No. 22-4489

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff–Appellee,

v.

OKELLO T. CHATRIE,

Defendant–Appellant.

On Appeal from the United States District Court
for the Eastern District of Virginia
Richmond Division (The Honorable M. Hannah Lauck)

BRIEF OF *AMICI CURIAE* TECHNOLOGY LAW AND POLICY CLINIC AT NEW YORK UNIVERSITY SCHOOL OF LAW & ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANT–APPELLANT

Jennifer Lynch
Andrew Crocker
Hannah Zhao
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
jlynch@eff.org

Jacob M. Karr
TECHNOLOGY LAW AND POLICY CLINIC
NEW YORK UNIVERSITY SCHOOL OF LAW
245 Sullivan Street, 5th Floor
New York, NY 10012
(212) 998-6042
jacob.karr@law.nyu.edu

Counsel for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

OTHER AUTHORITIES

INTEREST OF *AMICI CURIAE*[1]

The **Technology Law and Policy ("TLP") Clinic at New York University School of Law** is concerned with how technological advances drive legal, social, political, and economic change. Founded in 2012, the TLP Clinic represents a wide range of individuals, nonprofits, and consumer groups engaged with these questions from a public interest perspective. Through this work, the TLP Clinic has developed an interest in ensuring that settled law continues to serve the public good in the face of novel technologies. This case relates directly to that interest. The TLP Clinic submits this brief to assure the preservation of constitutional protections against unreasonable searches and seizures in the age of mass consumer data collection.

The **Electronic Frontier Foundation ("EFF")** is a non-profit organization that has worked for more than 30 years to ensure technology supports freedom, justice, and innovation for all people. With over 30,000 dues-paying members, EFF represents the interests of technology users in court cases and policy debates concerning the application of law in the digital age. EFF regularly participates as

---

[1] *Amici* submit this brief with the consent of all parties. Fed. R. App. P. 29(a)(2). No counsel for any party authored this brief in whole or in part, and no person or entity other than *amici* or their counsel made a monetary contribution intended to fund the preparation or submission of this brief. Fed. R. App. P. 29(a)(4)(E).

amicus, in this Court and other federal courts, in cases concerning Fourth Amendment rights in the digital age, including *Carpenter v. United States*, 138 S. Ct. 2206 (2018); *United States v. Jones*, 565 U.S. 400 (2012); *Leaders of a Beautiful Struggle v. Balt. Police Dep't*, 2 F.4th 330 (4th Cir. 2021); *United States v. Bosyk*, 933 F.3d 319 (4th Cir. 2019); and *United States v. Kolsuz*, 890 F.3d 133 (4th Cir. 2016).[2]

[2] *Amici* would like to thank Talya Nevins and Yanan Wang, students in the Fall 2022 TLP Clinic, for their significant contributions to this brief.

INTRODUCTION & SUMMARY OF ARGUMENT

The Framers crafted the Fourth Amendment to protect future Americans from the invasive general warrants that plagued them during the colonial era. These "writs of assistance" allowed British officers to indiscriminately rummage through homes without warning, instilling in people the fear that their intimate possessions might be combed through at any moment. Such indignities trampled on people's privacy and severely limited their freedoms, creating an antagonistic relationship between civilians and law enforcement. Geofence warrants are a contemporary incarnation of the general warrants that the Framers so reviled.

Like general warrants, geofence warrants grant police immense discretion to search people without probable cause. A geofence warrant like the one the district court rejected in this case authorizes police to require Google to produce a vast amount of its users' Location History data.[3] When making a geofence demand, police draw a line roughly around a geographic area and designate a time window—together comprising the "geofence." In response, Google turns over

[3] "Location History" is Google's official name for its most comprehensive, most detailed, and most user-specific location tracking tool. JA1330 (Op. 4). Google also has other location-tracking tools, but Location History is the tool best equipped to identify users present within a geofence, so it is generally the pool of data from which Google draws in response to geofence requests. JA1331–35 (Op. 5–9). "Location History" within this brief should be understood to refer solely to Google's service.

Location History data for every one of its users with Location History enabled who appeared within or near the geofence. In this way, geofence warrants unlawfully enable police to search people for no reason other than their "mere propinquity" to a crime. *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979); *see also* JA125 (Google Amicus 3).

Geofence warrants permit police to obtain private information about countless Google users in one fell swoop. As of 2018, Google had Location History data on 592 million individuals. Declaration of Emily Moseley ¶ 3, *People v. Dawes*, No. 19002022 (Cal. Super. Ct., S.F. Cnty. May 4, 2022) ("Moseley Declaration"). Location History data provides a granular portrait of these users' movements and whereabouts, revealing their "familial, political, professional, religious, and sexual associations" and allowing police to invade their reasonable expectation of privacy. *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018) (quoting *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)). In fact, an underappreciated feature of Google's geofence procedure is that it even permits police to obtain revealing data about individuals' movements outside the bounds of the original geofence—and to do so without further approval from a neutral magistrate.

The dangers of geofence warrants extend far beyond this case. This Court has been careful in recent cases to ensure, as the Supreme Court has repeatedly

instructed, that Fourth Amendment rights do not become overrun by the speed of technological advance. *See Leaders of a Beautiful Struggle v. Balt. Police Dep't*, 2 F.4th 330, 347 (4th Cir. 2021) (en banc); *see also Carpenter*, 138 S. Ct. at 2214. This novel dragnet technology poses a distinct threat to the Fourth Amendment's guaranteed realm of privacy, threatens First Amendment rights, and exposes poor and marginalized communities to further over-policing. The Constitution demands greater protection than geofence warrants can ever provide.

