, N.Y. Times (Sept. 14, 2025), https://perma.cc/3ZE9-Y2S3 15

Martin Armstrong, *What's in the Cloud?*, Statista Global Consumer Survey (Sept. 30, 2021), https://perma.cc/3Q6E-STA5 17

Michael Levin & Josh Lowitz, *An Update on Apple Services – iCloud Still Leads the Way*, Consumer Intel. Rsch. Partners Apple Report (Feb. 18, 2026), https://perma.cc/7WLE-TRXG 16

Nils Gilman, *If You Tell ChatGPT Your Secrets, Will They Be Kept Safe?*, N.Y. Times (Nov. 10, 2025), https://perma.cc/698D-XKDP 13

PaloAlto Networks, *The State of Cloud Data Security 2023* (2023), https://perma.cc/F6G2-Y44J 17

Patrick Grother et al., Nat'l Inst. Stds. & Tech., *Internal Rep. 8280, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects* (2019), https://perma.cc/6THV-EVQL 22

Patrick Magee et al., *Beyond Neural Data: Cognitive Biometrics and Mental Privacy*, 112 Neuron 3017 (2024) 24

Petar Radanliev, *Privacy, Ethics, Transparency, and Accountability in AI Systems for Wearable Devices*, Frontiers in Digit. Health (2025) 23

Pratyusha Ria Kalluri et al., *Computer-Vision Research Powers Surveillance Technology*, 643 Nature 73 (2025).....20

Press Release, Apple, Inc., *Apple Reports First Quarter Results* (Jan. 29, 2026), https://perma.cc/SP87-QZMF 16

Raluca Budiu, *Mental Models for Cloud-Storage Systems*, Nielsen Norman Grp. (Nov. 24, 2019), https://perma.cc/32WT-57LK.....17

Rob. T. Lee, *AI Chat Data Is History's Most Thorough Record of Enterprise Secrets*, Dark Reading (Oct. 17, 2025), https://perma.cc/4YP7-Z3US 13

Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (2019) 23

Susan Freiwald & Paul Ohm, *Superwarrants*, 68 Ariz. L. Rev. 359 (2026) 27

T.J. Thomson et. al., *Visual Mis/disinformation in Journalism and Public Communications: Current Verification Practices, Challenges, and Future Opportunities*, 16 Journalism Prac. 938, 940 (2020) 19

Thomas Brewster, *Feds Ordered Google to Unmask Certain YouTube Users. Critics Say It's* 13

Vidhya Srinivasan, *AI, Personalization and the Future of Shopping*, Google (Mar. 3, 2025), https://perma.cc/PAA4-ATXT 12

INTEREST OF *AMICI CURIAE*

Amici curiae are law professors with expertise in Fourth Amendment jurisprudence and its application to digital surveillance. *Amici*'s interest here is limited to informing this Court about other reverse warrants that are relevant to the consideration of this case.[1]

Amici are[2]:

- Terrence Cain, Professor of Law, University of Arkansas at Little Rock William H. Bowen School of Law;
- Catherine Crump, Robert Glushko Clinical Professor of Practice in Technology Law, UC Berkeley, School of Law;
- Megan Graham, Clinical Professor, University of Iowa College of Law;
- Paul Ohm, Professor of Law, Georgetown University Law Center;
- Brian Owsley, Associate Professor of Law, University of North Texas Dallas College of Law; and
- Jordan Wallace-Wolf, Assistant Professor of Law, University of Arkansas-Little Rock William H. Bowen School of Law.

---

[1] Counsel for *amici* affirms that no party's counsel authored this brief in whole or in part, nor did any party or any party's counsel contribute money intended to fund preparing or submitting this brief. No person other than *amici* or their counsel contributed money to fund the preparing or submitting of this brief. All parties consent to the filing of this brief. Fed. R. App. P. 29(a)(2).

[2] Institutional affiliations are included for identification purposes only.

INTRODUCTION AND SUMMARY OF ARGUMENT

We write to help this Court understand that the outcome and reasoning of this case could unleash a much broader wave of similar reverse searches, and to identify pools of private information that investigators are likely to want to fish in next. Geofence queries are not unique and if the court permits them subject to nothing more than a simple (or multi-staged) search warrant, it will set the stage for a dramatic increase in law enforcement power to track location and many other sorts of private information.

We all create an ever-growing amount of data and information about our daily lives. We create data about our location on a second-to-second basis, detailed catalogues of our thoughts and questions about the world, images of everything in our lives, and detailed portraits of our health and wellbeing. For convenience, we keep much of this data in private storage with online service providers. This collection of information creates a ripe target for deep and detailed traditional searches aimed at a particular suspect or suspects of the kind at issue in *Carpenter*, actions that are likely constitutionally permitted when supported by individualized probable cause. 585 U.S. 296, 316 (2018). However, these data troves can also be swept into dragnet *reverse* searches, such as the geofence query conducted in this case, which sweep in the private information of many people, absent meaningful

and individualized suspicion about any particular person who may be caught up.

