# EVERYTHING-EVERYWHERE SEARCHES AND THE GEOFENCE PUZZLE

ANDREW GUTHRIE FERGUSON[†]

## ABSTRACT

*Police surveillance technologies have outpaced the Fourth Amendment doctrine. Arbitrary, generalized search powers stretching across entire cities and states now exist in forms that have no historical analog. Police can now search "everything everywhere all at once" and current Fourth Amendment doctrine has little to say about the resulting privacy and security threats.*

*This Symposium Essay addresses the "everything-everywhere" search problem with two goals in mind. First, it seeks to identify the technological and doctrinal problems of this type of AI-enhanced surveillance power. Policing technologies that arbitrarily rummage through vast streams of data for suspicious activities raise new and distinct Fourth Amendment concerns upending the traditional threshold search analysis.*

*The second goal of this Essay is to offer a new analytical lens to reframe everything-everywhere searches, focusing on the harm of rummaging. My argument, in brief, is that the Fourth Amendment was designed to protect against overbroad, generalized rummaging power. While the act of physically searching homes and papers was of obvious concern, the power to conduct the search – i.e., general warrants and the writs of assistance – was of paramount concern. Grants of unreasonable rummaging power to government agents raise this rummaging concern. This piece notes that everything-everywhere surveillance technologies (or laws granting such surveillance powers) need to be judged against the rummaging principle, which examines arbitrariness, overreach, intrusions on constitutionally protected interests, and threats of exposure. As will be explained, this rummaging principle helps clarify both the threshold search question and the resulting harm left unaddressed under the reasonable expectation of privacy test and our existing warrant practice.*

*After setting out the technological and constitutional problems of everything-everywhere surveillance, I will apply my digital rummaging analysis to the specific problem of geofence requests and geofence warrants. Geofence investigations offer a fascinating test case for the everything-everywhere-policing-problem, and the digital rummaging theory provides the solution to this hard Fourth Amendment puzzle.*

---

[†] Professor of Law, George Washington University Law School. Thank you to the editors of the George Washington Journal of Law & Technology Symposium for the invitation to contribute to its inaugural symposium.

# TABLE OF CONTENTS

## INTRODUCTION

Police surveillance technologies have outpaced Fourth Amendment doctrine. Arbitrary, generalized search powers stretching across entire cities and states now exist in forms that have no historical analog.[1] Today, thousands of networked surveillance cameras powered by video analytics can identify and record objects on city streets.[2] Today, New York State can track cars traveling on public roads, limited only by its investment in automated license plate readers (ALPRs).[3] Until recently, if police wanted to find a specific smartphone, they could use a warrant to obtain the locational data of any person with a Google-enabled app or phone from millions of such phones.[4] By following a geofence protocol, investigating agents could search the entire Google dataset for a particular phone at a particular place and time.[5]

While many scholars foretold the dangers of data-driven surveillance,[6] only recently have the threats been fully realized with the combination of artificial intelligence (AI) and almost infinite digital storage capacities.[7] Police can now search "everything everywhere all at once"[8] and current Fourth Amendment doctrine has little to say about the resulting privacy and security threats.[9] In an odd doctrinal consequence, by searching everyone and everything at the same time, police can elide the traditional threshold search and seizure questions because it is not clear what expectations anyone has under such continuous surveillance, or even when the search occurs.[10] And, with a judicial warrant, our digital trails are fair game for investigators, even if the initial

---

[1] *See, e.g.*, Andrew Guthrie Ferguson, *Persistent Surveillance*, 74 ALA. L. REV. 1, 5 (2022).

[2] Zac Larkman, *The Quiet Rise of Real-Time Crime Centers*, WIRED (July 28, 2023), https://www.wired.com/story/real-time-crime-centers-rtcc-us-police/ [https://perma.cc/NX9J-P6NB]; Jahd Khalil, *Real Time Crime Centers, Which Started in Bigger Cities, Spread Across the U.S.*, NPR (Aug. 16, 2023, at 5:10 ET), https://www.npr.org/2023/08/16/1194115202/real-time-crime-centers-which-started-in-bigger-cities-spread-across-the-u-s [https://perma.cc/J28W-HAGF] (estimating the current number of RTCCs at 135 and growing).

[3] Thomas Brewster, *This AI Watches Millions of Cars Daily and Tells Cops if You're Driving Like a Criminal*, FORBES (Aug. 16, 2023, at 6:30 ET), https://www.forbes.com/sites/thomasbrewster/2023/07/17/license-plate-reader-ai-criminal/ [https://perma.cc/RYN8-9J2V].

[4] United States v. Chatrie, 590 F. Supp. 3d 901, 907 (E.D. Va. 2022), *aff'd*, 107 F.4th 319 (4th Cir. 2024) (describing the use of a geofence warrant); United States v. Chatrie, 136 F.4th 100 (4th Cir. 2025) (*en banc*).

[5] Brian L. Owsley, *The Best Offense is a Good Defense: Fourth Amendment Implications of Geofence Warrants*, 50 HOFSTRA L. REV. 829, 831 (2022). As will be discussed, the geofence warrant process has been altered by Google's internal corporate policies which stopped collecting locational data through the Sensorvault. *See infra* note 60.

[6] *See, e.g.*, Barry Friedman & Danielle Keats Citron, *Indiscriminate Data Surveillance*, 110 VA. L. REV. 1351, 1363 (2024); Woodrow Hartzog, Evan Selinger & Johanna Gunawan, *Privacy Nicks: How the Law Normalizes Surveillance*, 101 WASH. U. L. REV. 717, 775 (2024); Kate Weisburd, *Punitive Surveillance*, 108 VA. L. REV. 147, 153 (2022); Chaz Arnett, *Race, Surveillance, Resistance*, 81 OHIO ST. L.J. 1103, 1116 (2020); Ngozi Okidegbe, *When They Hear Us: Race, Algorithms and the Practice of Criminal Law*, KAN. J.L. & PUB. POL'Y, Summer 2020, at 329, 334; Lindsey Barrett, *Model(ing) Privacy: Empirical Approaches to Privacy Law & Governance*, 35 SANTA CLARA HIGH TECH. L.J. 1, 27 (2018); Ifeoma Ajunwa, Kate Crawford & Jason Schultz, *Limitless Worker Surveillance*, 105 CALIF. L. REV. 735, 740 (2017); BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 13–87 (2015); David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 95 (2013); Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1339 (2012); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1138 (2002).

[7] *See, e.g.*, ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT 16 (2017); Sarah Brayne, *Big Data Surveillance: The Case of Policing*, 82 AM. SOCIO. REV. 977, 985 (2017).

[8] *Everything Everywhere All at Once*, IMDB, https://www.imdb.com/title/tt6710474 [https://perma.cc/62FK-WZMK]; *see also* Jennifer Pattison Tuohy, *Ring's Car Cam Is for Those Who Want to Record Everything Everywhere All at Once*, THE VERGE (Feb. 15, 2023, at 15:19 ET), https://www.theverge.com/2023/2/15/23600450/ring-car-cam-review-amazon-security-dash-cam [https://perma.cc/P2R4-VS85].

[9] Dan Solove, *Privacy in Authoritarian Times: Surveillance Capitalism and Government Surveillance*, 67 B.C. L. REV. 51 (2026); Matthew Tokson, *Artificial Intelligence and the Anti-Authoritarian Fourth Amendment*, 27 PENN. J. CONST. L. 1067, 1072 (2025).

[10] *See* Barry Friedman, *Lawless Surveillance*, 97 N.Y.U. L. REV. 1143, 1166 (2022); Barry Friedman & Danielle Keats Citron, *Constitutionality of Indiscriminate Surveillance*, 110 VA. L. REV. 1351 (2024).

search runs against everyone.

This Symposium Essay addresses the "everything-everywhere" search problem with two goals in mind. First, it seeks to identify the technological and doctrinal problems of this type of AI-enhanced surveillance power.[11] Policing technologies that arbitrarily rummage through vast streams of data for suspicious activities raise new and distinct Fourth Amendment concerns upending the traditional threshold search analysis.[12] When everything is continuously being searched, nothing is a "search" for Fourth Amendment purposes.[13] In addition, privacy and security harms exist even with a judicial warrant.[14] While it is true that a judicial warrant offers a form of particularized cabining within a broad collection of data, the reality is that for many particularized warrant-based searches to work, a generalized non-warrant-based collection of data must have already occurred.[15] As will be discussed, to "search" in a Fourth Amendment sense to find data *with* a warrant, one must have already "searched" in a literal sense to collect data *without* a warrant, and that initial warrantless collection creates the constitutional problem.[16]

The second goal of this Essay is to offer a new analytical lens to reframe everything-everywhere searches, focusing on the harm of rummaging.[17] Current Fourth Amendment doctrine focuses on "reasonable expectations of privacy"[18] and "particularized"[19] warrants, failing to address the harms of more ubiquitous and persistent surveillances technologies. Two related questions emerge at this intersection of new surveillance power and old constitutional law. First, when does the search occur when everything is always being surveilled? Second, what is the harm in this type of everything-everywhere surveillance? As will be detailed in Part I.B., current Fourth Amendment doctrine provides little clarity to these questions in the context of AI surveillance. My answer in this Essay centers around the concept of digital rummaging.[20] In prior work, I have offered the "rummaging principle" as a new way to see the Fourth Amendment in the digital age.[21]

My argument, in brief, is that the Fourth Amendment was designed to protect against a type of overbroad, generalized rummaging power. While the act of physically searching homes and papers was of obvious concern, *the power* to conduct the search – i.e., general warrants and the writs of assistance – was of paramount concern.[22] Grants of unreasonable rummaging power

---

[11] Sheila Dang, *AI Explosion Merits Regulation to Rein in Threats, Experts Say*, REUTERS (July 12, 2023, at 21:55 ET), https://www.reuters.com/technology/reuters-momentum-ai-explosion-merits-regulation-rein-threats-experts-say-2023-07-12/ [https://perma.cc/SW5B-JDRY].

[12] *See infra* Part II.

[13] *Id*.

[14] Miguel F.P. de Figueiredo, Brett Hashimoto, & Dane Thorley, *Unwarranted Warrants? An Empirical Analysis of Judicial Review in Search and Seizure*, 138 HARV. L. REV. 1959, 1963 (2025).

[15] Carpenter v. United States, 585 U.S. 296, 301–02 (2018).

[16] *See infra* Part I.

[17] Andrew Guthrie Ferguson, *Digital Rummaging*, 101 WASH. U.L. REV. 1473, 1476 (2024).

[18] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[19] Andresen v. Maryland, 427 U.S. 463, 480 (1976) (discussing warrant particularity).

[20] Ferguson, *supra* note 17, at 1476.

[21] *Id*. at 1509.

[22] *Id*. at 1476 ("Rummaging–and the fear of government agents abusing their search powers–can be traced from the Founding debates around the Writs of Assistance and General Warrants to modern cases involving digital technologies.").

to government agents raise this rummaging concern.[23] My argument here is that everything-everywhere surveillance technologies (or laws granting such surveillance powers) need to be judged against the rummaging principle that examines arbitrariness, overreach, intrusions on constitutionally protected interests, and threats of exposure.[24] As will be explained, this rummaging principle helps clarify both the threshold search question and the resulting harms left unaddressed under the reasonable expectation of privacy test and our existing warrant practice.

After setting out the technological and constitutional problems of everything-everywhere surveillance, I will apply my digital rummaging analysis to the specific problem of geofence requests.[25] Geofence requests offer a fascinating test case for the everything-everywhere-policing-problem. Geofence requests involve law enforcement demands for geolocation data from third-party providers like Google, Fog Data Science, or other geolocation data collectors.[26] The search runs to anyone with a digitally-connected device all across the United States.[27] The geofence debate has created a (yet unresolved) split between the United States Court of Appeals for the Fifth Circuit[28] and the United States Court of Appeals for the Fourth Circuit.[29] In January 2026, the Supreme Court granted certiorari in the Fourth Circuit's case, *United States v. Chatrie*.[30]

This Symposium Essay will use the geofence debate as a proxy for technological and doctrinal questions arising from everything-everywhere searches. As will be discussed, the federal courts have differed in how to approach the collect-everything technological future and have offered an unsatisfying Fourth Amendment response. [31] This Essay then offers a way forward. In applying the rummaging principle to the problem of geofence requests, a new framework for analyzing everything-everywhere searches emerges.