ARGUMENT

I. Geofence warrants are unconstitutional general warrants.

Geofence warrants function as digital dragnets that allow police to rummage through troves of people's highly sensitive data without any reason to suspect them of wrongdoing. Such expansive police discretion was a hallmark of colonial-era general warrants, which placed "the liberty of every man in the hands of every petty officer." *Stanford v. Texas*, 379 U.S. 476, 481 (1965). Upon receipt of a geofence warrant, Google generally follows a three-step compliance procedure that gives police immense discretion to pick and choose which Google users they subject to highly invasive location tracking.[4] And because geofence warrants target

[4] Approximately one third of Google's 1.5 billion users enable Location History. *See* Moseley Declaration ¶ 3. Other companies such as Amazon and Apple also retain users' location data, but Google is the only company publicly known to turn over such data in response to geofence warrants. Leila Barghouty, *What Are*

places, not people, they inevitably implicate innocent individuals who happen to be in the wrong place at the wrong time.

A. Geofence searches invade people's reasonable expectations of privacy in their Location History data.

The Location History data that is the object of a geofence warrant is highly sensitive and private. Indeed, it is even more detailed and revealing than cell-site location information ("CSLI"), which the Supreme Court held in *Carpenter* is protected by the Fourth Amendment.

In *Carpenter*, the Supreme Court recognized cell phone owners' reasonable expectations of privacy in CSLI because such a log of location information has the capacity to reveal the "privacies of life" with "encyclopedic" precision. 138 S. Ct. at 2216–18. Because most people carry cell phones at all times, the Court found that time-stamped cell phone location data can reveal intimate details about a person's life, such as his "familial, political, professional, religious, and sexual associations." *Id.* at 2217 (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)). Moreover, the Court explained, the collection of CSLI is more retroactive, cheap, efficient, and detailed than traditional surveillance tactics. *Id*. at 2218. These features were crucial to the *Carpenter* holding that CSLI requests

---

Geofence Warrants?, Markup (Sept. 1, 2020) https://themarkup.org/the-breakdown/2020/09/01/geofence-police-warrants-smartphone-location-data.

invade reasonable expectations of privacy. The Court noted that CSLI records allow the government, "with just the click of a button, . . . [to] access each carrier's deep repository of historical location information at practically no expense." *Id.* By holding that CSLI records are protected by the Fourth Amendment, the Court defended all cell phone owners from what they identified as a novel degree of "tireless and absolute surveillance." *Id.*

This Court recently decided that *Carpenter* compels the conclusion that government collection of location information is a Fourth Amendment search, even in contexts outside of CSLI. In *Leaders of a Beautiful Struggle v. Baltimore Police Department*, this Court—sitting en banc—held that a program of citywide aerial surveillance was a Fourth Amendment search because it allowed police to retroactively surveil anyone of their choosing in great detail. 2 F.4th 330. The surveillance was so broad and detailed that "'[w]hoever the suspect turn[ed] out to be,' they ha[d] 'effectively been tailed'" since the beginning of the program. *Id.* at 341 (quoting *Carpenter*, 138 S. Ct. at 2218). This Court reasoned that, like CSLI surveillance, Baltimore's aerial surveillance program invaded the right to privacy because it could reveal a person's intimate relationships and activities. *Id.* at 342. It concluded that "[b]ecause people's movements are so unique and habitual, it is almost always possible to identify people by observing even *just a few points* of their location history." *Id.* at 343 (emphasis added). Access to such data, this Court

explained, allows police to learn "otherwise 'unknowable' information" that is sensitive and private, and thus requires a warrant. *Id.* at 342 (quoting *Carpenter*, 138 S. Ct. at 2218).

Like the CSLI demands in *Carpenter* and the aerial surveillance in *Leaders of a Beautiful Struggle*—and unlike the kinds of tracking accomplished through traditional location surveillance techniques—geofence data is pulled from a preexisting database of cell phone users' past movements. This costs police nothing to collect, because Google has already collected it for them. As the district court explained, Google can provide police with information about a person's whereabouts for "almost every minute of every hour of every day." JA1379 (Op. 53). This means that the Government "has an almost unlimited pool from which to seek location data," such that the police's eventual suspect (and countless others) will have "'effectively been tailed' since they enabled Location History." JA1362 (Op. 36) (quoting *Leaders of a Beautiful Struggle*, 2 F.4th at 341). When police obtain Google's vast trove of historical location information, they gain access to a highly detailed, comprehensive, and otherwise private body of data about Google users' lives.