Supreme Court precedent has long established that the Fourth Amendment requires "some quantum of individualized suspicion" before the government can search through the privacies of life. *Id.* at 317. Whether the government can carry out a particular criminal investigative technique hinges on having such suspicion.

Reverse warrants literally reverse this principle, turning it on its head. Though each type of reverse search presents its own doctrinal concerns, there are common traits among investigative techniques that are dangerously "reverse" in nature. Those features include that the investigative technique will: (1) likely result in many persons' information being turned over to law enforcement based on the search; (2) target large quantities of user-generated information; (3) capture information about behavior that is overwhelmingly legal and, in any case, highly sensitive or intimate in nature, even if there are also legitimate suspects in the warrant return; and (4) cast suspicion on individuals because of their mere proximity to allegedly illegal activities.

These four dangers—present to various degrees in every reverse search we highlight—are magnified because each search can enable and incentivize other reverse searches. A geofence search may place someone at a scene, which enables camera footage to be used to view

their likely route away from it, which may reveal an item, which can then be reverse image searched to find others who came into contact with it, etc. In short, reverse investigative tools individually, and when chained together, risk massively increasing government power in a way that is in direct tension with traditional Fourth Amendment jurisprudence. As such, this Court should rule that the geofence warrant in this case violated Mr. Chatrie's Fourth Amendment rights and craft rules to prevent the expansive use of other reverse searches.

ARGUMENT

I. Reverse Warrants Gratuitously Empower the Government Without Appropriate Fourth Amendment Checks.

"From the founding onward," the Supreme Court has repeatedly explained that "the Fourth Amendment has sought to secure the 'privacies of life' against the exercise of 'arbitrary power.'" *Chatrie v. United States*, 146 S. Ct. 2193, 2205 (2026); *see also Carpenter*, 585 U.S. at 303 (quoting *Camara v. Mun. Ct.*, 387 U.S. 523, 528 (1967)). "Although no single rubric definitively resolves which expectations of privacy are entitled to protection, the analysis is informed by historical understandings of what was deemed an unreasonable search and seizure when the Fourth Amendment was adopted." *Carpenter,* 585 U.S. at 304–05 (footnote, quotation marks, and brackets omitted) (quoting *Carroll v. United States*, 267 U.S. 132, 149 (1925)). And, as the Supreme Court has repeatedly recognized, "the Fourth Amendment was the

founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity." *Riley v. California*, 573 U.S. 373, 403 (2014); *Carpenter*, 585 U.S. at 303 (quoting *Riley* for this proposition); *see also* Andrew Guthrie Ferguson, *Digital Rummaging*, 101 Wash. U. L. Rev. 1473 (2024).

In *Carpenter*, the Court found the warrantless search of known individuals' cell-site location information was too intrusive to survive constitutional challenge. 585 U.S. at 316. In Mr. Chatrie's case, the Supreme Court recognized that geofence warrants involve searches that are even more revealing than the targeted search at issue in *Carpenter*. *See Chatrie*, 146 S. Ct. at 2208, 2213. The government in this and similar cases rummages through millions of accounts without particular suspicion as to any specific account. *See* Brian L. Owsley, *The Best Offense Is a Good Defense: Fourth Amendment Implications of Geofence Warrants*, 50 Hofstra L. Rev. 829, 835 (2022). Geofence queries are difficult to distinguish from similar kinds of reverse searches that are poised to provide push-button access to huge pools of private evidence stored with online providers. Your location data is hardly the only data that can be reverse-queried.

No warrant that ranges over the protected data of hundreds of millions of people can be said to comply with the textual requirement of

"particularly describing the place to be searched, and the persons or things to be seized," U.S. Const. amend. IV, or the precedents elaborating that requirement. *E.g.*, *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979); *Groh v. Ramirez*, 540 U.S. 551, 561 (2004) ("[T]he purpose of the particularity requirement is not limited to the prevention of general searches. A particular warrant also assures the individual whose property is searched or seized of the lawful authority of the executing officer, his need to search, and the limits of his power to search." (internal quotation marks and citations omitted)); *Berger v. New York*, 388 U.S. 41, 55–58 (1967). As the Supreme Court has made clear,

> [w]here the standard is probable cause, a search or seizure of a person must be supported by probable cause particularized with respect to that person. This requirement cannot be undercut or avoided by simply pointing to the fact that coincidentally there exists probable cause to search or seize another or to search the premises where the person may happen to be.

Ybarra, 444 U.S. at 91.