## I. THE PROBLEM OF EVERYTHING-EVERYWHERE-ALL-AT-ONCE SEARCHES

This Part examines the technological and legal challenges brought about by new everything-everywhere surveillance technologies. The first section examines the practical reality of everything-everywhere surveillance and how it reshapes police power. The second section examines how the existing Fourth Amendment doctrine fails to meet this technological challenge.

---

[23] *Id*. at 1478 ("The goal of this Article is to refocus attention on the government's power to rummage through personal data.").

[24] These terms will be discussed in detail *infra* Part II.

[25] Haley Amster & Brett Diehl, *Against Geofences*, 74 STAN. L. REV. 385, 394 (2022).

[26] *Id*. *See also* Bennett Cyphers & Aaron Mackey, *Fog Data Science Puts Our Fourth Amendment Rights Up for Sale,* ELEC. FRONTIER FOUND. (Aug. 31, 2022), https://www.eff.org/deeplinks/2022/08/fog-data-science-puts-our-fourth-amendment-rights-sale [https://perma.cc/HZ6W-V5XN]; Matthew Guariglia, *What is Fog Data Science? Why is the Surveillance Company so Dangerous?*, ELEC. FRONTIER FOUND. (Aug. 31, 2022), https://www.eff.org/deeplinks/2022/06/what-fog-data-science-why-surveillance-company-so-dangerous [https://perma.cc/53T4-J5NN]; Rachel Silver, *A Miscarriage of Justice: How Femtech Apps and Fog Data Evade Fourth Amendment Privacy Protections*, 30 WASH. & LEE J. CIVIL RTS. & SOC. JUST. 141, 159 (2023).

[27] Cyphers & Mackey, *supra* note 26.

[28] United States v. Chatrie, 107 F.4th 319, 322 (4th Cir. 2024), *reh'g en banc granted*, No. 22-4489, 2024 WL 4648102 (4th Cir. Nov. 1, 2024); United States v. Chatrie, 590 F. Supp. 3d 901, 908 (E.D. Va. 2022), *aff'd*, 107 F.4th 319 (4th Cir. 2024).

[29] United States v. Smith, 110 F.4th 817, 821 (5th Cir. 2024).

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

[31] As of the date of the symposium in February 2025, the Fifth Circuit had denied *en banc* review, and the Fourth Circuit was considering the case *en banc*. As will be discussed *infra*, the *en banc* Fourth Circuit did not resolve the Fourth Amendment questions. *See* United States v. Chatrie, 136 F.4th 100 (4th Cir. 2025) (*en banc*) and the United States Supreme Court granted certiorari in January 2026.

Conceptions of reasonable expectations of privacy in public and particularized warrants within overbroad collection systems miss the mark about what is happening with new forms of mass surveillance.[32] The third section introduces the geofence request problem as an illustrative example of how the existing Fourth Amendment doctrine fails to grasp the harms of everything-everywhere searches. This section examines how neither side of the debate gets the analysis exactly right. Part II will then apply the rummaging principle to the questions developed in these sections.

### *A. Everything-Everywhere Surveillance: A New Technological Problem*

Police have always conducted surveillance. Yet, modern digital policing offers an exponential advancement in terms of scale, scope, and scalability.[33] While the technologies might look superficially similar, they are not. This subsection briefly details how AI-surveillance enhancements alter police power and personal privacy.

As one example, in an analog world, a human police officer might use a video camera to record a city street. Today, in cities with sophisticated Real-Time Crime Centers, thousands, if not tens of thousands of cameras watch an equal number of streets.[34] In New York City, New Orleans, Louisiana, Chicago, Illinois and dozens of smaller cities, camera systems are centralizing public and private camera feeds into central command centers.[35] Overlaying those video streams are video analytics hardware and software that can turn digital video networks into a tracking technology.[36] Object recognition, trained by AI models, can identify any "thing" (man, woman, dog, car, van, red hat, backpack, etc.) across the city and trace its path back to its starting point.[37] Police departments using video cameras conduct virtual patrols across the feeds and initiate retrospective investigations on the images captured across this growing network of private and public cameras.[38] AI can also identify "anomalies" and redirect police patrols to investigate unusual patterns of

---

[32] *See* Ferguson, *supra* note 17, at 1476, 1509.

[33] Friedman & Citron, *supra* note 6, at 1363; Andrew Guthrie Ferguson, *Why Digital Policing Is Different*, 83 OHIO ST. L.J. 817, 843 (2022).

[34] Keely Quinlan, *Police Real-Time Crime Centers Are Becoming Data Powerhouses*, STATE SCOOP (Aug. 24, 2023) https://statescoop.com/real-time-crime-centers-police-privacy/ [https://perma.cc/9K64-ZENW]; Timothy Williams, *Can 30,000 Cameras Help Solve Chicago's Crime Problem?*, N.Y. TIMES (May 26, 2018) https://www.nytimes.com/2018/05/26/us/chicago-police-surveillance.html [https://perma.cc/G7A5-BBBG]; JOHN S. HOLLYWOOD ET AL., USING VIDEO ANALYTICS AND SENSOR FUSION IN LAW ENFORCEMENT 4 (2018).

[35] Olivia J. Greer, *No Cause of Action: Video Surveillance in New York City*, 18 MICH. TELECOMM. & TECH. L. REV. 589, 596 (2012) ("The term 'real-time video analytics' refers to a programmable network, which can be built to recognize and flag–in real-time–scenarios such as abandoned packages in the subway."); Jake Shore, *What to Know: New Savannah Police Technology Can ID Suspects by Clothes, License Plates*, GEORGIA PUB. BROAD. (Oct. 27. 2022, at 9:47 ET), https://www.gpb.org/news/2022/10/27/what-know-new-savannah-police-technology-can-id-suspects-by-clothes-license-plates [https://perma.cc/X866-ATZZ] ("[Briefcam's] video analytics program is employed by several police departments in cities across the country, including Hartford, C.T., Beverly Hills, C.A., Chicago, Detroit and New Orleans. Airports and "smart cities" are also listed as BriefCam customers.").

[36] *Video Analytics Fundamentals Guide*, INDEP. INTEL. FOR PHYSICAL SEC. (Mar. 04, 2021, at 11:00 ET), https://ipvm.com/reports/analytics-fundamentals; JAY STANLEY, ACLU, *The Dawn of Robot Surveillance: AI, Video Analytics, and Privacy*, 3–9 (2019).

[37] Dave Maass & Matthew Guariglia, *Video Analytics User Manuals Are a Guide to Dystopia*, ELEC. FRONTIER FOUND. (Nov. 19, 2020), https://www.eff.org/deeplinks/2020/11/video-analytics-user-manuals-are-guide-dystopia [https://perma.cc/3LY6-BK5Z] ("BriefCam sorts people and objects into specific categories to make them easier for the system to search for. BriefCam breaks people into the three categories of 'man,' 'woman,' and 'child.'").

[38] Avi Asher-Schapiro, *Privacy or Safety? U.S. Brings Surveillance City to the Suburbs*, THOMPSON-REUTERS, (May 11, 2023) https://www.reuters.com/article/technology/privacy-or-safety-us-brings-surveillance-city-to-the-suburbs-idUSL8N35O0IE/ [https://perma.cc/2ZGK-NUYP].

activity.[39] Everything in the city is being recorded, stored, and analyzed through these camera systems. This is an everything-everywhere technology only limited by the numbers of cameras and the digital storage capacity in the Real-Time Crime Center.

Another example of everything-everywhere surveillance is automated license plate readers (ALPRs).[40] In an analog world, police would patrol the streets with a list of stolen cars, detailing make, model, and license plate number. If they observed a "hot" car, they could make a stop to investigate the matter.[41] Today, automated license plate readers positioned on police cars, streetlights, stationary poles, and toll booths record millions and millions of license plates a year.[42] An ALPR attached to a police car can scan thousands of license plates a minute with the location and photograph of each car stored in a database for years.[43] AI software can be run on the patterns to identify suspicious activities.[44] In New York State, for example, David Zayas was arrested because the ALPR algorithm flagged his travels from Massachusetts to New York as indicative of drug trafficking (and the predictive hunch turned out to be correct).[45] City or state cameras have been augmented by private companies like Flock Safety that sell ALPR technology to homeowners' associations, counties, and private communities.[46] The collected database which includes license plate number, time, date, location, and a photograph of the car (and anyone near it) grows every minute and runs against anyone with a car in public.[47]

Almost all new automobiles are sold with tracking capabilities.[48] In an analog world, police might have had to stake out a suspicious car and surreptitiously tail it as part of a criminal investigation.[49] Today, in a world of smart, connected cars, cars are sold with GPS enabled service

---

[39] Nirja Chokshi, *How Surveillance Cameras Could be Weaponized with AI*, N.Y. TIMES (June 13, 2019), https://www.nytimes.com/2019/06/13/us/aclu-surveillance-artificial-intelligence.html [] ("Advancements in artificial intelligence could supercharge surveillance, allowing camera owners to identify 'unusual' behavior, recognize actions like hugging or kissing, easily seek out embarrassing footage and estimate a person's age or, possibly, even their disposition.").

[40] *See* Commonwealth v. McCarthy, 142 N.E.3d 1090, 1095 (Mass. 2020); Yash Dattani, *Big Brother is Scanning: The Widespread Implementation of ALPR Technology in America's Police Forces*, 24(4) VAND. J. ENT. & TECH. L. 749, 758 (2022).

[41] John L. Bellah, *Car of the Week: 1964 Plymouth Savoy Police Car*, OLD CARS WEEKLY (July 16, 2019, at 2:43 PT), https://www.oldcarsweekly.com/features/car-of-the-week-1964-plymouth-savoy-police-car [https://perma.cc/976M-ZWN5] (explaining the hot-sheets used before ALPR technology).

[42] *Automated License Plate Readers: Street-Level Surveillance*, ELEC. FRONTIER FOUND., https://www.eff.org/pages/automated-license-plate-readers-alpr [https://perma.cc/E5WS-MB36] ("ALPRs are high-speed, computer-controlled camera systems that are typically mounted on street poles, streetlights, highway overpasses, mobile trailers, or attached to police squad cars.").

[43] Maneka Sinha, *The Automated Fourth Amendment*, 73 EMORY L.J. 589, 609 (2024) ("ALPRs use high-speed cameras mounted on police vehicles or stationary structures to automatically take pictures of thousands of license plates a minute. Photographs of the license plate and car, along with information about when and where a license plate was observed, are stored in databases.").

[44] Will Nesbit, *A Matter of Time: Artificial Intelligence, the Fourth Amendment, and Changing Privacy Expectations*, 73 AM. U.L. REV. F. 237, 247 (2024) ("Westchester County Police Department (Westchester PD) uses a network of 480 automated license plate reader (ALPR) cameras across various roads and highways throughout the county to collect and store over 16 million license plate reads per week.").

[45] Brewster, *supra* note 3.

[46] Louise Matsakis, *Flock Safety Says Its License Plate Readers Reduce Crime. It's Not That Simple*, WIRED (Oct. 24, 2019, at 12:00 ET), https://www.wired.com/story/flock-safety-license-plate-readers-crime/ [https://perma.cc/9VEQ-LZZ2].

[47] *Id.*

[48] Anthony Gordon, *Every New Car is a 'Privacy Nightmare,' Mozilla Researchers Conclude*, VICE (Sep. 6, 2023, at 10:19 ET), https://www.vice.com/en/article/every-new-car-is-a-privacy-nightmare-mozilla-researchers-conclude/ [https://perma.cc/38N8-9P6B]; Thomas Germain, *If You've Got a New Car, It's a Data Privacy Nightmare*, GIZMODO, (Sep. 7, 2023), https://web.archive.org/web/20230906030203/https://gizmodo.com/mozilla-new-cars-data-privacy-report-1850805416#expand.