But geofence data is even more revealing than CSLI. Whereas CSLI can only estimate a person's location within "dozens to hundreds of city blocks," geofence data can pinpoint a person's location within twenty meters. JA132

(Google Amicus 10). Because geofence data is so detailed, even a few minutes of geofence data can show a person travel from her home to a church, from her church to a health clinic, or from her health clinic to a romantic rendezvous. At the district court level, defense counsel demonstrated how invasive this surveillance can be by presenting examples of three individuals who were followed to appointments and errands around town by the *Chatrie* geofence warrant. JA1358–59 (Op. 32–33). The defense's expert witness testified that he could identify these individuals based solely on their movements and other publicly available information. JA1358–59 (Op. 32–33). Such tracking easily exposes an individual's "associations and activities," violating her reasonable expectation of privacy. *See Leaders of a Beautiful Struggle*, 2 F.4th at 342–44; *see also Carpenter*, 138 S. Ct. at 2217.[5]

[5] Under *Carpenter*, the fact that Google users share their Location History data with Google, a third party, does not obviate the Fourth Amendment's warrant requirement for two independent reasons. First, the highly sensitive nature of Location History data undermines the third-party doctrine's assumption that people indicate a reduced privacy interest in information they share with third parties. *See* 138 S. Ct. at 2219. Second, people share Location History data with Google incident to the demands of modern life, contradicting the third-party doctrine's traditional assumption that when people voluntarily expose information to third parties, they assume the risk that those third parties will disclose that information to law enforcement. *See id.* at 2220; *see also* JA128–31 (Google Amicus 6–9) (user must enable Location History to use many Google services).

B. Geofence warrants bear all the hallmarks of general warrants.

Geofence warrants bear a striking resemblance to the general warrants that the Fourth Amendment was designed to eradicate. Geofence searches start with a broad sweep of Location History data, then give police discretion over which devices to further track and identify, all without additional judicial gatekeeping or scrutiny. Google's three-step compliance procedure evades judicial oversight, yet gives police access to data that is revealing enough to deduce a Google user's identity *even when it is anonymized*. *See infra* I.B.2; JA1359 (Op. 33). The revealing nature of Location History data and the unmitigated breadth of geofence demands mean that geofence warrants can lead police to wrongfully search and incriminate innocent passersby—and they have. *See infra* I.B.3.

1. The Fourth Amendment bars the use of general warrants.

The Framers drafted the Fourth Amendment against a backdrop of invasive authority at even the lowest levels of colonial law enforcement. Most notoriously, the legal process known as the "writ of assistance" gave British officers "blanket authority to search where they pleased"—an authority that Revolutionary advocate James Otis called "'the worst instrument of arbitrary power' . . . because they placed 'the liberty of every man in the hands of every petty officer.'" *Stanford*, 379 U.S. at 481. Much like geofence warrants, "[t]he general warrant specified only an offense . . . and left to the discretion of the executing officials the decision as to

which persons should be arrested and which places should be searched." *Steagald v. United States*, 451 U.S. 204, 220 (1981). The affronts of these searches, "which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity," directly contributed to the Founders' efforts to realize a new country. *Riley v. California*, 573 U.S. 373, 403 (2014).

It has therefore been long understood that overbroad warrants that give police too much discretion—in essence, general warrants—violate the Fourth Amendment's requirements for particularity and probable cause. *See, e.g.*, *Boyd v. United States*, 116 U.S. 616 (1886); *Andresen v. Maryland*, 427 U.S. 463 (1976); *Ashcroft v. al-Kidd*, 563 U.S. 731 (2011). The second clause of the Fourth Amendment emphasizes its purpose to protect against all general searches. "Since before the creation of our government, such searches have been deemed obnoxious to fundamental principles of liberty." *Go-Bart Importing Co. v. United States*, 282 U.S. 344, 357 (1931).

2. Geofence warrants facilitate expansive police discretion to invade individuals' privacy interests.

Google's geofence compliance policy eschews judicial supervision at every step. Under the policy, a broad initial approval is followed by case-by-case negotiations with the police, facilitating discretionary police access to highly revealing data. According to Google, its three-step procedure protects user privacy by providing only anonymized data at Step 1, then asking police to identify subsets

of "relevant" devices before providing additional data at Steps 2 and 3. JA134–36 (Google Amicus 12–14). But police can easily deanonymize Step 1 data, and they determine the level of detail at Steps 2 and 3 without further judicial oversight. Ultimately, corporate pledges of enhanced privacy are no substitute for the Fourth Amendment's guarantee of a neutral magistrate interposed between private information and the police.

i. Police can easily identify the subjects of anonymized Step 1 geofence data.

Even if a geofence warrant limited results exclusively to anonymous Step 1 data, the tool would still give police impermissible levels of discretion to infringe upon peoples' privacy. Once Step 1 geofence data is produced, police can easily deduce the identity of any individual whose device appears within the geofence because police have myriad other tools to identify the subjects of anonymous geofence data.

As an initial matter, this Court recently explained that, "because people's movements are so unique and habitual, it is almost always possible to identify people by observing even just a few points of their location history." *Leaders of a Beautiful Struggle*, 2 F.4th at 343. But police can also obtain nominally anonymous devices' associated subscriber information via grand jury subpoena, rendering Step 2 and Step 3 of Google's compliance process entirely superfluous. *See In re Search of Info. Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 750 (N.D.

Ill. 2020) ("*Illinois Geofence Case I*") (finding the Step 1 data alone allows law enforcement "to identify the users by subpoena, based entirely upon its own discretion"). Even in the rare case where a judge *requires* police to seek judicial approval before requesting subscriber information from Google, *see, e.g.*, *In re Search of Info. That Is Stored at the Premises Controlled by Google LLC*, 579 F. Supp. 3d 62, 90 (D.D.C. 2021), police can identify a device's owner by cross-referencing the device's Location History with publicly available information such as real estate, tax, employment, or social media records. JA1357–59 (Op. 31–32) (describing expert witness testimony about how law enforcement can deanonymize even a tiny amount of geofence data based on publicly available records). Police can also identify "the people behind the pixels" by combining Step 1 data with information gleaned from other surveillance tactics, such as security camera footage or automated license plate readers. *Leaders of a Beautiful Struggle*, 2 F.4th at 343–44 (explaining how police can deduce peoples' identities by combining information developed through aerial surveillance, camera networks, license plate readers, and gunshot detectors).