We are guided by Supreme Court precedents explaining that although *Katz* focuses on expectations of *privacy*, the central goal of the Amendment is to place limits on the *power* of law enforcement. *Carpenter* outlines two "basic guideposts" for the expectation of privacy test:

> First, that the Amendment seeks to secure "the privacies of life" against "arbitrary power." *Boyd v. United States*, 116 U.S. 616, 630 (1886). Second, and relatedly, that a central

> aim of the Framers was "to place obstacles in the way of a too permeating police surveillance." *United States v. Di Re*, 332 U.S. 581, 595 (1948).

Carpenter, 585 U.S. at 305; *see also Chatrie*, 146 S. Ct. at 2205. These decisions make clear that a key role of the Fourth Amendment is to stand in the way of the government enjoying a passive inheritance of digital omniscience.

This focus on power has led the Supreme Court to emphasize the science-fiction-like capabilities of the modern technologies provided by device manufacturers and online service providers. *See, e.g.*, *Carpenter*, 585 U.S. at 312 (comparing searching cell-site location information to time travel); *Riley*, 573 U.S. at 385 (comparing advances in cell phones to rocket travel and questioning what Martians would make of our attachment to them). Keeping with the science fiction theme, these devices and the records they produce essentially transform law enforcement officers into crime-fighting robots outfitted with superhuman powers. They can peer into the past, avoiding the "frailties of recollection." *Carpenter*, 585 U.S. at 312. They can track every suspect "every moment of every day for five years." *Id.* They are "tireless," "ever alert, and their memory is nearly infallible." *Id.* at 312, 314.

The point of the Supreme Court's method is not to engage in speculation about an uncertain future. It is to help identify when and where to "place obstacles in the way of a too permeating police

surveillance," *id.* at 305 (quoting *Di Re*, 332 U.S. at 595). And courts must attend to the extraordinary power of the police not only when deciding whether something qualifies as a "search," but also when ensuring that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV.

II. There Are Many Other Data Sources that May Lead to Invasive Reverse Searches If the Geofence Warrant in This Case Is Found Constitutional.

Geofence queries are not the only reverse searches the police have employed in recent years. There are other, newer forms of reverse location searches that are emerging, including so-called area or Timing Advance warrants for information from cell phone providers. *See, e.g.*, *United States v. Dickerson*, No. 24-cr-83-BHL, 2025 WL 2779095, at *1 (E.D. Wis. Sept. 30, 2025) (stating that two Timing Advance location information warrants resulted in law enforcement identifying 44,000 devices in the relevant areas); *United States v. McCracken*, No. 24-cr-3-JFM, 2025 WL 3034953, at *1 (E.D. Pa. Oct. 30, 2025) (stating that Timing Advance and related warrants revealed information about "thousands of devices"); *see also In re Four Appls. for Search Warrants Seeking Info. Associated with Particular Cellular Towers*, No. 3:25-CR-38, 2026 WL 2260371, at *10 (S.D. Miss. Aug. 5, 2026) (stating that cell

tower-dump information sought "could produce thousands if not tens of thousands of cellular records" if warrants were issued). And law enforcement agencies have obtained warrants to search through Google's and other companies' databases of search engine queries, conducting fishing expeditions through the thoughts and reading habits of millions of users.

But these sorts of reverse queries are just the tip of the iceberg. As this Court considers this geofence warrant, it should be mindful of other data sources that will attract police dragnets if this search warrant is upheld. Understanding what will follow on the heels of this case will help this Court fashion rules that attend not only to geofence searches but also to their close investigative cousins.

A. The Critical Characteristics of Geofence and Other Reverse Searches Raise Significant Constitutional Concerns.

Geofence warrants possess several critical characteristics that raise significant concerns about user privacy, government power, and constitutionality. These characteristics serve as a guide for identifying other private data stores that might attract problematic reverse search requests in the future.

To be clear, each of the examples we review are similar but not identical to geofence warrants. Each will implicate privacy and government power in its own way. We do not mean to suggest that

these characteristics offer a rule for assessing Fourth Amendment questions; they are instead a "field guide" for identifying the kinds of investigative novelties that police may turn to next, if they feel empowered by this Court's opinion.

First, like geofence queries, each of our examples involve the information of many people being turned over to law enforcement.

Second and relatedly, the reverse searches we identify target large databases of user-generated information.

Third, the information accumulated by these searches overwhelmingly concerns legal conduct that is highly intimate or sensitive in nature, and which is often given legal protection in its own right.

Fourth, each of these searches group people into proximate association with other people based not necessarily on human relationships, much less conspiratorial association, but rather on superficial attribute matching. For example, they group together people in the same place, who use the same kinds of keywords, or who read the same kind of content.

Consider the following examples of reverse searches. Some of these are already being used by the police, albeit in sporadic fashion. Others loom on the horizon.

