No. 25-112

IN THE

Supreme Court of the United States

OKELLO T. CHATRIE, *Petitioner*

v.

UNITED STATES, *Respondent*

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

BRIEF FOR THE INNOCENCE PROJECT AND THE CENTER ON RACE, INEQUALITY, AND THE LAW AT NEW YORK UNIVERSITY SCHOOL OF LAW AS *AMICI CURIAE* IN SUPPORT OF PETITIONER

M. CHRIS FABRICANT
MATTHEW A. WASSERMAN
INNOCENCE PROJECT, INC.
40 Worth Street, Suite 701
New York, NY 10013

JAMES C. DUGAN
Counsel of Record
FERDINAND G. SUBA JR.
CORINNE D. CATHCART
WILLKIE FARR
& GALLAGHER LLP
787 Seventh Avenue
New York, NY 10019
(212) 728-8000
jdugan@willkie.com

Counsel for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Other Authorities

INTERESTS OF *AMICI CURIAE*[1]

The Innocence Project (the "Project") is a nonprofit organization dedicated primarily to providing pro bono legal and related investigative services to innocent people wrongfully convicted of crimes. To date, the Project has freed or exonerated 255 innocent individuals, who were wrongfully incarcerated for a total of 4,078 years.

In addition to fighting for the exoneration of those already wrongfully convicted, the Project also seeks to prevent future injustices through reform initiatives that improve accuracy in our criminal legal system. Because wrongful convictions destroy lives and subvert justice, the Project's work serves as an important check on the power of the state over people accused of crimes and helps to ensure a safer and more just society.

Drawing on the lessons from studying cases where innocent people were convicted, the Project advocates reforms designed to enhance the truth-seeking functions of the criminal process, ensure the reliability of evidence, and prevent future wrongful convictions. In recent years, harmful surveillance and investigative technologies have increased the risk of wrongful conviction by eroding the presumption of

---

[1] Pursuant to Supreme Court Rule 37.6, counsel for *amici* certifies that no counsel for a party authored this brief in whole or in part, and no party or its counsel made a monetary contribution intended to fund the preparation or submission of this brief. No person other than *amici* or its counsel made a monetary contribution to this brief's preparation or submission.

innocence and inducing investigators to focus on individuals identified through opaque machine processes—even in the presence of exculpatory evidence. Dragnet technologies like geofence warrants impose an unreasonable burden of suspicion on innocent individuals and create an unacceptable risk of wrongful arrests and convictions.

The Center on Race, Inequality, and the Law at New York University School of Law[2] (the "Center") confronts and upends the array of American laws, policies, and practices that lead to racial oppression and injustice. By illuminating the history and impact of racism on law and society, the Center is able to find solutions to the injustice it causes and take action to advance freedom and fairness, for everyone.

The Center recognizes that machines and algorithms now make decisions about who gets hired, who gets housing, who receives public benefits, and who is policed, often through opaque automated systems that impose life-altering judgments. These tools, presented as neutral and efficient, frequently reproduce racial bias, operate without transparency, and leave people with little recourse when harm occurs. The Center challenges and works to dismantle these harmful systems through litigation, policy advocacy, research, and collaborations that focus on the racial justice concerns at the intersection of technology and power. The Center supports efforts to

[2] The Center on Race, Inequality, and the Law is affiliated with New York University School of Law, but does not purport to present the school's institutional views, if any, in this *amicus curiae* brief or otherwise.

ensure that actors in the criminal legal system are held accountable when they exercise discretion in ways that undermine the fair administration of justice. The Center aims not only to stop technological harm, but to reimagine how technology can advance racial justice, institutional accountability, and community power.

Amici curiae share a compelling interest in mitigating the risks of wrongful conviction. Accordingly, the undersigned submit this brief to urge the Court to hold that the court below erred in finding that the execution of the geofence warrant did not violate the Fourth Amendment.

SUMMARY OF ARGUMENT

Google Location History data obtained via geofence warrants is fraught with reliability problems, and such warrants have already led to wrongful arrests. This is no surprise, as geofence warrants seek data from all Location History-enabled devices located in a certain geographic area at a certain time. Unlike traditional warrants, geofence warrants are not dependent on evidence establishing probable cause. Instead, by design, they ensnare innocent people who happened to have a device near the time and place of a suspected crime. Geofence warrants are dangerous digital dragnets that capitalize on the ubiquity of data gathering by companies like Google at the expense of innocent people.