Geofencing thus facilitates unchecked police access to broad swaths of highly sensitive personal information in violation of the Fourth Amendment. In *Leaders of a Beautiful Struggle*, this Court found that the Fourth Amendment protects anonymous location data when, combined with other information or

techniques, it enables police to deduce someone's identity. *Id.* at 345–46. Referring to broad aerial surveillance of Baltimore that enabled police to track the movements of anyone near the scene of a crime, this Court held that "[a]llowing the police to wield this power unchecked is anathema to the values enshrined in our Fourth Amendment." *Id.* at 347. Just as the Constitution prevents police from obtaining outright such highly sensitive, personally revealing data, so too the Constitution prevents police from obtaining an anonymized copy of that data when they can deanonymize it at their discretion. *See Illinois Geofence Case I*, 481 F. Supp. 3d at 749 (rejecting a geofence warrant that would produce only anonymized data on the grounds that the Government could still subpoena identifying information, and stating that "[t]he principle that the government may not accomplish indirectly what it may not do directly is well-settled in the jurisprudence of constitutional rights").

ii. Google's three-step procedure is a flexible, negotiable, and merely internal guideline that is no substitute for independent judicial supervision.

Google's three-step geofence procedure, which the company claims protects user privacy, in fact gives law enforcement extraordinary discretion to access highly sensitive data without judicial supervision. In particular, Step 2 presents police with "contextual" data for a subset of devices—selected by police without judicial oversight—that extends beyond the warrant's physical and time

constraints. JA1346–47 (Op. 20–21). Records the government obtains during Step 2 are "geographically unlimited," JA1358 (Op. 32), and thus exceed the judicially-approved bounds of the warranted geofence. And at Step 3, Google produces identifying subscriber information for "devices of interest," again selected by the police without judicial oversight. JA1346 (Op. 20).

The lack of judicial supervision over this so-called "narrowing" process improperly cedes the neutral magistrate's oversight role to Google's compliance officers and "fails to curtail or define the agents' discretion in any meaningful way." *In re Search of: Info. Stored at Premises Controlled by Google, as Further Described in Attachment A*, No. 20 M 297, 2020 WL 5491763, at *6 (N.D. Ill. July 8, 2020); *see also In re Search of Info. Stored at the Premises Controlled by Google*, No. KM-2022-79, 2022 Va. Cir. LEXIS 12, at *24 (Va. Cir. Ct. Feb. 24, 2022) (finding that Step 2's "[e]nlarged zones circumvent judicial oversight"). All of this contravenes the purpose of the Fourth Amendment's warrant requirement, which serves "to interpose a neutral magistrate between the citizen and the law enforcement officer." *Nat'l Treasury Emps. Union v. Von Raab*, 489 U.S. 656, 667 (1989).

The variability of Google's compliance practices further attests to the three-step procedure's unreliability as a guardrail against police discretion. Even Google presents the three-step procedure as a policy that is "typically" followed, not

stringently observed. JA134 (Google Amicus 12). Indeed, the company negotiates different procedures with police from case to case. *Compare, e.g.*, JA1377 (Op. 51) (describing how one Google specialist insisted that police engage in Step 2 narrowing), *with, e.g.*, *In re Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d 345, 353 (N.D. Ill. 2020) ("*Illinois Geofence Case II*") (describing a procedure that skipped Step 2 altogether). Ultimately, this vacillating and negotiable corporate procedure is no substitute for the Fourth Amendment's protections against unfettered police discretion. *See Illinois Geofence Case II*, 497 F. Supp. 3d at 362 (stating that the narrowing procedure "should not be viewed as in any way supporting the constitutionality of the warrant").

3. Geofence warrants can wrongfully search and incriminate people for no reason other than their proximity to a crime.

Since geofence warrants target places, not people, they naturally implicate individuals who are lawfully going about their private business in areas where alleged crimes may contemporaneously occur. This puts geofence warrants in direct tension with the Supreme Court's holding that "a person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person." *Ybarra v. Illinois*, 444 U.S. at 91.

"The Fourth and Fourteenth Amendments protect the 'legitimate expectations of privacy' of persons, not places." *Id.*

Geofence searches seriously threaten the privacy principle expressed in *Ybarra*. In that case, police officers patted down each of the nine to thirteen customers at a tavern where drugs were suspected to be in someone's possession. *Id.* at 88. The Court held that the search violated the "constitutional protections possessed individually by the tavern's customers" because each tavern patron was owed their own protection against an unreasonable search or seizure that was "separate and distinct" from the Fourth Amendment rights possessed by the suspects. *Id.* at 91. While the search warrant permitted officers to search the premises and the suspect, it gave them *no* authority to search other customers who happened to be at the tavern at the same time. *Id.* at 92. "'[O]pen-ended' or 'general' warrants are constitutionally prohibited. . . . It follows that a warrant to search a place cannot normally be construed to authorize a search of each individual in that place." *Id.* at 92 n.4.

A geofence warrant does precisely what the *Ybarra* Court declared unlawful: it allows police to search the Location History data of each individual in—or even just near—the police's place of interest. Google itself noted that geofence searches seek to identify a broad group of users "even though law enforcement has no

particularized basis to suspect that all those users played a role in, or possess any information relevant to, the crime being investigated." JA125 (Google Amicus 3).