[49] *See* GREENWOOD ET AL., THE CRIMINAL INVESTIGATION PROCESS VOLUME III: OBSERVATIONS & ANALYSIS 25 (1975).

automatically turned on.[50] Whether it is a mapping function, connected WiFi, or some entertainment system, the car is being tracked by the car company and other third-party vendors (like insurance companies) everywhere it travels.[51] It is why you can call for emergency assistance with a push of a button or follow a digital map home.[52] If the police wish to find a particular car within a state, the car company and several other consumer data collection companies all have the answer.[53] The smart cars have already been tracked.[54] The data exists.[55] All police need to do is request it via a subpoena or warrant.[56]

Cars are only one of the smart devices that reveal our paths, and at least cars do not follow us into our homes or offices.[57] Our smartphones do.[58] In an analog world, individuals might go about their lives unburdened by being tracked (absent unusual circumstances).[59] For centuries, people would go to work, school, church, stores, bars, restaurants, gyms, doctors' appointments, legal appointments, and such without anyone having access to their travels. Their paths and patterns were not secret, but nor were they accessible to police by a quick search query. Today, smartphones that we carry on our errands reveal location, interests, and associations. Third party companies collect the location data as part of business models to sell consumer goods or advertising to individuals.[60] This locational data can be shared with law enforcement.[61] Some companies have designed portals specifically for police to use the locational data for police

---

[50] *See generally* Adam M. Gershowitz, *The Tesla Meets the Fourth Amendment*, 48 B.Y.U. L. REV. 1135, 1139 (2023); Matt Burgess, *How Your New Car Tracks You*, WIRED (June 21, 2023, at 7:00 ET), https://www.wired.com/story/car-data-privacy-toyota-honda-ford/ [https://perma.cc/8Y8X-FQSB]; Jack Morse, *Your Car Knows Too Much About You. That Could Be A Privacy Nightmare*, MASHABLE (Sep. 18, 2021), https://mashable.com/article/privacy-please-what-data-do-modern-cars-collect [https://perma.cc/G2LL-WZ48].

[51] *See* Jen Caltrider et al., *It's Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy*, MOZILLA (Sep. 6, 2023), https://www.mozillafoundation.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/ [https://perma.cc/4C3R-JJGN]; '*Privacy Nightmare on Wheels': Every Car Brand Reviewed By Mozilla —Including Ford, Volkswagen and Toyota—Flunks Privacy Test*, MOZILLA (Sep. 6, 2023), https://www.mozillafoundation.org/en/blog/privacy-nightmare-on-wheels-every-car-brand-reviewed-by-mozilla-including-ford-volkswagen-and-toyota-flunks-privacy-test/ [https://perma.cc/64Q3-R4QG]; *See also* Kashmir Hill, *Automakers Are Sharing Consumers' Driving Behavior with Insurance Companies*, N.Y. TIMES (Mar. 13, 2024), https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html [https://perma.cc/2Q6A-GPRG].

[52] Burgess, *supra* note 50.

[53] *See also* Hill, *supra* note 51.

[54] *Id.*

[55] *Id.*; *but see FTC Takes Action Against General Motors for Sharing Drivers' Precise Location and Driving Behavior Data Without Consent*, FED. TRADE COMM'N (Jan. 16, 2025), https://www.ftc.gov/news-events/news/2025/01/ftc-takes-action-against-general-motors-sharing-drivers-precise-location-driving-behavior-data [https://perma.cc/6586-2EP5].

[56] Sam Biddle, *Your Car is Spying on You and a CBP Contract Show the Risks*, THE INTERCEPT (May 3, 2021), https://theintercept.com/2021/05/03/car-surveillance-berla-msab-cbp/ [https://perma.cc/2BUJ-EY8Q].

[57] Herbert B. Dixon, *Your Cell Phone is a Spy*, AMER. BAR. ASSN. (July 29, 2020); Cullen Seltzer, *Google Knows Where You've Been. Should It Tell the Police?*, SLATE (May 16, 2022, at 11:04 ET), https://slate.com/technology/2022/05/google-geofence-warrants-chatrie-location-tracking.html [https://perma.cc/7S4P-K3CK].

[58] *Id*.

[59] Solove, *supra* note 6, at 1090 (identifying the conflation of privacy and secrecy in Fourth Amendment doctrine).

[60] Ryan Nakashima, *Google Tracks Your Movements, Like It or Not*, ASSOCIATED PRESS (Aug. 13, 2018, at 18:15 ET), https://apnews.com/article/828aefab64d4411bac257a07c1af0ecb [https://perma.cc/4M33-NCJ6]; Ryan Nakashima, *Google Clarifies Location-Tracking Policy*, ASSOCIATED PRESS (Aug. 16, 2018, at 20:09 ET), https://apnews.com/article/ef95c6a91eeb4d8e9dda9cad887bf211 [https://perma.cc/5QF2-5ESP]; Zach Whittaker, *Google Moves to End Geofence Warrants. A Surveillance Problem It Largely Created*, TECH CRUNCH (Dec. 16, 2023, at 8:30 PT), https://techcrunch.com/2023/12/16/google-geofence-warrants-law-enforcement-privacy/ [https://perma.cc/Q7SW-UFVW].

[61] Ramon Padilla & Javier Zarracina, *How Police Work With Google to Obtain Cellphone Location Data for Criminal Investigations*, USA TODAY (Sep. 8, 2022, at 11:58 ET) [https://perma.cc/SKA4-RJ3Q].

investigations.[62] The result is that everyone's phone already has been tracked.

The technologies that shape the everything-everywhere-all-at-once problem share three commonalities. First, they are pervasive, capturing information across a network, a city, or state. Whether through sensors, video streams, cell site location data, the capture of information is widespread, comprehensive, and voluminous. Second, the technologies are digital, allowing for large scale storage and search capabilities. This recall capability includes the ability to search back in time, aggregate the data, and connect personal data points for new insights. Third, these technologies collect information constantly against everyone, innocent, guilty, or anywhere in between. The technologies, of course, differ in the types of information they capture, how they can be accessed, and even who controls the capture (private parties or the government), but their similarities allow analytical work to be done.

In prior work, I have made the argument that digital policing is different enough that it needs to be thought of separately from analog policing technologies.[63] In simple terms, the act of surveillance is different, the result of the surveillance is different, and the scale and scalability of the surveillance are different.[64] More specifically, six factors distinguish digital persistent surveillance from traditional human policing and analog surveillance: (1) automation, (2) acceleration, (3) accuracy, (4) accumulation, (5) aggregation, and (6) actualization of data.[65] As will be discussed, these technical differences have doctrinal effect, because they provide arguments for why old-fashioned, analog cases should not control questions about the digital future.

More relevantly, here, the factors apply to everything-everywhere technologies like video analytics, ALPR, or geolocational tracking services. What police are doing, what information they are collecting, and how they can use the information needs to be seen as a different analytical problem than the analog surveillance that gave rise to our existing Fourth Amendment precedent. In several prior articles, I have detailed how technologies like facial recognition,[66] networked cameras,[67] video analytics,[68] smart city sensors,[69] IoT devices,[70] persistent surveillance planes,[71] and long-term pole cameras[72] distort the existing Fourth Amendment framework and require new thinking. For purposes of this Essay, I will simply state that the everything-everywhere policing

---

[62] Will Greenberg, *Fog Revealed, A Guided Tour of How Cops Can Browse Your Location Data*, ELEC. FRONTIER FOUND. (Aug. 31, 2022), https://www.eff.org/deeplinks/2022/08/fog-revealed-guided-tour-how-cops-can-browse-your-location-data [https://perma.cc/8M4A-JT34].

[63] Ferguson, *supra* note 33, at 843.

[64] *Id*.

[65] Ferguson, *supra* note 1, at 16 ("Because all digital persistent surveillance technologies involve increased (1) automation, (2) acceleration, (3) accuracy, (4) accumulation, (5) aggregation, and (6) actualization of data, the resulting surveillance capacity is in fact different from the traditional analog equivalent.").

[66] Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105, 1141 (2021).

[67] *Id*. at 1116.

[68] Andrew Guthrie Ferguson, *Video Analytics and Fourth Amendment Vision*, 103 TEX. L. REV. 1253, 1292 (2025).

[69] Andrew Guthrie Ferguson, *Structural Sensor Surveillance*, 106 IOWA L. REV. 47, 70 (2020).

[70] Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547, 554 (2017).

[71] Ferguson, *supra* note 1, at 44.

[72] *Id*.

problem offers a similar technological challenge that requires a new doctrinal approach.

### *B. Everything-Everywhere Surveillance and Old Law*

The Fourth Amendment needs a digital update. At a very basic level, the cases that make up the Fourth Amendment search canon are informed by antiquated, analog technology.[73] As any Criminal Procedure professor knows, teaching the seminal Fourth Amendment search cases also involves explaining to students about coin-operated phone booths,[74] reel-to-reel tape recorders,[75] limited-range radio frequency beepers,[76] microfilm,[77] landline telephones,[78] and basic thermal imaging devices.[79] In a world of globally networked data streams, AI models, and quantum computing, these explanations make old professors seem ancient.[80]

More practically, the analog surveillance at issue involved one-off technologies that were limited in power, scale, and scope. They were necessarily particularized because as a technical matter the technology could not capture more data. The tape recorder in *Katz* could only capture one conversation at a time.[81] The beeper in *Karo* could only follow one car.[82] The pen register in *Smith* was monitoring one landline telephone line.[83] They were one-thing-one-place technologies because they just did not have the capacity for anything more. In addition, because they were not digital, the information could not be easily aggregated or searched retrospectively. Talking about an expectation of privacy from a single tape recorder device that had to be manually turned on and off by investigating agents, is not analogous to city-wide digital audio sensors always listening. Talking about a single beeper that required officers to follow behind the device so not to lose contact is not analogous to a nationwide global tracking system via a combination of GPS, WiFi, Bluetooth, and other communications connecting points that track everyone continuously.

---

[73] As will be discussed, the technologies arose in an era before widespread adoption of digital technology.

[74] Katz v. United States, 389 U.S. 347, 353 (1967); Brief for Petitioner at 5, *Katz*, 389 U.S. 347 (No. 35) ("Petitioner's conversation was overheard and recorded [and later transcribed] by means of a tape recorder which was placed on top of the middle booth. One of the three booths was placed out of order by the FBI with the consent of the telephone company." (citations omitted)).

[75] Brief for Respondent at 3, *Katz*, 389 U.S. 347 (No. 35) ("Connected to the recorder were two microphones, which were taped to the outside of two of the booths. None of the equipment (the recorder, the microphones and the fastenings) penetrated the booths." (footnote omitted) (citation omitted)).

[76] United States v. Knotts, 460 U.S. 276, 285 (1983).

[77] United States v. Miller, 425 U.S. 435, 438 (1976) ("At the Bank of Byron, an agent was shown microfilm records of the relevant account and provided with copies of one deposit slip and one or two checks. At the Citizens & Southern National Bank microfilm records also were shown to the agent, and he was given copies of the records of respondent's account during the applicable period. These included all checks, deposit slips, two financial statements, and three monthly statements.").

[78] Smith v. Maryland, 442 U.S. 735, 737 (1979).

[79] Kyllo v. United States*,* 533 U.S. 27, 29 (2001); Brief for Respondent at 4, *Kyllo*, 533 U.S. 27 (No. 99-8508) ("On January 16, 1992, between 3:30 and 4:00 a.m., Oregon National Guard Sergeant Dan Haas used an Agema 210 thermal imager to scan the triplex where Tova Shook and petitioner lived. The thermal scan showed a high amount of heat emanating from the roof over the garage and the side wall of petitioner's house. In addition, it showed that petitioner's house was emitting more heat than the other houses in the triplex. The unusual heat loss detected by the imager was consistent with the heat loss associated with marijuana grow operations that Detective Haas had observed in the past." (citations omitted)).

[80] *See, e.g.*, Me.

[81] *See* Katz v. United States, 389 U.S. 347, 353 (1967); Brief for Petitioner at 5*, Katz*, 389 U.S. 347 (No. 35).

[82] David H. Goetz, *Locating Location Privacy*, 26 BERKELEY TECH. L.J. 823, 839 (2011) ("[T]he beepers used in *Knotts* and *Karo* were simple radio transmitters of limited range that forced the agents tracking the device to stay in close physical proximity to the device."); United States v. Karo, 468 U.S. 705 (1984).

[83] Brief for Respondent at 2, Smith v. Maryland, 442 U.S. 73 (1979) (No. 78-5374) ("[A] pen register: 'is a mechanical device attached to a given telephone line and usually installed at a central telephone facility. It records on a paper tape all numbers dialed from that line.'").

The simplistic nature of these early technologies did allow for two advantages in analysis. First, courts could isolate when the search occurred. Second, courts could visualize the privacy harm. Because of the one-off nature of the surveillance, courts could analyze what was happening at the moment of the search. For example, the collection of voice recordings in *Katz*, or the location of the beeper in *Karo*, or the capture of the thermal image in *Kyllo* were all distinct in time and action.[84] This focus also allowed courts to evaluate why that single act violated a reasonable expectation of privacy. Again, courts could focus on an individualized privacy harm made manifest against a single person.