B. Reverse Keyword Searches

A reverse keyword search warrant enables law enforcement to discover every person who has used a search engine to obtain information about any topic imaginable. Instead of starting with probable cause for a specific target or suspect identified with particularity, a reverse keyword search warrant pores through every search query that every user of that search engine has submitted (possibly confined to a period of time or from IP addresses associated with a specific city or region), obtaining data on a global scale. These warrants target specific words or phrases to attempt to develop a lineup of potential suspects instead of targeting a known suspect. In other words, law enforcement can and does use reverse keyword search warrants to identify potential suspects based on their thoughts and ideas as expressed in internet searches.

When law enforcement applies for a reverse keyword search warrant from search engine providers, the government utilizes a multi-staged process similar to the one used for geofence warrants. *See People v. Seymour*, 536 P.3d 1260, 1268–69 (Colo. 2023). Thus, reverse keyword search warrants raise serious constitutional concerns similar to those raised by geofence warrants, including lack of particularity and overbreadth. Although specific numbers on how often they are used are unavailable, law enforcement's use of this investigative approach is on the rise. *See, e.g.*, Brian L. Owsley, *Searching a Person's Thoughts:*

Keyword Search Warrants and Fourth Amendment Concerns, 28 Stan. Tech. L. Rev. 66 (2025).

Search engine providers complying with this type of warrant are required to search databases that capture the sum total of their users' queries to find users who have expressed particular thoughts or interests included on the government's list of terms. In a given day, Google alone receives more than 13.5 billion search queries. *See* Vidhya Srinivasan, *AI, Personalization and the Future of Shopping*, Google (Mar. 3, 2025), https://perma.cc/PAA4-ATXT (indicating that, based on internal data, there are "more than 5 trillion searches on Google annually"). Such a search will invariably capture numbers of innocent individuals who innocuously typed in the phrase, leading to some receiving significantly closer scrutiny by law enforcement and potentially facing charges, even though all they did was search a term or phrase. *See Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971) (decrying "a general, exploratory rummaging in a person's belongings" by law enforcement); *Ybarra*, 444 U.S. at 91.

Additionally, reverse warrants that are intertwined with people's thoughts are not strictly limited to search query databases. They can also be used to search for all users who watched particular videos on platforms like TikTok and YouTube. *See* Thomas Brewster, *Feds Ordered Google to Unmask Certain YouTube Users. Critics Say It's "Terrifying.*," Forbes (May 22, 2024), http://perma.cc/Z8L3-A6Q3. Such a

search will not only affect many innocent adults, but likely minors as well.

As with geofence warrants, reverse keyword searches are overly broad, targeting large quantities of user-generated information that captures far too many individuals' personal data. Geofence warrants have swept up innocent persons who merely were in the wrong place at the wrong time. *See, e.g.,* Owsley, *The Best Offense*, *supra*, at 829–30 (discussing Zachary McCoy and Jorge Molina who were both falsely accused until obtaining attorneys to defend them). It is only a matter of time before innocent people suffer unjustified police scrutiny or worse due to what they have searched, or put another way, due to what they have thought.

C. AI Chatbots

The emerging and growing use of artificial intelligence ("AI") in many aspects of life provides a new target for government investigations. Rob. T. Lee, *AI Chat Data Is History's Most Thorough Record of Enterprise Secrets*, Dark Reading (Oct. 17, 2025), https://perma.cc/4YP7-Z3US; Nils Gilman, *If You Tell ChatGPT Your Secrets, Will They Be Kept Safe?*, N.Y. Times (Nov. 10, 2025), https://perma.cc/698D-XKDP. ChatGPT use has grown faster than any consumer software application in history, and it is used by roughly 900 million people weekly, many of them minors. Aisha Malik, *ChatGPT Reaches 900M Weekly Active Users*, TechCrunch (Feb. 27, 2026),

https://perma.cc/AMQ6-A6Z4. The youngest generations may not learn to "search" at all, but to "chat." Jennifer King et al., *User Privacy and Large Language Models: An Analysis of Frontier Developers' Privacy Policies*, 8 Ass'n for Advancement of A.I./Ass'n for Computing Machinery Conf. on AI, Ethics & Soc. 1465 (2025); Junfeng Jiao et al., *LLMs and Childhood Safety: Identifying Risks and Proposing a Protection Framework for Safe Child-LLM Interaction* 12 (Urb. Info. Lab, Univ. of Tex., Working Paper DOI: 10.48550, 2025). All this use generates an ocean of data in the form of saved conversations, an irresistible one through which to drag law enforcement nets.[3]

Reverse searches through chat data—e.g., "who chatted about setting a building on fire in this area around this time?"—will trawl through the unguarded and raw thoughts of millions. Unlike a diary, chatbots do not just receive the thoughts of the user, but they are designed to adapt to them, elicit them, and anticipate them. The interactive nature of chatbots encourages private disclosures because users respond to the life-like aspect of a chatbot, even if they know, at