To make matters worse, geofence warrants give police the advantage of technology that effectively permits them to travel back in time. The Court in *Ybarra* was concerned that police searched all the customers in the tavern at the time of the suspected crime, but at least the police also had to be physically present. A geofence search has no such limitation. This search can be executed at any time, at the police's leisure.

Furthermore, a geofence search often implicates far more people than the nine to thirteen customers whose Fourth Amendment rights were violated in *Ybarra*. For instance, when the Bureau of Alcohol, Tobacco, Firearms and Explosives obtained geofence warrants for one investigation in Milwaukee, they drew an area covering three hectares, more than seven football fields. Thomas Brewster, *Google Hands Feds 1,500 Phone Locations in Unprecedented 'Geofence' Search*, Forbes (Dec. 11, 2019), https://www.forbes.com/sites/thomasbrewster/2019/12/11/google-gives-feds-1500-leads-to-arsonist-smartphones-in-unprecedented-geofence-search. In response, Google provided location data for nearly 1,500 users. *Id.*

As a result, people are regularly subjected to geofence searches simply for being in the wrong place at the wrong time—and the resulting harms can be

serious. Though geofence warrants are relatively novel, there are already devastating instances of wrongful incrimination facilitated by their unprecedented breadth.

For example, Jorge Molina became the lead suspect in a murder investigation after a geofence warrant erroneously placed him near the site of a Phoenix-area shooting. 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. Molina was not, in fact, at the scene of the crime. He had signed into his Google account on several other phones, including one that was linked to a subsequent suspect. Meg O'Connor, *Avondale Man Sues After Google Data Leads to Wrongful Arrest for Murder*, Phoenix New Times (Jan. 16, 2020), https://www.phoenixnewtimes.com/news/google-geofence-location-data-avondale-wrongful-arrest-molina-gaeta-11426374. Even so, Molina sat in jail for six days while police issued a press release and mugshot to dozens of media outlets, naming him as the sole and primary suspect. Compl. ¶ 70, *Molina v. Avondale*, No. 2019-015311 (D. Ariz. filed Feb. 18, 2020), ECF No. 1.

Similarly, Zachary McCoy, a Florida cyclist, lost thousands of dollars in attorney's fees spent to clear his name after a geofence search wrongly linked him to a burglary in his neighborhood. *See* Jon Schuppe, *Google Tracked His Bike Ride*

Past a Burglarized Home. That Made Him a Suspect, NBC News (Mar. 7, 2020), https://www.nbcnews.com/news/us-news/google-tracked-his-bike-ride-past-burglarized-home-made-him-n1151761.

The harms that can flow from geofence searches are only proliferating. In states that criminalized abortion after the Supreme Court's decision in *Dobbs v. Jackson Women's Health Org.*, 143 S. Ct. 2228 (2022), police could obtain geofence warrants for medical clinics suspected of providing or assisting abortions, which in many cases are the same places that continue to provide critical, still-legal reproductive care. *See* Alfred Ng, *'A Uniquely Dangerous Tool': How Google's Data Can Help States Track Abortions*, Politico (July 18, 2022), https://www.politico.com/news/2022/07/18/google-data-states-track-abortions-00045906; Charlotte Scott, *Geofence Warrants Are 'Slippery Slope' in Texas*, Spectrum News (July 20, 2022), https://spectrumlocalnews.com/tx/south-texas-el-paso/politics/2022/07/21/geofence-warrants-are--slippery-slope--in-texas. This means that someone visiting a clinic for a routine gynecological exam, breast cancer screening, or STI test could become the subject of a criminal investigation into illegal abortions, simply because they visited a reproductive health facility.

Each time a geofence warrant is executed, numerous innocent people may have their private Location History data exposed to police—or worse, be wrongfully incriminated like Molina or McCoy. The indiscriminate nature of these

searches, paired with the wide discretion they grant to law enforcement, make more wrongful arrests a virtual inevitability.

II. Geofence warrants are uniquely dangerous surveillance tools.

In addition to functioning as unconstitutional general warrants, geofence warrants present unique threats to the Fourth Amendment's guaranteed realm of privacy, place First Amendment rights in peril, and threaten to compound the over-policing of poor and marginalized communities.

A. The broad scope and detailed nature of geofence searches threaten the balance between privacy interests and government power.

Courts must exercise great caution and scrutiny where new technologies significantly impact the privacy guaranteed to citizens at the time of the Founding. *See Kyllo v. United States*, 533 U.S. 27, 34 (2001). The problem with geofence warrants is not merely that such tools were inconceivable when the Fourth Amendment was written, but that the level of insight such searches give law enforcement into the "privacies of life" entirely diverges from the balance between privacy interests and government power that the Fourth Amendment envisioned. *Boyd v. United States*, 116 U.S. 616, 630 (1886); *see Riley*, 573 U.S. at 407 (Alito, J., concurring) (explaining that the capacity of cellphones to store a large amount of information, "some highly personal, that no person would ever have had on his

person in hard-copy . . . calls for a new balancing of law enforcement and privacy interests"); *see also supra* I.A.