At a theoretical level, advancements in surveillance technology complicates the controlling search theories. For example, a "reasonable expectation of privacy" makes sense in the context of human beings watching other human beings. From the *Katz* case onwards, courts have looked at what an individual has chosen to keep private (even in public) from other people.[85] The question of a reasonable expectation of privacy was generally directed against human observers and human police officers, with reasonableness turning on steps taken to preserve private acts from other human beings.[86] If a suspect had taken objectively reasonable steps to preserve privacy from other people, courts would be more willing to protect that claim. A reasonable expectation of privacy test makes less sense in a world where everything and everyone can be observed through automated, non-human digital surveillance systems.[87] In everywhere-everything systems there are few realistic choices to make to preserve privacy against the technology. In addition, the surveillance capabilities far exceed human monitoring.

This tension in the Fourth Amendment doctrine can be observed in the Supreme Court's more recent cases involving digital surveillance. Questions about when a search occurred, and the nature of the privacy harm were left unclear.

*United States v. Carpenter*[88] best highlights this reality. *Carpenter* involved police acquisition of privately owned, cell-site location information (CSLI) over a course of seven days.[89] Federal investigators suspected Timothy Carpenter of masterminding a series of robberies at local electronics stores.[90] Investigators requested Carpenter's cell site location data in an effort to place him at the scene of the crimes during the time of the robberies.[91] In order to obtain the data, investigators requested CSLI data from the cellphone providers that as a matter of course collect the cellphone location data of all of their subscribers.[92] The CSLI helped prove that Carpenter's

---

[84] *See* Katz*,* 389 U.S. 347; *Karo*, 468 U.S. 705; *Kyllo,* 533 U.S. 27.

[85] Katz, 389 U.S. at 351 ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.").

[86] Ferguson, *supra* note 33, at 853 ("One of the most striking realizations in studying the early Fourth Amendment cases is how dependent the surveillance was on human agents (and agency).").

[87] For more on the human/non-human distinction in police surveillance, *see id*. at 842.

[88] Carpenter v. United States, 585 U.S. 296, 311 (2018).

[89] *Id.*

[90] *Id*.

[91] *Id*.

[92] *Id*.

phone was at the locations of the robberies during the time of the robberies and with that information he was convicted. Carpenter appealed arguing that the collection of CSLI without a warrant violated his reasonable expectation of privacy and thus the Fourth Amendment.[93]

The Supreme Court agreed with Carpenter, holding that a warrant was required for collection of long-term CSLI (seven days' worth or more).[94] Numerous scholars have addressed *Carpenter* and what it means for the future of the Fourth Amendment,[95] but for purposes here, three points are important. First, the majority expressed concern with police surveillance capacities that allowed for overbroad, retrospective, aggregating, pervasive, and arbitrary searches against large portions of the population.[96] The Supreme Court focused on the capacity to search against everyone with a cellphone, as opposed to focusing on the precise information obtained against a single cellphone subscriber.[97] Second, the Court left unclear when exactly the search occurred, using the word "acquired" to signify the moment of the Fourth Amendment search.[98] Third, the Court suggested that with a warrant, this type of CSLI tracking would be constitutional.[99]

*Carpenter* adopted the arguments of five concurring Justices in *United States v. Jones*, a case involving long-term tracking of a vehicle via GPS technology.[100] The *Carpenter* Court explicitly addressed the harms of warrantless long-term tracking identified by Justice Sotomayor in her *Jones* concurrence.[101] In addition, the *Carpenter* Court acknowledged the qualitative and quantitative differences involved with digital exposure that they had first articulated in *Riley v. California*, a case involving the warrantless search of a smartphone.[102] *Carpenter* confirmed that "digital is different" when it comes to the Fourth Amendment but left many questions unanswered.[103]

*Carpenter* offers a helpful, but incomplete introduction to the everything-everywhere search problem. CSLI itself is an everything-everywhere technology. The catch is that the technology is being operated by a private company (the cellphone company), not the government. That distinction allowed the Supreme Court to focus on acquisition of the data from the company and avoid the harder question of what the analysis would be if the government was collecting the CSLI directly.[104] To put a finer point on it, imagine if the FBI was continually tracking everyone's

---

[93] *Id*.
[94] *Id*. at 310 ("[W]e hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI".).
[95] *See, e.g.*, Matthew Tokson, *The Carpenter Test as a Transformation of Fourth Amendment Law*, 2023 U. ILL. L. REV. 507, 527 (2023); Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. 357, 360 (2019); Evan H. Caminker, *Location Tracking and Digital Data: Can* Carpenter *Build a Stable Privacy Doctrine?*, 2018 SUP. CT. REV. 411, 451 (2019).
[96] Carpenter, 585 U.S. at 311–12.
[97] *Id*. at 312.
[98] *Id*. at 316–17.
[99] *Id*. at 318.
[100] *Id.* at 310 ("A majority of this Court has already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements.").
[101] *Id*. at 311–12.
[102] *Id.*
[103] Ferguson, *supra* note 33, at 819–20.
[104] Although arguably, the Supreme Court suggested in *Carpenter* that it would not make a difference whether the government or a private party owned the technology. Carpenter, 585 U.S. at 309–10 ("Whether the Government employs its own surveillance technology as in

cellphone location at all times. Would the Supreme Court find the FBI's tracking system a violation of a reasonable expectation of privacy? Or to borrow the facts from *Jones*, if the FBI were tracking all automobiles via GPS, would the Supreme Court find the tracking system a violation of a reasonable expectation of privacy? When was the search? At the setup of the collection system? When anyone's data was collected? When the suspect's data was collected? What if there was an enabling law that authorized mass collection on every American cellphone user? Would the law be constitutional?

Relatedly, *Carpenter* hints at a harder question of whether a warrant could allow the use of this system of mass location data collection against everyone.[105] If the FBI directly collected all the locations of cellphones and cars but did not examine the data until they obtained a warrant for a particular person, would that legal process save the system from being found unconstitutional? This issue was not central to *Carpenter* because the initial collection was done by a private, non-governmental entity outside of Fourth Amendment scrutiny, but would arise if the FBI was seeking to collect the data itself.[106] The open question is whether the FBI could do the initial data capture against everyone, if, after the fact, they obtained a warrant to target a particular suspect.[107]

As is evident, these are the same questions arising in the geofence debate. When does the search occur? Who has an expectation of privacy? Who is harmed? And, can a warrant cure the privacy harm? These are all contested issues and are the subjects of the next section.

### *C. The Geofence Debate*

Geofence queries offer a revealing example of an everything-everywhere search. Geofence queries involve law enforcement requests for geolocation data from third-party providers (for example Google, smart car telematics, cellphone providers, Uber, or Fog Science Reveal).[108] A geofence query seeks access to stored location data to find a suspect or a witness to a crime.[109] For example, until 2024, Google ran a massive data collection system called the "Sensorvault."[110]

---

*Jones* or leverages the technology of a wireless carrier, we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI.").

[105] Carpenter, 585 U.S. at 311.

[106] *Id.*

[107] This issue has been litigated in the international national security context in the form of Fourth Amendment challenges to NSA bulk collection. *ACLU v. Clapper*, 785 F.3d 787, 826 (2d Cir. 2015); Charlie Savage, *Surveillance Court Rules that N.S.A. Can Resume Bulk Data Collection*, N.Y. TIMES (June 30, 2015), https://www.nytimes.com/2015/07/01/us/politics/fisa-surveillance-court-rules-nsa-can-resume-bulk-data-collection.html [https://perma.cc/2KKS-85JH].

[108] *See, e.g.*, United States v. Chatrie, 590 F. Supp. 3d 901, 906 (E.D. Va. 2022); *In re* Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation, 497 F. Supp. 3d 345, 349 (N.D. Ill. 2020); Amster & Diehl, *supra* note 25, at 392 ("Questions surrounding geofence warrants' legality thus occupy less explored regions at the intersection of new technology and the Fourth Amendment: probable cause, particularity, and proper warrant execution.").

[109] *See* Jennifer Valentino-DeVries, *Google's Sensorvault Is a Boon for Law Enforcement. This Is How It Works.*, N.Y. TIMES (Apr. 13, 2019), https://www.nytimes.com/2019/04/13/technology/google-sensorvault-location-tracking.html [https://perma.cc/FPL9-KRX6]; Reed Sawyers, *For Geofences: An Originalist Approach to the Fourth Amendment*, 29 GEO. MASON L. REV. 787, 789 (2022) ("Geofence queries utilize the enormous repositories of location data collected by technology companies during their ordinary business activities. In a geofence query, investigators request that these companies scan their location databases to identify users present within a 'geofence'–a specified set of geographic and temporal coordinates virtually 'enclosing' a target location. Queries are used to identify individuals who were geographically and temporally proximate to a crime scene.").

[110] *See* Valentino-DeVries, *supra* note 109; Note, *Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508, 2512 (2021) ("Geofence warrants rely on the vast trove of location data that Google collects from Android users–approximately 131.2 million

Sensorvault, like other geolocational data systems, collected digital clues about where individuals were located and where they travelled.[111] Other third-party databrokers like Fog Reveal also provide law enforcement direct access to location data.[112] The result is an amazingly powerful geolocational tool that could reveal everywhere you have been with your digital device and by inference everything you have been doing there.[113] The data collection was constant, ongoing, revealing, and virtually inescapable if you possessed a smartphone. Everyone was tracked everywhere they went.

For example, assume police requested the Sensorvault data about one of Timothy Carpenter's co-conspirators in the robberies. Police could have asked for Google data about which smartphones were at a particular electronics store around the time of a known robbery. The request would be limited in time, place, and duration, but the dataset of possible Google identifiers to be searched is almost unlimited (potentially all of Google's 500+ million users stored data).[114] The search would only be possible because of the scale of data collected and sophisticated algorithms that can retrieve the necessary data. A judge deciding on the constitutionality of the warrantless acquisition of this information would need to ask whether the court is supposed to evaluate the potential privacy risk of this vast dataset running against everyone (which is significant) or just evaluate the actual data revealed about the suspect (which is limited).[115] It is not a straightforward analysis. A careful examination of the *Carpenter* majority opinion shows that the Supreme Court was more concerned with the potential privacy risk of police accessing a vast trove of locational data against everyone than what police actually requested about Mr. Carpenter.[116] Again, the harms articulated in the majority opinion all involved the potential abuse of an unlimited, retrospective tracking technology.[117] At the same time, the actual request of particular incriminating facts was fairly limited (in terms of the facts revealed about the suspect).[118]

Beyond the first-order question of whether acquisition of geofence data is a search for

---

Americans–and anyone who visits a Google-based application or website from their phone, including Calendar, Chrome, Drive, Gmail, Maps, and YouTube, among others."); *In re* Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation, 497 F. Supp. 3d 345, 351–52 (N.D. Ill. 2020).

[111] Amster & Diehl, *supra* note 25, at 389 ("Google uses the SensorVault to target advertisements, determine when stores are busy, help users track their movements, and provide traffic estimates. But law-enforcement officials now also use the SensorVault for criminal investigations."); Jennifer Lynch, *Google's Sensorvault Can Tell Police Where You've Been*, ELEC. FRONTIER FOUND. (Apr. 18, 2019), https://www.eff.org/deeplinks/2019/04/googles-sensorvault-can-tell-police-where-youve-been [https://perma.cc/AC94-3M6W].

[112] Dell Cameron, *What is Fog Reveal? The Police App Tracking Your Phone*, GIZMODO, (Sep. 9. 2022), https://gizmodo.com/what-is-fog-reveal-police-app-tracking-your-phone-1849514556 [https://perma.cc/TQK3-ULKW].

[113] *See generally*, Alicia Solow-Niederman, *Information Privacy and the Inference Economy*, 117 NW. U. L. REV. 357 (2022); Owsley, *supra* note 5, at 838.

[114] United States v. Chatrie, 136 F.4th 100, 102 (4th Cir. 2025) (*en banc*) (Diaz, C.J. concurring) ("Google collects the Location History of over 500 million users, and it's this data that law enforcement accesses via a geofence warrant.").

[115] This distinction between the capacity of a surveillance system and the actual data collected is address in a prior article. Ferguson, *supra* note 1, at 40.

[116] *See* Carpenter v. United States, 585 U.S. 296, 312 (2018) ("Critically, because location information is continually logged for all of the 400 million devices in the United States—not just those belonging to persons who might happen to come under investigation—this newfound tracking capacity runs against everyone.").

[117] Ferguson, *supra* note 1, at 34 (describing the Supreme Court's concern with arbitrary policing).