[3] Traditional searches of AI chatbot data based on individualized suspicion are already happening. *See e.g.*, Jill Cowan & Valerie B. Ramsey, *Who Is Jonathan Rinderknecht? What We Know About the Palisades Fire*, N.Y. Times (Oct. 8, 2025), https://perma.cc/EK4D-FG8U; Aff. at 10, Compl., *United States v. Rinderknect*, No. 2:25-mj-06103 (C.D. Cal. Oct. 2, 2025), https://perma.cc/HB5U-YHSA. It is only a matter of time before reverse searches follow, if they have not happened already.

some level, that it is not a human companion or adviser. Emmelyn A. J. Croes et al., *Digital Confessions: The Willingness to Disclose Intimate Information to a Chatbot and Its Impact on Emotional Well-Being*, 36 Interacting with Comput. 279 (2024). This leads many people to lower their guards as they chat, responding to what feels like a free-flowing conversation.

Moreover, chatbot conversations can be about highly sensitive topics involving intimate thoughts. A full list would overwhelm, but users engage chatbots as: financial advisors; doctors; lawyers; spiritual advisors; companions and confidants; role-players and fantasy facilitators; and more. *See, e.g.*, Gina Kolata, *A.I. Is Making Doctors Answer a Question: What Are They Really Good For?*, N.Y. Times (Feb. 9, 2026), https://perma.cc/VN8B-CFMB (chatbots as doctors); *United States v. Heppner*, No. 25-CR-503-JSR, 2026 WL 436479, at *1–*4 (S.D.N.Y. Feb. 17, 2026) (as lawyers); Lauren Jackson, *Finding God in the App Store*, N.Y. Times (Sept. 14, 2025), https://perma.cc/3ZE9-Y2S3 (as spiritual advisors).

If this Court permits broad geofence queries like what happened in this case, it will help clear the way for prosecutors to explore the dragnet possibilities of conducting reverse searches of chatbot data, as they have with keyword search data. Rather than obtain information about a particular suspect's chats, investigators might request chats about the circumstances of the crime or its location, raising the specter

of revealing highly private, innocent chats that may superficially match a search query, but are instead the products of fantasy, role play, hyperbole, or curiosity.

D. Cloud Searches

Individuals and businesses have increasingly embraced cloud storage over the past decade-plus, largely because of its convenience. Disclosures from some of the biggest cloud providers suggest that the total user base numbers in the billions. Google Cloud Blog, *Building the Industry's Best Agentic AI Ecosystem with Partners* (Apr. 9, 2025), https://perma.cc/V42B-5BUJ (indicating over 3 billion global users for Google Workspaces); Press Release, Apple, Inc., *Apple Reports First Quarter Results* (Jan. 29, 2026), https://perma.cc/SP87-QZMF (stating there are 2.5 billion active Apple devices); Michael Levin & Josh Lowitz, *An Update on Apple Services – iCloud Still Leads the Way*, Consumer Intel. Rsch. Partners Apple Report (Feb. 18, 2026), https://perma.cc/7WLE-TRXG (70% of recent U.S. Apple device buyers report paying for the upgraded tier of iCloud storage in the most recent quarter); Dropbox, Inc., Annual Report (Form 10-K) (Feb. 20, 2026) (stating Dropbox has over 700 million registered users).

The kinds of data stored in the cloud are comprehensive, sensitive, and personal. Apple automatically stores data including a user's passwords, financial transactions, travel history from connected GPS apps, photos, email messages, personal notes and reminders, calendars,

contacts, and work or personal documents in its cloud. Apple, *Introduction to iCloud*, *in* iCloud User Guide, https://perma.cc/K89C-YS2C (last visited Sept. 7, 2026). An analysis of thirteen billion files stored in public cloud environments found that over thirty percent of cloud data assets contained sensitive information, including social security numbers, credit card numbers, and other types of personally identifiable information. PaloAlto Networks, *The State of Cloud Data Security 2023* (2023), https://perma.cc/F6G2-Y44J. A 2020 user survey concluded that a significant portion of U.S. users store sensitive information in the cloud, including office documents (thirty-five percent), passwords and log-in data (twenty-seven percent), and financial information (seventeen percent). Martin Armstrong, *What's in the Cloud?*, Statista Global Consumer Survey (Sept. 30, 2021), https://perma.cc/3Q6E-STA5. Surveys suggest that people trust the security and privacy of the cloud, especially when their employers bolster the legitimacy of the cloud through professional use. Raluca Budiu, *Mental Models for Cloud-Storage Systems*, Nielsen Norman Grp. (Nov. 24, 2019), https://perma.cc/32WT-57LK.