First, geofence searches are distinguishable from other digital surveillance tools because of their sheer breadth. They target a time and place rather than a suspect or person of interest, and at Step 2 of Google's compliance process, the government can expand its view of users' Location History records beyond the warranted radius and time frame. *See supra* I.B.2.ii. Executing a geofence search, therefore, is not comparable to viewing CCTV footage, looking through a particular suspect's cellphone, or tracking a person's movements through CSLI. Rather, geofence searches are a high-tech dragnet. *See Carpenter*, 138 S. Ct. at 2215 (noting that the Supreme Court distinguishes between rudimentary, targeted tracking and "more sweeping modes of surveillance" when considering Fourth Amendment constitutionality); *Kyllo*, 533 U.S. at 36 (finding that to protect citizens from "advancing technology," the Court must take into account "more sophisticated systems that are already in use or in development").

Second, geofence searches allow law enforcement to retrospectively surveil many people's movements in fine detail. As discussed above, the level of precision dangerously surpasses that of CSLI, with which the Court took issue in *Carpenter*. *Supra* I.A. Geofencing allows the government to reconstruct a "'detailed and comprehensive record [of the user's] movements,' even if only for an hour or

two—something that law enforcement would not be able to do using traditional investigative methods." JA146 (Google Amicus 24) (quoting *Carpenter*, 138 S. Ct. at 2217).

B. Geofence searches are inimical to democratic ideals because they endanger First Amendment rights.

Geofence searches threaten to create in citizens a sense of constant surveillance that alters their relationship with the government "in a way that is inimical to democratic society." *United States v. Jones*, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring). In recent years, courts have considered this awareness a particular danger of GPS technology, which "generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *Id.* at 415. Geofence searches present the same concerns, only magnified. *See supra* I.A. As a result, geofence searches threaten to chill the exercise of First Amendment rights: the freedoms of speech, assembly, and religion.

For example, the use of geofence warrants can chill lawful protest by rendering anyone at a public demonstration subject to arrest for other attendees' crimes. In August 2020, investigators sought six geofence warrants to investigate attempted arsons that took place in Kenosha, Wisconsin, during mass protests after the police shooting of Jacob Blake, a 29-year-old Black man. *See* Russell Brandom, *How Police Laid Down a Geofence Dragnet for Kenosha Protesters*,

Verge (Aug. 30, 2021), https://www.theverge.com/22644965/kenosha-protests-geofence-warrants-atf-android-data-police-jacob-blake. The search exposed the Location History of hundreds of peaceful protesters who passed through the damaged areas during one of the busiest nights of the demonstrations. *See* Julie Bosman & Sarah Mervosh, *Wisconsin Reels After Police Shooting and Second Night of Protests*, N.Y. Times (Sept. 10, 2020), https://www.nytimes.com/2020/08/24/us/kenosha-police-shooting.html. Just a few months earlier, police also used a geofence warrant to obtain data on protesters in the aftermath of George Floyd's murder in Minneapolis, on the premise of investigating an arson at a nearby car parts retailer. *See* Zack Whittaker, *Minneapolis Police Tapped Google to Identify George Floyd Protesters*, TechCrunch (Feb. 6, 2021), https://techcrunch.com/2021/02/06/minneapolis-protests-geofence-warrant. Among those exposed by that warrant was Said Abdullahi, a Minneapolis resident who received an email from Google notifying him that his information would be given to police. *Id.* Abdullahi was not involved in the violence and had only been in the area to take videos of the protests. *Id.*

The expansive scope and police discretion that characterize geofence searches can likewise imperil freedom of religion. Surveillance of religious communities can chill their ability to practice their faith freely and openly. Indeed, religious minorities have always had much to fear from state surveillance. *See*

Alvaro Bedoya, Introduction to *The Color of Surveillance: Government Monitoring of American Religious Minorities* at Georgetown University Law Center Color of Surveillance Symposium at 06:32 (Nov. 7, 2019) (referring to the "old and ugly idea . . . that religious minorities are different and dangerous, and that they need to be investigated"). In the years following the September 11 attacks, the New York Police Department ("NYPD") instituted a surveillance program aimed at Muslims. *See, e.g.*, Adam Goldman & Matt Apuzzo, *With Cameras, Informants, NYPD Eyed Mosques*, Associated Press (Feb. 23, 2012), https://www.ap.org/ap-in-the-news/2012/with-cameras-informants-nypd-eyed-mosques. As with geofence searches, the NYPD began by zoning in on specific neighborhoods and locales, not individuals. Once community members became aware of this surveillance, many were scared to speak out against it or even to publicly align themselves with their faith. *See* Creating Law Enforcement Accountability & Responsibility et al., *Mapping Muslims: NYPD Spying and its Impact on American Muslims* (2013), https://www.law.cuny.edu/wp-content/uploads/page-assets/academics/clinics/immigration/clear/Mapping-Muslims.pdf. Forced disclosure of membership can chill association, even if there is no disclosure to the general public. *See, e.g.*, *Ams. for Prosperity Found. v. Bonta*, 141 S. Ct. 2373, 2388 (2021) (finding that California's donor disclosure requirement created an unnecessary risk of chilling association by

"indiscriminately sweeping up the information of *every* major donor"). The breadth of geofence searches is poised to exacerbate the impact of such government monitoring. Indeed, in this case, the warrant encircled the Journey Christian Church, which offers round-the-clock activities to its 1,700 congregants. JA1348 (Op. 22).

As Justice Sotomayor warned in *Jones*, "[a]wareness that the government may be watching chills associational and expressive freedoms." *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring). In a democratic society, individuals must be able to go about their lives without fear that their daily, constitutionally protected choices might at any point place them in the crosshairs of police scrutiny. The use of geofence searches incites precisely this fear.

C. Geofence warrants will exacerbate the over-policing of poor and marginalized communities because they indiscriminately surveil people near targeted areas.