[118] For example, the Court in *Carpenter* specifically declined to address surveillance technologies similar to geofence warrants. *Carpenter*, 585 U.S. at 316 ("Our decision today is a narrow one. We do not express a view on matters not before us: real-time CSLI or "tower dumps" (a download of information on all the devices that connected to a particular cell site during a particular interval)").

Fourth Amendment purposes lurks the secondary question of whether a warrant would cure the privacy harm. As will be discussed, technology companies like Google developed a three-step geofence warrant process that allows a narrowing of data localization from all Google devices to the targeted individual.[119] These two questions are at the center of appellate court decisions on the geofence puzzle.

Due to the popularity of geofence warrants among law enforcement, Google was forced to change its corporate policy in 2024.[120] No longer is the data stored in the Sensorvault and accessible to police with a three-step warrant.[121] Google changed the default to store the location data on the phone itself. [122] This policy change forces police to obtain a warrant for the phone and directed at the phone's owner before accessing the data.[123]

Despite Google's corporate policy changes, geofence requests still present an interesting conceptual search problem because they involve the private collection of vast stores of personal location data but are only queried by police to investigate discrete moments in time.[124] In addition, other companies still have the capacity to track digital devices at a global scale for police use.[125] And, as mentioned, several cases involving geofence requests have divided the federal courts of appeal and will soon be before the United States Supreme Court.

1. Search Question

The first question courts must ask is whether a search occurs when police request geofence data from Google's Sensorvault (or equivalent).[126] Again, under current doctrine the answer turns on whether individuals have a reasonable expectation of privacy against the government in this Google-collected location data.[127]

It is not an easy question to answer in the abstract, as issues arise about the third-party

---

[119] Amster & Diehl, *supra* note 25, at 389 ("In response to increasing government requests for information, Google has crafted a three-step, self-directed process for law-enforcement officials trying to obtain user data. As Google explained in a 2020 court filing, it has "instituted a policy of objecting to any warrant that fail[s] to include "its mandated tailoring process."); *see* Gabriel J.X. Dance & Jennifer Valentino-DeVries, *Have a Search Warrant for Data? Google Wants You to Pay*, N.Y. TIMES (Jan. 24, 2020), https://www.nytimes.com/2020/01/24/technology/google-search-warrants-legal-fees.html [https://perma.cc/8RNW-WDAD]; *see also* Suppl. Decl. of Marlo McGriff at 2, United States v. Chatrie, 590 F. Supp. 3d 901 (E.D. Va. 2022).

[120] *See* Cyrus Farivar & Thomas Brewster, *Google Just Killed Warrants That Give Police Access to Location Data*, FORBES (Dec. 14, 2023, at 17:43 ET), https://www.forbes.com/sites/cyrusfarivar/2023/12/14/google-just-killed-geofence-warrants-police-location-data [https://perma.cc/AQ5C-E2CB]; Marlo McGriff, *Updates to Location History and New Controls Coming Soon to Maps*, GOOGLE (Dec. 12, 2023), https://blog.google/products/maps/updates-to-location-history-and-new-controls-coming-soon-to-maps [https://perma.cc/PE8F-F955].

[121] McGriff, *supra* note 120.

[122] *Id.*

[123] *See* Farivar & Brewster, *supra* note 120.

[124] Sawyers, *supra* note 109, at 792–93 ("[G]eofence queries seek to identify previously unknown individuals whose location history demonstrates they were at a specific location, often a crime scene, at a specific time.").

[125] Marc Dahan, *What is Fog Data Science and Why Should You Care?*, COMPARITECH (Jan. 2, 2023), https://www.comparitech.com/blog/information-security/fog-data-science [https://perma.cc/L67A-NJNK].

[126] In re Search of Information Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 736–37 (N.D. Ill. 2020) (obtaining a warrant and arguing for the validity of that warrant, "the [G]overnment is treating its proposed capture of information as a search").

[127] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

doctrine,[128] data as property,[129] and whether the amount of data collected changes the analysis.[130] Despite the difficulties, several courts have come to differing opinions on the subject.

For example, in *United States v. Chatrie*, a divided Fourth Circuit Court of Appeals panel held that an individual has no expectation of privacy in their Sensorvault data.[131] The Fourth Circuit panel rationalized that the data collected was both limited in time (only two hours) and voluntarily provided to Google by enabling the "location history" service on the individual's smartphone.[132] Judge Wynn wrote a lengthy dissent arguing why *Carpenter* should be read to find a Fourth Amendment search when applied to geofences.[133] The panel decision was reheard *en banc* in 2025.[134] The *en banc* court affirmed the panel opinion in a single sentence, but then proceeded to offer nine different concurring opinions with none of the opinions able to gain a majority of votes.[135] The splintered court thus avoided the hard Fourth Amendment search questions at issue in this Essay. As stated earlier, the United States Supreme Court granted certiorari in *Chatrie* in January 2026.

In contrast, a Fifth Circuit Court of Appeals panel held in *United States v. Jamarr Smith* that a geofence request was a Fourth Amendment search.[136] The court held that under *Carpenter*, this type of location data collection violated a reasonable expectation of privacy.[137] The Fifth Circuit panel detailed the permeating nature of geolocation data and how, like CSLI, it revealed too many of the privacies of life, even for a short time.[138] Further, the Fifth Circuit highlighted how the *Carpenter* opinion had protected even voluntary disclosure of CSLI, thus undermining the third-party doctrine argument.[139] After all, Timothy Carpenter knew he had a cellphone that was being tracked by the cellphone company and yet did not lose a reasonable expectation of privacy.[140] In short, the Fifth Circuit panel found analogies to *Carpenter* convincing enough to find the surveillance a search for Fourth Amendment purposes.[141]

In these cases and others that have considered the issue, the question of reasonable expectations remains unclear.[142] Which expectations are reasonable are just not established in any easily observable *ex ante* manner. In addition, like in *Carpenter,* it is not clear when the search

---

[128] Stephen E. Henderson, *After United States v. Jones, After the Fourth Amendment Third Party Doctrine*, 14 N.C. J. L. & TECH. 431, 437 (2013).
[129] James Grimmelmann & Christina Mulligan, *Data Property,* 72 AM. U. L. REV. 829, 850 (2023).
[130] Gray & Citron, *supra* note 6, at 95.
[131] United States v. Chatrie, 107 F.4th 319, 330 (4th Cir. 2024), *reh'g en banc granted*, No. 22-4489, 2024 WL 4648102, at *1 (4th Cir. Nov. 1, 2024).
[132] *Id.* at 331–32.
[133] *Id*. at 339 (Wynn J., dissenting).
[134] *See* United States v. Chatrie, 136 F.4th 100 (4th Cir. 2025) (*en banc*).
[135] *Id*.
[136] United States v. Smith, 110 F.4th 817, 820 (5th Cir. 2024).
[137] *Id.* at 834.
[138] *Id.* at 832.
[139] *Id.* at 836.
[140] *Id.*
[141] *Id.*
[142] *See generally* United States v. Smith, 110 F.4th 817 (5th Cir. 2024); Carpenter v. United States, 585 U.S. 296 (2018); *see also* People v. Meza, 312 Cal. Rptr. 3d 1, 21 (Ct. App. 2023).

occurs, complicating constitutional analysis.[143] This puzzle is further addressed in the next section.

2. Warrant Question

*Carpenter*, *Jones*, and *Riley* all suggest that a warrant would cure the Fourth Amendment privacy harm.[144] The expressed concern was that the arbitrary, overbroad, retrospective nature of the data collection against everyone could be mitigated by a particularly drawn judicial warrant.[145] Police officers seeking geofence information have thus used the warrant process to obtain the needed data. A warrant has not been judicially mandated, but Google's lawyers have demanded police follow the three-step warrant process that the company devised.[146]

The three-step warrant process is detailed in *Chatrie* and *Jamarr Smith*, but, in short, it requires an initial step of anonymously searching all of Google Sensorvault for accounts associated with a device in a particular area during a particular time.[147] Then, it requires a second step of requesting "contextual data" on travel of those (still anonymous) devices that might be consistent with the government's theory of the case.[148] Third, from that narrowed group of identifiable numbers, it requires Google to provide personal identifying information on specific device holder(s).[149] The idea is to search all of Google's data, but only reveal the identity of the few devices that are most likely the targeted suspect.[150]

The Fourth Circuit panel did not address whether Google's three-step warrant process satisfied the Fourth Amendment's requirement for reasonableness because the court resolved the question on the threshold search question (which was affirmed *en banc*).[151] The panel held that Chatrie had no reasonable expectation of privacy, and thus there was no Fourth Amendment search or need for a warrant.[152] The Fifth Circuit did address the threshold search question, determining that the initial search of the Sensorvault (Step One) was akin to a general warrant and thus

---

[143] *See* Carpenter, 585 U.S. at 310.

[144] *See, e.g.*, Riley v. California, 573 U.S. 373, 403 (2014) ("Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life,' The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.").

[145] *See* Amster & Diehl, *supra* note 25, at 394.

[146] Decl. of Marlo McGriff at 4–5; United States v. Chatrie, 590 F. Supp. 3d 901 (E.D. Va. 2022).

[147] Chatrie, 590 F. Supp. 3d 901 ("At Step 1, 'Google w[ould] provide "anonymized information" regarding the Accounts that are associated with a device that was inside the described geographical area' from 4:20 p.m. to 5:20 p.m.").

[148] *Id*. ("At Step 2, 'Law enforcement w[ould] return a list [of accounts] that they ha[d] attempted to narrow down.' Google would then 'produce contextual data points with points of travel outside of the geographical area.' During Step 2, the warrant expanded the timeframe to include thirty minutes before and thirty minutes after the initial hour-long window, so that the Step 2 window was two hours long in total.").

[149] *Id*. ("Finally, at Step 3, after Government review, Google would 'provide identifying account information/CSI for the accounts requested' by law enforcement.").

[150] *See id.*

[151] United States v. Chatrie, 107 F.4th 319, 322 (4th Cir. 2024), *reh'g en banc granted*, No. 22-4489, 2024 WL 4648102 (4th Cir. Nov. 1, 2024); United States v. Chatrie, 136 F.4th 100 (4th Cir. 2025) (*en banc*).

[152] Chatrie, 107 F.4th at 330.

unreasonable.[153] The Fifth Circuit held that this type of search against 500 million devices[154] to find the information for the second step of the warrant process was too overbroad and non "particularized" (to use the language of the Fourth Amendment).[155] After all, the initial search was against almost everyone with a Google phone or app in the Sensorvault (including you).[156] The lack of particularity made the warrant unreasonable.[157]

The Fifth Circuit panel's reasoning is interesting in its own right. If you take seriously the fact that to find the needle in the digital haystack you have to search through all the hay, you have a general search against everyone (or at least those covered by the U.S. Constitution). If the search of the American portion of those 500+ million devices[158] is not a general search, it is hard to think of what one would be. The search runs against everyone everywhere (including the justices of the Supreme Court).[159]

More provocatively, the reasoning calls into question whether a warrant would have made the *Carpenter* search reasonable. After all, viewed one way, the initial CSLI step one was a search against all of the cellphone company's subscribers in a geographic area. If reframed as a government order to search the entire CSLI database for a particular anonymized set of numbers in a large area, then the parallels to Sensorvault are easy to observe.[160] Put another way, if *Carpenter* had involved a three-step warrant, with the first step being a search of all CSLI in a large geographic area, then under the Fifth Circuit's logic, would that initial search through the data be akin to a general warrant so despised by the Founders?[161]

There is no satisfactory answer to these puzzles. The nature of mass data collection, even with a particularized target, still requires mass searching.[162] If that initial search is overbroad and thus unreasonable, no warrant can save it.[163] Such confusion opens the door to develop a new way

---

[153] Smith, 110 F.4th at 837–38 ("A general warrant cannot be saved simply by arguing that, after the search has been performed, the information received was narrowly tailored to the crime being investigated. These geofence warrants fail at Step 1—they allow law enforcement to rummage through troves of location data from hundreds of millions of Google users without any description of the particular suspect or suspects to be found.").