While we do not know the extent to which law enforcement has attempted to use reverse warrants to search the vast stores of information held by cloud storage providers, warrant applications have been filed in the traditional direction to compel disclosure of content stored in a particular, specified individual's cloud storage account. *See,*

e.g., *United States v. Ray*, 541 F. Supp. 3d 355 (S.D.N.Y. 2021) (upholding warrant to search defendant's iCloud account for communications, photos, and videos); *United States v. Pilling*, 721 F. Supp. 3d 1113, 1118–19 (D. Idaho 2024) (reviewing warrants to search the defendant's Google and iCloud accounts). It has also become routine for the police to order providers of cloud-based email services to produce a specified user's email messages. *See, e.g.*, *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) (holding that email users enjoy a reasonable expectation of privacy in the contents of emails stored with a provider).

This Court's ruling in this case may embolden law enforcement to begin searching our online files in reverse. Tax agents might ask a cloud service to search all its hosted accounts for tax forms indicating a particular form of tax fraud. The FBI investigating a government whistleblower might ask Dropbox to find draft copies of a letter sent to Congress or to the Washington Post. Homeland Security agents might ask Google to search email accounts for messages with file attachments containing photos taken at a protest or calendar accounts for appointments at the time and place of the protest. Police might ask Apple to search iCloud for any photos or videos taken of an arrest that garnered public attention.

E. People and Object Recognition in Video and Image Surveillance

The world is increasingly awash in cameras, creating a constant stream of still and moving images from public and private spaces, much of it stored or backed up into the cloud. Powerful machine learning algorithms allow this data to be searched, opening the possibility of traditional and reverse searches through this visual chronicle of all of our lives.

Today's digital cameras are used to create billions of new photos and hundreds of thousands of hours of video on a daily basis. T.J. Thomson et. al., *Visual Mis/disinformation in Journalism and Public Communications: Current Verification Practices, Challenges, and Future Opportunities*, 16 Journalism Prac. 938, 940 (2020) (indicating that at least 3.2 billion photos and 720,000 hours of video are created each day). Many of these cameras are handheld or installed in place by private actors. Homeowners place cameras in their doorbells, drivers place them on their car dashboards, parents place them inside nurseries, and nature lovers place them in their bird feeders, to say nothing of the cameras that are part of our cellphones. Commercial buildings install cameras on the corners of structures and in interior hallways. Public actors install cameras as well, from cameras in buses to law enforcement agencies sending cameras aloft on planes and drones. *See, e.g.*, *Leaders of a Beautiful Struggle v. Balt. Police Dep't*, 2

F.4th 330 (4th Cir. 2021) (en banc) (discussing a pervasive aerial surveillance program built and used to track people's movements).

Additionally, many of these images end up stored in data centers and are accessible to corporate cloud providers, as discussed above.

Meanwhile, computer science has rendered all of this imagery searchable. Facial recognition and object identification algorithms have dramatically improved in the last few decades. *See* Pratyusha Ria Kalluri et al., *Computer-Vision Research Powers Surveillance Technology*, 643 Nature 73 (2025) (study of computer vision research paper and patents, and discussing improvements in object recognition that have also been used to improve human-recognition models). When paired with large image datasets—for example, a database of video doorbell recordings—it is not difficult to imagine a reverse search to identify people or other objects across, say, an entire neighborhood. *See* Jennifer Pattison Tuohy, *Ring Cancels Its Partnership with Flock Safety After Surveillance Backlash*, The Verge (Feb. 12, 2026), https://perma.cc/Q25P-YCCC; *see also* Jason Koebler, *Leaked Email Suggests Ring Plans to Expand "Search Party" Surveillance Beyond Dogs*, 404 Media (Feb. 18, 2026), https://perma.cc/KH2P-SXKG.

What could reverse image searching at that scale accomplish? Many photos are time- and location-stamped, and hence can be woven into a digital collage. For example, one might search for all photos that capture a particular location during an interval of time. This could

replicate an ordinary geofence search, but with the possibility of photographically identifying people who were there but did not have a location-tracking device with them.

One could also imagine reverse "association" searches, searches for photos or videos of anyone who was depicted near a person or item of interest. *See generally* Deven R. Desai, *Constitutional Limits on Surveillance: Associational Freedom in the Age of Data Hoarding*, 90 Notre Dame L. Rev. 579 (2014). Rather than asking "who was here during this time" (a geofence query), an association search might ask "who came into contact with this person or knows them?" Such searches would create a chilling effect on whom people chose to associate with and would facilitate guilt by association. Jean Tirole, *Digital Dystopia*, 111 Am. Econ. Rev. 2007 (2021). The latter effects would be multiplied by the use of AI tools for predictive social graphing, which can be used to infer a person's First Amendment-protected decisions to talk to and be with other people. *See* Alicia Solow-Niederman, *Information Privacy and the Inference Economy*, 117 Nw. U. L. Rev. 357 (2022).