Because geofence warrants indiscriminately subject everyone in the vicinity of an investigated crime to highly revealing surveillance, *see supra* I, their use threatens to strip people who live and work in over-policed neighborhoods of any ability to keep their lives private from the government. Even specific geofences authorized by scrupulous judges will intensify the routine surveillance of poor and marginalized communities, especially in densely populated urban areas.

Poor communities are already subjected to privacy invasions that would cause uproar if replicated in affluent areas. As this Court recently explained, "[t]oo often today, liberty from governmental intrusion can be taken for granted in some neighborhoods, while others experience the Fourth Amendment as a system of surveillance, social control, and violence, not as a constitutional boundary that protects them from unreasonable searches and seizures." *Leaders of a Beautiful Struggle*, 2 F.4th at 348 (quotation marks omitted). Along those lines, one scholar has documented how poor people's privacy rights are systemically diminished and devalued by the law, reflecting a biased presumption that poor people's "enjoyment of privacy will realize no value or a negative value." Khiara M. Bridges, *The Poverty of Privacy Rights* 12 (2017).

Geofencing will intensify this reality. As police increasingly use geofence warrants to investigate crimes and even low-level infractions, it is not unrealistic to expect that highly policed neighborhoods could become blanketed with geofence surveillance that reveals every resident's nearly every movement. *See* JA125 (Google Amicus 3) (stating that Google saw a 7,500% increase in geofence data requests between 2017 and 2019); Jeremy Harris, *Layton Police Use Controversial "Geo-Fence" Warrants to Investigate Property Crimes*, KUTV (May 17, 2022), https://kutv.com/news/2news-investigates/layton-police-use-controversial-geo-fence-warrants-to-investigate-property-crimes (documenting how geofence

warrants are increasingly used to police petty crime). As this Court noted in *Leaders of a Beautiful Struggle*, marginalized communities bear the brunt of novel surveillance techniques through over-policing, inflated arrest rates, and increased police violence. 2 F.4th at 347–48. The argument that increased surveillance benefits these communities by reducing crime controverts the "humanity, dignity, and lived experience" of people whose loved ones and neighbors are policed and incarcerated at disproportionate rates. *Id.* at 348 (Gregory, C.J., concurring). Permitting police to further surveil these neighborhoods through geofencing's uniquely broad, retrospective, and highly revealing capabilities will contribute to the mass criminalization of communities with reduced political power. Geofence warrants will thus further strip the Fourth Amendment of its capacity to "remain a bastion of liberty in a digitizing world." *Id*. at 348; *see also United States v. Curry*, 965 F.3d 313, 337 (4th Cir. 2020) (en banc) (Wynn, J., concurring) ("Either people who happen to live in high crime areas are subject to a lower degree of Fourth Amendment protection, or any time a gun is fired in a populated area, the police may conduct suspicionless and wholly discretionary stops of all individuals in the vicinity. The former conclusion is untenable, as we may not relegate individuals who live in high-crime areas to second-class citizen status. The latter conclusion suggests that Fourth Amendment protections are lessened for those who own firearms or happen to be within earshot of gunfire.")

This dynamic has grim consequences for various traditionally special Fourth Amendment rights. In densely populated areas, geofence warrants will threaten the traditional right of privacy in one's home by ensnaring apartment-dwellers who live in highly policed areas. The information revealed by geofence data easily exposes to police who lives in a particular building, when they spend time at home, and whom else they invite over. JA1357 (Op. 31). But every person is entitled to keep that information private, no matter how many crimes the police investigate in their neighborhood. *See United States v. U.S. Dist. Ct.*, 407 U.S. 297, 313 (1972) ("[P]hysical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed.").

Similarly, geofence data allows police to observe which people receive medical treatment at a particular location. JA1358 (Op. 32) (describing how the *Chatrie* geofence observed a bystander at a 35-minute hospital visit). Medical information may be especially sensitive because of its association with criminalized or marginalized groups—for example, addiction treatment with illegal drug use, or HIV/AIDS screening with sex work or LGBTQ+ identity. *See* Trevor Hoppe, *Punishing Disease: HIV and the Criminalization of Sickness* 101–31 (2017) (describing how fear of homosexuality and sex work drove HIV criminalization laws). And geofence data can also reveal sensitive information

about one's religion. JA1348 (Op. 22) (finding that the *Chatrie* warrant encircled the Journey Christian Church).

If geofencing becomes a routine form of surveillance in over-policed areas, people may be afraid to be in their own homes, to seek sensitive medical treatment at clinics in certain neighborhoods, or to visit the local mosque or temple, for fear that the visit will be captured by geofence warrants targeting nearby crimes. Every person should be free to live an apartment, consult a doctor, or attend religious services of their own choosing without exposing that information to the police. Geofencing will disproportionately reduce such choices for marginalized groups with historically justified reasons to fear police surveillance.

CONCLUSION

For the reasons above, the Court should hold that this geofence warrant is an unconstitutional general warrant.

Dated: January 27, 2023

Respectfully submitted,

/s/ Jacob M. Karr

Jacob M. Karr
TECHNOLOGY LAW AND POLICY CLINIC
NEW YORK UNIVERSITY SCHOOL OF LAW
245 Sullivan Street, 5th Floor
New York, NY 10012
(212) 998-6042
jacob.karr@law.nyu.edu

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE

I certify that this brief complies with the type-volume limitation of Fed. R. App. P. 29(a)(5) and 32(a)(7). According to the word-processing system used to prepare this brief, it contains 6,471 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f).