[154] Chatrie, 136 F.4th at 102 (Diaz, C.J. concurring) ("Google collects the Location History of over 500 million users, and it's this data that law enforcement accesses via a geofence warrant."). As of 2023, the average household has twenty-one devices in the United States. Deloitte Ctr. for Tech., Media, & Telecomm., *Balancing Act: Seeking Just the Right Amount of Digital for a Happy, Healthy Connected Life*, DELOITTE INSIGHTS (Sep. 5, 2023), https://www.deloitte.com/us/en/insights/industry/telecommunications/connectivity-mobile-trends-survey/2023.html#explore [https://perma.cc/LYN9-YT9A]. Combined with the 133 million households in the United States as of 2025, the total number of devices in the nation totals 2.793 billion. *See* Bus. Env't Profiles, *Number of Households*, IBISWORLD (Sep. 8, 2025), https://www.ibisworld.com/united-states/bed/number-of-households/31/ [https://perma.cc/8TWZ-XUTV].

[155] Smith, 110 F.4th at 838 ("In sum, geofence warrants are '[e]mblematic of general warrants' and are 'highly suspect per se.'" (quoting *Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508, 2520 (2021))).

[156] *See id.* at 837.

[157] *See id.* at 837–38.

[158] United States v. Chatrie, 136 F.4th 100, 102 (4th Cir. 2025) (*en banc*) (Diaz, C.J. concurring).

[159] *See Smith*, 110 F.4th at 836–37 (reasoning that geofence warrants violate the Fourth Amendment by authorizing a search of everything or everyone).

[160] *But cf.* Carpenter v. United States, 585 U.S. 316 (2018) (ruling that the court's decision was narrow and did not consider real-time CSLI or tower dumps).

[161] *See id.* Perhaps the answer turns on the fact that CSLI are necessarily geographically limited because the companies are querying the cell towers near an incident. The search might not be against all of their collected subscriber data, but only a geographically and temporally limited subset. The difference with the Sensorvault could be the centralized nature of collection and storage.

[162] *See, e.g.*, FERGUSON, *supra* note 7, at 9.

[163] *See* Smith, 110 F.4th at 837–38.

of thinking about the Fourth Amendment. One of the clarifying realities of an otherwise muddled Fourth Amendment doctrine is that sometimes it creates an opening for a new theory.

## II. THE RUMMAGING PRINCIPLE

As is evident from Part I, current doctrine does not provide a clear answer to whether a geofence request is a Fourth Amendment search, or whether a geofence warrant satisfies the particularity requirement of the Fourth Amendment.[164] Stated more generally, everything-everywhere technologies like geofences complicate the traditional reasonable expectation of privacy analysis and the warrant process. The open question is whether there is another theory that can adequately fill the gaps between the existing Fourth Amendment tests. The next subsection explains my answer – the rummaging principle – and then applies it to the geofence puzzle.

### *A. Rummaging and the Fourth Amendment*

Almost all judges and scholars agree that that the Fourth Amendment arose in response to the reviled general warrants and writs of assistance that granted surveillance power to British agents to police the American Colonies.[165] The fear was that these broad grants of policing power allowed for arbitrary rummaging into the homes, papers, effects, and persons of the colonists.[166] The fear of rummaging can be seen in Founding era documents, speeches, and in the first cases interpreting the Fourth Amendment.[167] It is also the animating principle behind the particularity requirement of a Fourth Amendment warrant.[168]

Modern Fourth Amendment doctrine has echoed this fear about granting police unrestrained rummaging powers. Whether one examines the search incident to arrest doctrine, or plain view/plain feel doctrine, inventory search doctrine, hot pursuit, or special needs doctrine cases, the harm of rummaging is regularly used as a limiting principle to restrain police actions.[169] In fact, one can reinterpret most of the Fourth Amendment canon through the lens of rummaging and see that the Supreme Court – over several decades and across divergent political ideologies –

---

[164] *See supra* Part I.

[165] Barry Friedman & Cynthia Benin Stein, *Redefining What's "Reasonable": The Protections for Policing*, 84 GEO. WASH. L. REV. 281, 316–17 (2016) ("It has long been a common consensus that the Fourth Amendment guards against the evil of arbitrary government rummaging in people's lives."); Laura K. Donohue, *The Fourth Amendment in a Digital World*, 71 N.Y.U. ANN. SURV. AM. L. 553, 554 (2017).

[166] United States. v. Galpin, 720 F.3d 436, 445 (2d Cir. 2013) (quoting Payton v. New York, 445 U.S. 573, 583 (1980)) ("The chief evil that prompted the framing and adoption of the Fourth Amendment was the 'indiscriminate searches and seizures' conducted by the British 'under the authority of general warrants.'").

[167] Laurent Sacharoff, *The Fourth Amendment Inventory as a Check on Digital Searches*, 105 IOWA L. REV. 1643, 1653 (2020) (footnotes omitted) ("[R]ummaging through papers for new crimes is the very definition, for both the founding generation and contemporary courts, of the fishing expedition the Fourth Amendment (and likely Fifth Amendment) sought to prevent.").

[168] Paul Ohm, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 VA. L. REV. IN BRIEF 1, 10 (2011) ("The Supreme Court has repeatedly explained that the Fourth Amendment's particularity requirement arose, at least in part, from the founders' concerns about British writs of assistance, general warrants issued by the king permitting soldiers to look in homes and places of business with few restrictions."); *see also* Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971); Commonwealth v. Freiberg, 540 N.E.2d 1289, 1300 (Mass. 1989) ("The particularity requirement serves as a safeguard against general exploratory rummaging by the police through a person's belongings.").

[169] *See, e.g.*, Chimel v. California, 395 U.S. 752, 767–68 (1969) (search incident to arrest); *Coolidge*, 403 U.S. at 467 (plain view); Minnesota v. Dickerson, 508 U.S. 366, 378 (1993) (plain feel); Florida v. Wells, 495 U.S. 1, 4 (1990) (inventory searches).

remains consistently focused on the dangers of an enhanced government rummaging power.[170]

The Supreme Court's approach to digital searches only confirms this consistent recognition of rummaging harms.[171] In *California v. Riley*, *United States v. Jones,* and *Carpenter v. United States*, the Court highlighted the harms of rummaging – and arguably relied on the principle even if they did not acknowledge this fact.[172] For example, Chief Justice John Roberts begins *Carpenter*'s Fourth Amendment analysis by centering rummaging:

> The Founding generation crafted the Fourth Amendment as a "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."[173]

Of course, recognizing that the Supreme Court has consistently relied on the rummaging principle to protect Fourth Amendment rights is one thing.[174] Operationalizing it into a test for future analysis is another. The next section summarizes what I have called "the rummaging test" to identify what types of legislative or technological powers are unreasonable searches under the Fourth Amendment.

### *B. The Rummaging Test*

At its core, the Supreme Court's long-standing concern with rummaging recognizes four interrelated harms: (1) arbitrariness and the misuse of police power; (2) overreach and the exploratory expansion of initially justified search power; (3) intrusions into constitutionally protected areas; and (4) exposure leading to the risk that private details will be used to silence or embarrass individuals.[175] Whether you think about general warrants, or CSLI systems of nationwide tracking, or using the search incident to arrest doctrine to search an entire house, these four harms are repeated in case after case.[176] In *Digital Rummaging*, I rather exhaustively canvas the cases and history to show how these four themes repeat, creating a coherent throughline of Fourth Amendment theory.[177]

For purposes here, it is sufficient to posit that a rummaging test might serve as an equally helpful framework for Fourth Amendment analysis of geofence requests.[178] In addition to the test

---

[170] *Id.*

[171] *See* Riley v. California, 573 U.S. 373, 403 (2014); United States v. Jones, 565 U.S. 400, 403 (2012); Carpenter v. United States, 585 U.S. 296, 303 (2018).

[172] *See* Riley, 573 U.S. at 403; Jones, 565 U.S. at 403; Carpenter, 585 U.S. at 301–03. As I wrote in *Digital Rummaging*, Carpenter can best be understood as an anti-rummaging case, as opposed to a reasonable expectation of privacy case. *See* Ferguson, *supra* note 17, at 1476.

[173] *Carpenter*, 585 U.S. at 303.

[174] *See, e.g.*, Arizona v. Gant, 556 U.S. 332, 345 (2009) (recognizing that "the central concern underlying the Fourth Amendment [is] the concern about giving police officers unbridled discretion to rummage at will among a person's private effects").

[175] *See* Ferguson, *supra* note 17, at 1510–20.

[176] *Id.* at 1496–1510.

[177] *Id.* at 1501–10.

[178] *See Geofence Warrants and the Fourth Amendment*, *supra* note 110, at 2519.

being as consistent, if not more consistent, with the Founding history of the Fourth Amendment, the rummaging test resolves the gaps created by the reasonable expectation of privacy test in the digital era.[179] My argument here is that the rummaging test is a superior way to address everything-everywhere searches because it is easier to administer and because it resolves the temporal questions of when a Fourth Amendment search occurs or when the privacy harm occurs.

If the question becomes whether the government was using an arbitrary, overbroad, intrusive, and potentially embarrassing surveillance power, the Fourth Amendment answers might get easier to visualize.[180] Simply put – did government agents rummage through citizens' lives without a warrant? If the answer is "yes," then the Fourth Amendment applies.[181] Again, this would be the threshold test (akin to a reasonable expectation of privacy test) to see if the surveillance was the kind of search the Fourth Amendment was designed to address. (It could still be a "reasonable" search with a warrant or exception, but the point is the Fourth Amendment applies). The rummaging test asks whether the government action is the type of arbitrary, overbroad, intrusive, and embarrassing power that gave rise to the Fourth Amendment in the first place.[182]

For example, if I walk down the street in a city that uses facial recognition surveillance technology to track my whereabouts through images, sensors, or digital clues, I might have a hard argument to claim that I had a reasonable expectation of privacy on the street.[183] But, under a rummaging test, I might have an easier time making the argument that police surveillance power was a form of digital rummaging to see what, if anything, I was doing. Without any suspicion of wrongdoing, the police were tracking me to see if I might be up to no good—for weeks or months. This arbitrary, overbroad, intrusive, and exposing search power raises a rummaging concern and thus a Fourth Amendment search concern.[184] And, just as a matter of non-legal common sense, the police are in fact "searching" for incriminating information.

The rummaging test also helps clarify when the Fourth Amendment harm occurs.[185] As discussed earlier, one challenge with everything-everywhere searches is that it is not clear when a search or privacy harm occurs.[186] In contrast to the reasonable expectation of privacy test, the

---

[179] *See* Ferguson*, supra* note 175, at 1499.
[180] *Id.* at 1477.
[181] *Id*.
[182] *See* Ferguson, *supra* note 17, at 1477 ("The rummaging test poses a deceptively simple question: are police seeking otherwise secured information in an unparticularized or overbroad manner? If so, police are rummaging in violation of the Fourth Amendment, and the act is unreasonable and thus unconstitutional. Factors to determine whether a police agent is rummaging involve avoiding the harms that gave rise to the Fourth Amendment in the first place, namely: (1) avoiding *arbitrary* grants of generalized police power; (2) limiting *overreach* from initially justified searches; (3) protecting against *intrusion* of constitutionally protected interests (like the security of homes, papers, persons, and effects); and (4) minimizing *exposure* to embarrassing private information.").
[183] *But see* Ferguson, *supra* 68, at 1292 ("This Article argues that video analytics running on these citywide surveillance systems violates a reasonable expectation of privacy and is a search for Fourth Amendment purposes."); Ferguson, *supra* note 66, at 1141.
[184] *See* Ferguson, *supra* note 17, at 1477.
[185] *See* Emily Berman, *Digital Searches, the Fourth Amendment, and the Magistrates' Revolt,* 68 EMORY L.J. 49, 57 (2018) ("[D]igital storage medium seized because it contains evidence of criminality will include innocent data, raising privacy concerns. A search of a cell phone might reveal communications between coconspirators but also private text messages unrelated to the crime.").
[186] Again, in a traditional police search, it is easy to identify when an officer looks through some papers or opens the trunk of a car. The temporal questions about the act of searching and expectations of privacy are clear (even if the Fourth Amendment answers are not). With constantly collecting ALPRs, or video feeds, or cell signals, or geolocational details, when the police begin their search is less clear.

rummaging test focuses on the power to search, not just the act of searching.[187] The government's rummaging power threatens individual security before, during, and after the actual physical search.[188] Setting up a nationwide government-controlled CSLI database to track all cellphone locations might be just as chilling as the FBI using it in a particular criminal case.