Finally, researchers have shown that facial recognition technology, and many other forms of modern machine learning, are plagued with bias. *See, e.g.*, Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 Mach. Learning Rsch. 87 (2018) (finding error rates in three leading gender classification systems of up to 35% for darker

skinned females versus below 1% for lighter-skinned males); Patrick Grother et al., Nat'l Inst. Stds. & Tech., *Internal Rep. 8280, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects* 2–3 (2019), https://perma.cc/6THV-EVQL (reporting as much as 100 times more false positive errors for black face matches compared to white face matches). Powering reverse searches with biased algorithms will place disproportionate burdens on members of minority groups. *See* Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 Minn. L. Rev. 1105 (2021); Clare Garvie & Laura Moy, *America Under Watch: Face Surveillance in the United States*, Geo. Ctr. on Priv. & Tech. (May 16, 2019), https://perma.cc/DG38-HV7A.

F. What Comes Next: Capturing and Commodifying Human Experience

A significant swath of the material wealth and innovative brilliance of the modern American economy is directed at finding untapped repositories of human experience, rendering it into data gathered in the cloud, and analyzing it for the benefit of users and third parties. Some scholars describe our economy as built upon a system of surveillance capitalism. *See* Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (2019). Less-critical industry watchers refer to this as frictionless integration or data liquidity.

Whatever you call it, the result is the same. Companies continue to seek out everything we say and do, everyone we know and meet, and everywhere we go, and turn that information into vast online repositories. These large databases create a substantial risk that the government will dip their dragnets into different streams of deeply personal communications, content, and other evidence of speech, association, belief, and behavior.

In addition to the examples addressed above, consider the next generation of data gathering innovations arriving in your home soon. Each has the potential to generate vast new pools of sensitive information the police might target for their next reverse search. Wearable devices bring internet connectivity, cameras, microphones, and other sensors, to glasses, pendants, and clothing. Petar Radanliev, *Privacy, Ethics, Transparency, and Accountability in AI Systems for Wearable Devices*, Frontiers in Digit. Health (2025) ("Wearable sensors collect a vast amount of personal data, which can be helpful for personal health and productivity. . . . This can lead to invasive targeted advertising, increased insurance premiums based on health data, or even surveillance by governments or companies."). Smartwatches and fitness bands monitor heart rates, motion, sweat, and skin temperature, revealing detailed records of user activity. Kavous Salehzadeh Niksirat et al., *Wearable Activity Trackers: A Survey on Utility, Privacy, and Security*, 56 ACM Comput. Surv. 1, 11–12 (2024) (summarizing

information that can be obtained or inferred from wearable activity trackers, including: mental-health states and disease indicators; specific user activities such as eating, drinking, or smoking; personality traits, mood, and handwriting; and precise user location). And brainwave sensors placed near, or even surgically inside, the brain will soon monitor traces of what we think and how we feel. Patrick Magee et al., *Beyond Neural Data: Cognitive Biometrics and Mental Privacy*, 112 Neuron 3017, 3017 (2024) ("Recent advancements in artificial intelligence . . . have further demonstrated the potential to establish privacy-sensitive statistical correlations between neural data and particular mental states. This capability, while beneficial for personalized health and wellness applications, also poses unique challenges to mental privacy, potentially leading to unwanted surveillance and manipulation if not properly regulated.").

What all of these advances have in common is that they will render suddenly legible the private details of individual lives that have never been externally knowable before, much less stored in the data centers of distant corporations. Courts are sure to struggle even with traditional search requests about some of this data: what was User 24601 saying, listening to, or thinking last Monday at 2pm? Deciding what to do about *reverse* searches of such data—who experienced a sudden increase in heart rate Saturday evening?—will be even more

fraught without strict constitutional guardrails around novel forms of surveillance.

III. Implications

If this Court declares that reverse searches are general searches, it will break the automatic turn-key inheritance law enforcement agencies enjoy for these pools of information.

Even if this Court decides that the warrant used in Mr. Chatrie's case was not a general warrant, it can and should still articulate restrictions on the use of geofence warrants that address their reverse nature. Most fundamentally, this Court should focus on the requirements of particularity and individualized suspicion that are so often at odds with reverse searches. *Ybarra*, 444 U.S. at 91; *Carpenter*, 585 U.S. at 317; *see also Chatrie*, 146 S. Ct. at 2215–16. This requires serious consideration of the rights of the many innocent or completely unrelated third parties who will have their personal information revealed without proper protection or justification when a search like this is conducted. *See, e.g.*, *United States v. Brown*, No. 1:16-cr-427-AT-JKL-31, 2025 WL 1674283, at *16 (N.D. Ga. June 13, 2025). In other words, courts must attend to the false positives—the people who just happened to be in the wrong place at the wrong time, the people who just happened to search for the unlucky phrase, or the person who just happened to say the unfortunate thing to the AI chatbot. Courts must also consider the person who was not even in the wrong place at the

wrong time, but who erroneously appears to have been due to messy data, a noisy GPS chip, or buggy code.