I further certify that this brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type-style requirements of Fed. R. App. P. 32(a)(6) because it has been prepared in a proportionally spaced typeface, Times New Roman, in 14-point font.

Dated: January 27, 2023

/s/ Jacob M. Karr
Jacob M. Karr

Counsel for Amici Curiae

CERTIFICATE OF SERVICE

I certify that I electronically filed the foregoing on January 27, 2023 with the Clerk of the U.S. Court of Appeals for the Fourth Circuit via the Court's CM/ECF system.

I further certify that counsel for all parties will be electronically served via the Court's CM/ECF system.

Dated: January 27, 2023

/s/ Jacob M. Karr
Jacob M. Karr

Counsel for Amici Curiae

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

DISCLOSURE STATEMENT

- In civil, agency, bankruptcy, and mandamus cases, a disclosure statement must be filed by **all** parties, with the following exceptions: (1) the United States is not required to file a disclosure statement; (2) an indigent party is not required to file a disclosure statement; and (3) a state or local government is not required to file a disclosure statement in pro se cases. (All parties to the action in the district court are considered parties to a mandamus case.)
- In criminal and post-conviction cases, a corporate defendant must file a disclosure statement.
- In criminal cases, the United States must file a disclosure statement if there was an organizational victim of the alleged criminal activity. (See question 7.)
- Any corporate amicus curiae must file a disclosure statement.
- Counsel has a continuing duty to update the disclosure statement.

No. 22-4489 Caption: United States of America v. Okello T. Chatrie

Pursuant to FRAP 26.1 and Local Rule 26.1,

Technology Law and Policy Clinic at New York University School of Law (Washington Square Legal Services, Inc.) & Electronic Frontier Foundation
(name of party/amicus)

who is Amici Curiae, makes the following disclosure:
(appellant/appellee/petitioner/respondent/amicus/intervenor)

1. Is party/amicus a publicly held corporation or other publicly held entity? ☐ YES ☑ NO

2. Does party/amicus have any parent corporations? ☐ YES ☑ NO
If yes, identify all parent corporations, including all generations of parent corporations:

3. Is 10% or more of the stock of a party/amicus owned by a publicly held corporation or other publicly held entity? ☐ YES ☑ NO
If yes, identify all such owners:

4. Is there any other publicly held corporation or other publicly held entity that has a direct financial interest in the outcome of the litigation? ☐YES ☑NO
If yes, identify entity and nature of interest:

5. Is party a trade association? (amici curiae do not complete this question) ☐YES ☑NO
If yes, identify any publicly held member whose stock or equity value could be affected substantially by the outcome of the proceeding or whose claims the trade association is pursuing in a representative capacity, or state that there is no such member:

6. Does this case arise out of a bankruptcy proceeding? ☐YES ☑NO
If yes, the debtor, the trustee, or the appellant (if neither the debtor nor the trustee is a party) must list (1) the members of any creditors' committee, (2) each debtor (if not in the caption), and (3) if a debtor is a corporation, the parent corporation and any publicly held corporation that owns 10% or more of the stock of the debtor.

7. Is this a criminal case in which there was an organizational victim? ☑YES ☐NO
If yes, the United States, absent good cause shown, must list (1) each organizational victim of the criminal activity and (2) if an organizational victim is a corporation, the parent corporation and any publicly held corporation that owns 10% or more of the stock of victim, to the extent that information can be obtained through due diligence.

Signature: /s/ Jacob M. Karr Date: January 27, 2023

Counsel for: Amici Curiae

Print to PDF for Filing

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

APPEARANCE OF COUNSEL FORM

BAR ADMISSION & ECF REGISTRATION: If you have not been admitted to practice before the Fourth Circuit, you must complete and return an Application for Admission before filing this form. If you were admitted to practice under a different name than you are now using, you must include your former name when completing this form so that we can locate you on the attorney roll. Electronic filing by counsel is required in all Fourth Circuit cases. If you have not registered as a Fourth Circuit ECF Filer, please complete the required steps at Register for eFiling.

THE CLERK WILL ENTER MY APPEARANCE IN APPEAL NO. 22-4489 as

☐ Retained ☐ Court-appointed(CJA) ☐ CJA associate ☐ Court-assigned(non-CJA) ☐ Federal Defender

☑ Pro Bono ☐ Government

COUNSEL FOR: Technology Law and Policy Clinic at New York University School of Law & Electronic Frontier Foundation as the
(party name)

☐ appellant(s) ☐ appellee(s) ☐ petitioner(s) ☐ respondent(s) ☑ amicus curiae ☐ intervenor(s) ☐ movant(s)

/s/ Jacob M. Karr
(signature)

Please compare your information below with your information on PACER. Any updates or changes must be made through PACER's Manage My Account.

Jacob M. Karr
Name (printed or typed)

(212) 998-6042
Voice Phone

NYU Technology Law and Policy Clinic
Firm Name (if applicable)

Fax Number

245 Sullivan Street, 5th Floor

New York, NY 10012
Address

jacob.karr@law.nyu.edu
E-mail address (print or type)

CERTIFICATE OF SERVICE *(required for parties served outside CM/ECF)*: I certify that this document was served on _____ by ☐ personal delivery; ☐ mail; ☐ third-party commercial carrier; or ☐ email (with written consent) on the following persons at the addresses or email addresses shown:

Signature

Date