This claim finds support in other areas of the Fourth Amendment. If you reexamine the Fourth Amendment through this lens of power, you will see that it regularly controls the outcome of cases.[189] General warrants were threatening because of the power they granted (even if a British agent never used that power).[190] The threat to use arbitrary policing power creates the harm and arises before and after the physical act of searching by a government official. Similarly, judicially crafted limits around the search incident to arrest exception, or the inventory exception, or the particularity of warrants are all about controlling the power of police within specific authorized grants of authority.[191] The limits are less directed toward the acts of the police when they are investigating as much as limiting grants of power *ex ante*.[192] In essence, the cases say that to prevent rummaging with a warrant, you may not extend a search beyond the initial limited authorization granted in the warrant.[193] As a final example, CSLI collection was deemed harmful to privacy not because it revealed where Timothy Carpenter was at the time a robbery, but because it gave police power to expose anyone with a cellphone for any reason (without a warrant).[194] The time that mattered to the court was not the six moments of CSLI collection in various electronics stores but the store of CSLI collection usable against everyone.[195] The Fourth Amendment harms ran toward a fear of continuous mass surveillance power, less than the actual information recovered.[196] In short, the Supreme Court has recognized the harm that arises from the power to rummaging through our lives in an arbitrary, overbroad, intrusive, and embarrassing manner goes beyond a specific act of searching.[197]

---

[187] *See* Fergusion, *supra* note 17, at 1477 (articulating questions to be asked in context of rummaging test).

[188] *See* David Gray, *Collective Rights and the Fourth Amendment After* Carpenter, 79 MD. L. REV. 66, 82 (2019) (The "collective nature of the Fourth Amendment is clear when considering precise nature of the right it preserves. The Fourth Amendment commands that 'the people' shall live in a state free from fear of being the targets of unreasonable searches and seizures, particularly when wielded as tools to punish disfavored groups.").

[189] *See* Carpenter, 585 U.S. at 301–02 (rummaging language connects the harm of British officers arbitrarily searching through homes as driving force for American pursuit of independence).

[190] Donald A. Dripps, *"Dearest Property": Digital Evidence and the History of Private "Papers" as Special Objects of Search and Seizure*, 103 J. CRIM. L. & CRIMINOLOGY 49, 61 (2013) ("The Fourth Amendment is generally seen as a response to two protests against particular abuses, the first against Writs of Assistance in the colonies in 1761–1762 and the second against general warrants in England in 1764–1765.").

[191] *See, e.g.*, Chimel v. California, 395 U.S. 752, 767–68 (1969) (discussing rummaging and search incident to arrest); Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971) (discussing rummaging and plain view); Andresen v. Maryland, 427 U.S. 463, 480 (1976) (discussing rummaging and warrant particularity); Minnesota v. Dickerson, 508 U.S. 366, 378 (1993) (discussing rummaging and frisks); Florida v. Wells, 495 U.S. 1, 4 (1990) (discussing rummaging and inventory searches).

[192] *Id.*

[193] Chimel v. California, 395 U.S. 752, 767 (1969) ("'After arresting a man in his house, to rummage at will among his papers in search of whatever will convict him, appears to us to be indistinguishable from what might be done under a general warrant; indeed, the warrant would give more protection, for presumably it must be issued by a magistrate.'") (quoting United States v. Kirschenblatt, 16 F. 2d 202, 203 (1926)).

[194] *See* Carpenter, 585 U.S. at 12–13.

[195] *Id.* at 13–14.

[196] *Id.*

[197] *See id.* at 316–20.

To identify whether the Fourth Amendment applies, courts should ask when the police acquired the power to rummage. In physical government surveillance systems (ALPRs, video analytics) the time might be when the surveillance system was turned on and began searching through the available data. If the question is whether a city-wide ALPR/video analytics systems is an arbitrary, overbroad, intrusive, and potentially embarrassing surveillance power, the answer is yes, and the Fourth Amendment threshold question has been answered in the affirmative.[198]

In private data collection systems (CSLI, Sensorvault), the threshold might be when police acquire the data from a third-party provider. The Fourth Amendment search happens when the government acquires the power to conduct arbitrary, overbroad, intrusive, and exposing collections of information and thus engage in rummaging through third-party collections.[199] This could also mean obtaining a legislative grant of generalized police power (akin to a general warrant) or demanding via subpoena a third-party to provide arbitrary, overbroad, intrusive, and exposing data on a suspect.[200] To make this rummaging argument more concrete, I will apply the rummaging test to the geofence puzzle.

### *C. Rummaging Applied to Geofences*

The first question to ask is whether a warrantless geofence request is a "search" for Fourth Amendment purposes—not under a reasonable expectation of privacy test, but under a rummaging test.[201] This first question responds to the Fourth Circuit's *Chatrie* panel opinion but with an alternative frame of analysis.[202] The second question is whether even with a three-step geofence warrant, the initial collection against everyone raises digital rummaging harms sufficient to make the search unreasonable. This second question responds to the Fifth Circuit's *Jamarr Smith* panel opinion and the court's analogy to general warrants.[203]

#### 1. Warrantless Geofence Requests and Digital Rummaging

Under a rummaging test, the analysis about *warrantless* geofence requests is straightforward. If the question is when did the police acquire the power to rummage, the answer is when they requested Google to provide the Step One search data. This is the threshold inquiry.[204] This analysis also holds if we imagined a Fog Data Science portal that allows police officers to examine digital clues around a crime. At a basic level, the police are, in fact, searching/rummaging for clues when requesting the data of people who might have been at the scene of a crime.[205] Police do not know who did the crime and are casting a wide net to find the suspect and others who might

---

[198] *See* Ferguson, *supra* note 17, at 1521–23.
[199] *Id.*
[200] *See* Carpenter, 585 U.S. at 303–04.
[201] *See* Ferguson, *supra* note 17, at 1521.
[202] United States v. Chatrie, 107 F.4th 319 (4th Cir. 2024), *aff'd per curiam*, 136 F.4th 100 (4th Cir. 2025).
[203] *See* United States v. Smith, 110 F.4th 817, 837–838, 840 (5th Cir. 2024).
[204] Ferguson, *supra* note 17, at 1521.
[205] Sidney Fussell, *Creepy "Geofence" Finds Anyone Who Went Near a Crime Scene*, WIRED (Sep. 4, 2020, at 7:00 ET), https://www.wired.com/story/creepy-geofence-finds-anyone-near-crime-scene/ [https://perma.cc/Y3S8-ZT8Q].

have been around.[206] Police are rummaging for possible leads without any particularized limitation.[207]

Each of the rummaging principles applies. First, a concern about arbitrary power is raised in warrantless geofence requests. The advent of locational tracking technology combined with the ubiquity of cellphone and other smart device ownership has created an unprecedented and almost unlimited source of personal data.[208] The potential for arbitrary searches is grave.[209] Police can track anyone anywhere for any reason (again, without a warrant) within the collected geolocational data.[210]

Second, the overreach problem also arises with geofence requests. Initial suspicions might generate a geofence request that could lead to other as-of-yet-unknown crimes or embarrassing revelations.[211] The idea that the government can just virtually search through places and people without cause is ripe for abuse. For example, with a geofence request, one could trace back all the people who went to a substance abuse clinic or house of worship.[212] Police could track protesters from political marchers, or politicians from fundraisers, or gun owners from gun shows. The resulting data could be used to initiate other completely unconnected criminal investigations. Many of the people will be innocent of criminal wrongdoing but will still be tracked. In fact, even with a crime and a suspect, a geofence request will regularly capture the data of innocent people.[213] After all, other people around a particular area will be identified along with the suspect. Those data trails will be investigated and even if the information is used to exclude them from suspicion, their information will be collected by government agents and possessed for future use in future criminal cases.[214]

Third, as to intrusion into constitutionally protected interests, *Carpenter* and *Jones* extended the traditional constitutional interests protected by the Fourth Amendment to include locational data.[215] While not in the constitutional text, and while ostensibly based on conceptions of reasonable expectations of privacy, there is little question now that long-term location tracking

---

[206] *Id.*

[207] Note, *supra* note 110, at 2519 ("Geofence warrants necessarily involve the very sort of 'general, exploratory rummaging' that the Fourth Amendment was intended to prohibit.").

[208] Jennifer Valentino-DeVries, *Tracking Phones, Google Is a Dragnet for the Police*, N.Y. TIMES (Apr. 13, 2019), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html [https://perma.cc/5CK5-LKKH].

[209] Drew Harwell and Craig Timberg, *How America's Surveillance Networks Helped the FBI Catch the Capitol Mob*, WASH. POST (Apr. 2, 2021, at 9:00 ET), https://www.washingtonpost.com/technology/2021/04/02/capitol-siege-arrests-technology-fbi-privacy/ [https://perma.cc/Q257-LHYT].

[210] Valentino-DeVries, *supra* note 208.

[211] Jon Schuppe, *Google Tracked His Bike Ride Past a Bulgarized Home. That Made Him a Suspect*, NBC NEWS (Mar. 7, 2022), https://www.nbcnews.com/news/us-news/google-tracked-his-bike-ride-past-burglarized-home-made-him-n1151761 [https://perma.cc/JAK7-BG28].

[212] *See* Sidney Fussell, *Creepy "Geofence" Finds Anyone Who Went Near a Crime Scene*, WIRED (Sep. 4, 2020, 7:00 AM), https://www.wired.com/story/creepy-geofence-finds-anyone-near-crime-scene/ [https://perma.cc/Y3S8-ZT8Q].

[213] Alfred Ng, *Geofence Warrants: How Police Can Use Protesters' Phones Against Them*, CNET (June 16, 2020, 9:52 AM), https://www.cnet.com/news/privacy/geofence-warrants-how-police-can-use-protesters-phones-against-them/ [https://perma.cc/XY5C-CRGP].

[214] State v. Burch, 961 N.W.2d 314 (2021).

[215] Carpenter, 585 U.S. at 310 ("A majority of this Court has already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements.") (citing Jones, 565 U.S. at 430).

implicates the Fourth Amendment.[216] Securing this private information from governmental intrusion is thus a legitimate concern of the Fourth Amendment.[217] In addition, the data comes from the person (and technically the smartphone effect), is the equivalent to digital papers, and implicates the same locational privacy interests protected in *Carpenter/Jones* discussed above. Thus, for purposes of analyzing rummaging, the question of intrusion is straightforward: bulk private locational data is the kind of information that the Fourth Amendment secures against government acquisition.

Finally, the data could be used to embarrass, intimidate, or expose people and groups. If the government can access location data on a whim such a reality—even just the potential of collection—might discourage people from attending protests, attending religious services, or seeking substance abuse treatment among other things. Again, in the warrantless context, the power to conduct generalized searches of areas is a privacy-threatening tool.

Analyzing the rummaging harms of geofence requests suggests that warrantless acquisition of the data implicates Fourth Amendment principles.[218] Concerns about intrusions into private activity, location, plus the arbitrary nature of its application to anyone, and the potential for overreach, and public embarrassment all suggest a digital rummaging concern. The harms are real and suggest an unreasonable grant of police power against most people with a Google app enabled. While the same constitutional conclusion could be found by applying *Carpenter* and *Jones* and a reasonable expectation of privacy test, the rummaging harms make an even stronger argument for requiring a warrant.[219]

Applying the rummaging test, a court would find that geofence requests are a search under the Fourth Amendment because they are the type of rummaging power that gave rise to the Fourth Amendment in the first place. Without a warrant, such governmental search power triggers Fourth Amendment scrutiny (similar to how a violation of a reasonable expectation of privacy triggers Fourth Amendment protection).[220] In a traditional geofence scenario with a third-party's data, the request to acquire the information is the act that triggers Fourth Amendment scrutiny.[221] The act could also be the governmental collection of data if the surveillance technology were owned and operated by the government (or provided through a police-controlled portal). For example, if the police developed their own CSLI tracking system or Sensorvault, the rummaging test would apply at the collection stage.

The above discussion focused on a warrantless request. The more difficult question is

---

[216] *Id.*; *see also* Ohm, *supra* note 95, at 369.

[217] Alfred Ng, *Geofence Warrants: How Police Can Use Protesters' Phones Against Them*, CNET (June 16, 2020, 9:52 AM), https://www.cnet.com/news/privacy/geofence-warrants-how-police-can-use-protesters-phones-against-them/ [https://perma.cc/XY5C-CRGP]; Amster & Diehl, *supra* note 25, at 394 ("Google's SensorVault is a prodigious pool of consumer location information, pioneered in part to target advertisements but now routinely used by law enforcement for geofence warrants.").

[218] Google asserts that government acquisition of its customer data is a Fourth Amendment search. *See* Brief of Amicus Curiae Google LLC in Support of Neither Party Concerning Defendant's Motion to Suppress Evidence from a "Geofence" General Warrant at 11–12 (arguing that geofence requests are searches for Fourth Amendment purposes).