We may be out of practice in this kind of analysis. With more traditional searches, the incidental invasion of the privacy of third parties can be thought justified by the particularity and probable cause supporting the underlying warrant. *See, e.g.*, *Zurcher v. Stanford Daily*, 436 U.S. 547, 559 (1978). But when the warrant at issue is indiscriminate by its nature, third-party privacy is put directly at issue by the government's search strategy and must be protected more aggressively. *E.g.*, *In re Search of Info. that Is Stored at Premises Controlled by Google LLC*, 579 F. Supp. 3d 62, 82–85 (D.D.C. 2021) (carefully analyzing the effect on a geofence search on third parties); *see also Zurcher*, 436 U.S. at 560 (indicating traditional searches may be unreasonable even if they are "supported by a warrant issued on probable cause and properly identifying the place to be searched and the property to be seized").

Beyond strictly policing particularity and individualized suspicion, there are other safeguards courts can impose during the warrant process to protect privacy and limit police power. A key lesson of *Berger v. New York* is that the constitutional requirements of particularity and probable cause can sometimes only be met by reaching into a broader judicial toolkit. 388 U.S. at 55–60. When a novel technological threat, "[b]y its very nature . . . involves an intrusion on privacy that is broad

in scope," *id.* at 56, it "imposes 'a heavier responsibility on this Court in its supervision of the fairness of procedures.'" *Id.* (quoting *Osborn v. United States*, 385 U.S. 323, 329 n.7 (1966)); *see also* Susan Freiwald & Paul Ohm, *Superwarrants*, 68 Ariz. L. Rev. 359 (2026). When the novel technological threat to privacy was voice wiretaps, the Supreme Court endorsed protections such as time limits, expiry dates, and limits on the number of renewals. *Berger*, 388 U.S. at 59.

In crafting "adequate judicial supervision or protective procedures," *id.* at 60, to address reverse searches, it should keep in mind the many forms that such searches take.

One measured and sensible limit would be to impose the requirement of necessity, so that invasive dragnet powers should be exercised only as last resorts. The government should not be permitted to turn to geofence queries, or other reverse searches, unless and until they have tried to use other, less invasive investigative steps that failed to solve the crime. *Cf.* 18 U.S.C. § 2518(3)(c) (requiring proof that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous" to obtain a wiretap order); *United States v. Torres*, 751 F.2d 875, 884 (7th Cir. 1984) (requiring similar proof under the Fourth Amendment for conducting video surveillance not covered by the Wiretap Act).

This Court should also consider limiting geofence queries to serious crimes rather than trivial ones. *In re Search of Info. Stored at Premises Controlled by Google, as Further Described in Attachment A*, No. 20-mc-297, 2020 WL 5491763, at *8 (N.D. Ill. July 8, 2020) ("The government's undisciplined and overuse of this investigative technique in run-of-the-mill cases that present no urgency or imminent danger poses concerns to our collective sense of privacy and trust in law enforcement officials.").

Finally, in ruling on the substantive questions in this case, this Court should signal how the reasoning applies to other types of reverse warrants. Otherwise, courts in this Circuit will likely rely on the good faith exception for each new kind of reverse search that emerges because their "legality . . . [is] unclear." *United States v. Chatrie*, 590 F. Supp. 3d 901, 937 (E.D. Va. 2022), *aff'd*, 107 F.4th 319 (4th Cir. 2024), *on reh'g en banc*, 136 F.4th 100 (4th Cir. 2025), *vacated and remanded*, 146 S. Ct. 2193 (2026) (quoting *United States v. McLamb*, 880 F.3d 685, 691 (4th Cir. 2018)). Numerous courts have refused to suppress geofence warrants on the grounds that the search technology is novel, and hence mistakes in its use should be excused and should not trigger suppression. *See, e.g.*, *id.* at 936–41; *United States v. Smith*, 110 F.4th 817, 838–40 (5th Cir. 2024), *cert. denied*, 146 S. Ct. 356 (2025).

CONCLUSION

For the foregoing reasons, *amici* respectfully urge this Court to reverse the denial of Mr. Chatrie's motion to suppress.

Respectfully submitted,

Dated: September 8, 2026

/s/ *Megan Graham*

Megan Graham
Clinical Law Programs
University of Iowa College of Law
380 Boyd Law Building
Iowa City, Iowa 52242
(319) 335-9023
megan-k-graham@uiowa.edu

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(g), I certify as follows:

1. This brief complies with the type-volume limitation of Fed. R. App. P. 32(a) and Fed. R. App. P. 29(a)(5) because this brief contains 6,315 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type-style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 365 in 14-point font in Century Schoolbook.

/s/ *Megan Graham*

Megan Graham
Clinical Law Programs
University of Iowa College of Law
380 Boyd Law Building
Iowa City, Iowa 52242
319) 335-9023
megan-k-graham@uiowa.edu

Counsel for Amici Curiae