[219] Carpenter, 585 U.S. at 296; United States v. Jones, 565 U.S. 400, 411.

[220] Katz v. United States, 389 U.S. 347 (1967).

[221] This is similar to Carpenter: it was the request to access the CSLI that triggered the Fourth Amendment. Carpenter, 585 U.S. at 31–11.

whether even with a judicial warrant, such a geofence request runs afoul of the rummaging principle. This is the subject of the next subsection.

2. Geofence Warrants and Digital Rummaging

The difference between a geofence *request* and a geofence *warrant* is the presence of a signed judicial order with an accompanying sworn affidavit.[222] It is important to emphasize the judicial nature of the warrant process. As admirable as it is for a private company like Google to require a heightened process to protect data privacy, from a constitutional perspective the only valid procedural protection should be a judicial warrant.[223] On a whim, Google could change its corporate policy or modify it based on political pressure. Or another competitor could simply offer the police the same capability through different digital surveillance services.

Two separate questions arise from the geofence warrant question. Again, for purposes of this Essay we are focusing on Google's three-step geofence warrant that was at issue in the federal cases.[224] The first question asks whether, standing alone, Step One violates the rummaging test. The second question focuses on the full three-step process, asking whether the narrowing process in Step Two and Step Three allows the warrant to survive a rummaging test analysis. This section answers both questions together because they necessarily involve overlapping arguments and analysis.

i. Step One Searches

If police request a warrant to search all of Google's Sensorvault data is that Step One search arbitrary, overbroad, intrusive, and potentially embarrassing? Step One is a search against all collected data from all phones everywhere the phones were located.[225] The warrant is literally a general authorization of power to search against all phones at all locations within the collected dataset.[226] One way of looking at a Step One request is that it is a request to authorize police to search everything collected by Google and stored in the Sensorvault.[227] In many ways, the Step One search is worse than the Founders' general warrants because instead of authorizing a general power to search for anyone suspected of wrongdoing, it is an authorization to search against everyone's data even those not suspected of wrongdoing.[228] While the data is usually less revealing than a search of a home (only providing anonymous locations and the inferences therefrom), the

---

[222] *See, e.g.*, United States v. Chatrie, 590 F. Supp. 3d 901, 905 (E.D. Va. 2022) (holding a geofence warrant violated the Fourth Amendment); Sawyers, *supra* note 109, at 795 ("[I]nvestigators focused on Chatrie's because his movement patterns matched those of the robber, records showed that he had recently purchased a nine-millimeter G2C Taurus semiautomatic handgun (matching the description of the gun used in the robbery), and because he owned a car of the same color, make, and model in which, according to witnesses, the robber fled the scene.").

[223] In practice, police investigators request that a court follow Google's three-step warrant process, such that the practice includes judicial authority.

[224] *See* discussion *supra* Introduction.

[225] United States v. Chatrie, 590 F. Supp. 3d 901, 915 (E.D. Va. 2022).

[226] United States v. Smith, 110 F.4th 817, 837 (5th Cir. 2024).

[227] *See id.*

[228] *See id.* at 836, 838.

arbitrariness of the rummaging power granted is arguably greater.[229]

In addition, the overreach problem exists even with a warrant. Step One of a geofence warrant is necessarily overinclusive, capturing more people than just the suspect and capturing other activities of the suspect.[230] Again, the geofence warrant at the abortion clinic targeting one woman seeking services (perhaps illegal in her state), will also capture other people's private data. A particularly drawn warrant might avoid some of this overreach against innocents, but there is a real risk of a dragnet that is not easily avoided. As a practical matter, in almost every populated area, even a particularized warrant at Step One will be overbroad, collecting personal details (even if anonymized) from many others who should not have private facts revealed to the police. In other words, an initially justified search (based on a completed crime) will necessarily expand to cover other people and their private interests.

The intrusion factor with Step One is the same with or without a warrant, turning on the argument that location data is an intrusion onto privacy protected by the Fourth Amendment (under *Jones/Carpenter*).[231] While a warrant particularized to a specific time limits the aggregated nature of a person's travels, meetings, patterns etc., even with a warrant, many of the same privacy concerns arise.[232] For example, one hour of locational information around a cancer treatment clinic might be just as revealing as a week's worth of travel around a city. Many of the places we go—to a doctor, to a protest, to a social club—intrude on personal details that deserve some protection from government intrusion.

Finally, the potential embarrassment and exposure harm arises because of the knowledge that a geofence warrant could be obtained by the government. Once the technology exists and the police have potential access through a warrant, people know they can be tracked anywhere and everywhere.[233] The threat of revealing location information may discourage people from certain associational or political activities.[234] People choosing to go to a government protest might be concerned that their data could be used to embarrass them or expose them.[235] While a judge might sign off on a particular suspect, the reality is that those other individuals around the target will also be caught in the digital net and exposed.[236] Warrants can theoretically reduce the purely political or personal abuse of such surveillance, but the fear of abuse still exists. After all, the general warrants of the Founding Era were political in nature, and it was their threat of abuse that motivated

---

[229] *See id.* at 824–25, 837.
[230] *See id.* at 837.
[231] Carpenter, 585 U.S. at 309–10.
[232] *See* Ferguson, *supra* note 1, at 28 ("The more pieces of data collected and the more revealing those pieces are about a person's life, then the more likely the surveillance technology would raise Fourth Amendment concerns.").
[233] *See* Hartzog, Selinger & Gunawan, *supra* note 6, at 723 ("When lawmakers allow privacy nicks to become routine, repeated exposures can acclimate people to being vulnerable and watched in increasingly intimate ways.").
[234] *See* Solove, *supra* note 9 (explaining that erosions of privacy by the government may quash dissent by threatening, embarrassing, or discrediting critics).
[235] *See* Samantha Lai & Brooke Tanner, *Examining the Intersection of Data Privacy and Civil Rights*, BROOKINGS (July 18, 2022), https://www.brookings.edu/articles/examining-the-intersection-of-data-privacy-and-civil-rights/ [https://perma.cc/N2VR-XH9T] ("Law enforcement officials can collect or subpoena social media and location data, undermining the civil rights of activists and protesters.").
[236] *See generally* Solow-Niederman, *supra* note 113; Valentino-DeVries, *supra* note 208.

the drafting of the Fourth Amendment.[237]

Focused just on Step One, then, a geofence warrant raises the harms of rummaging.[238] If courts begin and end their analysis there, geofence warrants violate the rummaging test and thus the Fourth Amendment.[239] The power granted is too broad, too unlimited, and too revealing of private information that should be secured against police acquisition.[240]

ii. Steps Two & Three

The open question is whether steps Two and Three of the three-step warrant process save what is otherwise a rummaging problem. If—and it is an if—one can ignore the initial overbroad search against everybody and only focus on the narrowed results—then many of the rummaging concerns recede. Steps Two and Three are obvious attempts to limit the arbitrary and overreaching nature of government surveillance power. The latter two steps of the warrant process speak directly to the harms of rummaging and the power to search. The judge's role, the narrowing process, and the requirement of probable cause help avoid the worst harms of a rummaging power. An argument can be made that Steps Two and Three (if drafted carefully) offer the particularity demanded in the constitutional text to prevent rummaging. After all, the authority envisioned for law enforcement within the Fourth Amendment involves particularized warrants as a response to generalized rummaging power.[241] If you skip to the final result, the actual personal information revealed about the target is neither arbitrary nor overbroad. What is revealed is the whereabouts and identity of a single person (or perhaps a few people) at a particular date and time and through the judicial process after a crime has been committed.[242]

Yet, even within a narrowed search, there exist potential rummaging concerns. For some locations, even Step Two will be overbroad. For example, a warrant for the geolocational details for all the people near a bank during banking hours would be broad (necessarily collecting many incidental and innocent people).[243] It might not be a search against everyone's data in the Sensorvault but is a search against dozens of innocent people.[244] This was the theory of the *Chatrie* trial judge who criticized the warrant as being unparticularized.[245] That said, perhaps, a warrant for the geolocational details for all the people near a bank at the time of a midnight robbery when the bank was closed would be permissible because it would only identify culpable individuals. Put another way, in many cases, Step One and Two still create an expansive net that creates moderate rummaging harms, but not in all cases.

---

[237] *See* Laura K. Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181, 1300, 1317 (2016).
[238] *See* United States v. Smith, 82 F.4th 653, 660–61 (5th Cir. 2024) (geofence warrants are general warrants "categorically prohibited").
[239] *Id.*
[240] *See* Solow-Niederman, *supra* note 113.
[241] Carpenter, 585 U.S. at 303.
[242] *See* United States v. Chatrie, 590 F. Supp. 3d 901, 916 (E.D. Va. 2022).
[243] This overbreadth and lack of particularity has been the reasons two federal courts have struck down geofence warrants. *See* Chatrie, 590 F. Supp. 3d at 941. *See also* Smith, 110 F.4th at 840.
[244] Chatrie, 590 F. Supp. 3d at 909.
[245] *Id.* at 930.

Finally, there is the concern that while warrants do avoid the arbitrary and overbreadth rummaging harms, the power to expose and embarrass still exists simply from the potential of police access to the greater dataset. If citizens know that their location data is only a warrant away from exposure (via access to the collected data) this will chill activism, dissent, and enhance police power.[246] In addition, because what society considers "criminal" is contingent on political pressure, actions like obtaining an abortion, or protesting the police, can be criminalized with relative ease.[247] A lawful warrant is little protection when the laws are written to target certain groups.[248] True, perhaps, that fear focuses more on the politics of substantive laws than the restraints of government in enforcing those laws,[249] but the fear is real and speaks to the original concern in granting government such expansive surveillance powers.[250] The privacy fears of the Founding were political in nature.[251]

Again, in terms of a grant of power, it is hard not to see the rhetorical parallels between geofence warrants and the general warrants that gave rise to the Fourth Amendment. This reality is most easily seen if one just imagined that the FBI collected the Sensorvault data instead of Google. A government mandated database of every American's location (stored, searchable, and retained forever) would raise rummaging fears, even if the most particularized of warrants were required for access to that collected data, and even if the database was not accessed on a regular basis. The authorization to collect the data standing alone creates the rummaging fear.

If, as I have argued, the Fourth Amendment harm arises from a grant of governmental power to rummage through personal information for incriminating evidence, a particularized warrant only slightly alleviates that concern. If we are reliant on a warrant to protect us from everything-everywhere surveillance, significant new weight will need to be placed on redefining particularity in very specific ways. In addition, each of the rummaging harms will need to be considered and addressed in the warrant. Even then, we may not be comfortable with the result.

---

[246] Ana Pajar Blinder, *Don't (Tower) Dump on Freedom of Association: Protest Surveillance Under the First and Fourth Amendments*, 111 J. CRIM. L. & CRIMINOLOGY 961 (2021) (noting that law enforcement gains expanded power by using cell-phone location data to trace and identify individuals attending protests); Lai & Tanner, *supra* note 235.

[247] Alec Karakatsanis, *The Punishment Bureaucracy: How to Think About "Criminal Justice Reform,"* 128 YALE L.J.F. 848, 855–56 (2019) (detailing the political nature of determining what is a "crime").

[248] *See Warrantless Surveillance Under Section 702 of FISA*, ACLU, https://www.aclu.org/warrantless-surveillance-under-section-702-of-fisa [https://perma.cc/8U3Z-EX87] (last visited Oct. 3, 2025) (explaining that legal surveillance can easily be deployed against critics, activists, and minority communities).

[249] Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1936 (2013) (arguing that surveillance chills civil liberties and "distorts the power relationships between the watcher and the watched, enhancing the watcher's ability to blackmail, coerce, and discriminate against the people under its scrutiny").

[250] *See* Donohue, *The Original Fourth Amendment*, *supra* note 237, at 1183–84 (explaining that the Fourth Amendment reflected concern over unchecked surveillance by limiting searches to warrants with particularized descriptions).

[251] *Id.*

## CONCLUSION

This Symposium Essay exposes how new technologies and old-fashioned law both threaten to upend the Fourth Amendment's relevance in a digital age. Everything-everywhere surveillance technologies need a new doctrinal response. Applying the theory of digital rummaging to the problems revealed in everything-everywhere searches offers a new frame for analysis. While perhaps my new test is as fraught as the reasonable expectation of privacy test, the rummaging test offers other advantages in terms of application and analysis. As observed in the geofence analysis, the rummaging principles might offer a better fit for the technologies of the digital age.