Beyond subverting Fourth Amendment rights by casting suspicion on persons in the absence of probable cause, geofence warrants may also fail to identify the actual perpetrator of the crime. Geofence warrants depend on the data they capture via smartphones or other devices that have a location history feature enabled. For crimes committed by persons who do not have that feature enabled or are not carrying such devices at all, geofence warrants are essentially useless. In effect, geofence warrants generate false leads and cast suspicion on innocent people while turning a blind eye to perpetrators who may be incidentally or purposefully evading location history tracking.

Geofence warrants also worsen law enforcement's susceptibility to cognitive biases like tunnel vision, confirmation bias, and automation bias, which have been known to contribute to wrongful convictions. As law enforcement entities seek to use innovative technology to improve their ability to investigate and apprehend criminals, they also risk becoming overly reliant on such technology despite its shortcomings. Although geofence warrants may be attractive to law enforcement due to their purportedly objective nature—the data is collected from a given geographic area in a given time frame with no regard to individualized suspicion—these same characteristics can mask flaws in the data; encourage investigative tunnel vision, priming police to selectively interpret other evidence to confirm *what* and *who* geofence data has already led them to suspect; and produce

automation bias, leading police to privilege location history data over exculpatory analog evidence.

Finally, geofence warrants are an unreliable investigative tool. The location data tends to be imprecise, and at least one empirical study found that Google's confidence intervals may at times overstate the data's accuracy. Moreover, even when data obtained via geofence warrants accurately captures a device's location, it may fail to locate the account owner whose data is being tracked. These factors make them particularly ripe for producing wrongful arrests and potentially wrongful convictions.

For these reasons, *amici* urge the Court to hold that the geofence warrant in this case violated the Fourth Amendment.

ARGUMENT

I. Geofence Warrants Create an Unacceptable Risk of Wrongful Arrests and Wrongful Convictions.

A. Geofence Warrants Have Already Led to Wrongful Arrests and Accusations.

Geofence warrants, by their very nature, target and potentially expose to law enforcement the location data of individuals who are not suspected of criminal activity. Rather than being based on individualized suspicion, they capture data from everyone in a certain geographical area at a certain time using a suitably configured electronic device. The broad net

cast by geofence warrants makes it virtually inevitable that they will lead to arrests of innocent people who were simply in the wrong place at the wrong time.

Indeed, this has already happened. In one documented instance, investigators improperly conflated the presumed location of a cell phone with that of an account owner, despite compelling evidence that the account owner was elsewhere and the phone was in a different person's possession. Meg O'Connor, *Avondale Man Sues After Google Data Leads to Wrongful Arrest for Murder*, PHX. NEW TIMES (Jan. 16, 2020, 9:11 AM), https://www.phoenixnewtimes.com/news/google-geofence-location-data-avondale-wrongful-arrest-molina-gaeta-11426374/. In another case, an innocent person became a burglary suspect when his bicycling route happened to place him within a geofence. Jon Schuppe, *Google tracked his bike ride past a burglarized home. That made him a suspect.*, NBC NEWS (Mar. 7, 2020, 6:22 AM), https://www.nbcnews.com/news/us-news/google-tracked-his-bike-ride-past-burglarized-home-made-him-n1151761.

Jorge Molina was wrongly arrested, spent six days in jail, and lost his job and his car due to a geofence warrant. On December 13, 2018, police officers in Avondale, Arizona arrested 23-year-old Molina on a first-degree murder charge in connection with a fatal

shooting, relying on Location History data[3] obtained via a geofence warrant from Google. O'Connor, *supra*. The Location History data showed that a device logged into Molina's Google account was in the area at the time of the murder. *Id.* Within a day of Molina's arrest, however, police were alerted to compelling alibi evidence: text messages and Uber receipts confirming that Molina had attended a movie with friends and was two miles away from the crime scene at the time of the shooting. *Id.* There were also other indications that the Location History data might not reflect Molina's true whereabouts. *Id.* On one date, for instance, the location data that the police obtained showed a device logged into Molina's account at the retirement community where his mother worked at the same time as debit card records documented him making a purchase on the other side of town. *Id.*

Police also learned that Molina's stepfather had a history of violence and had been using Molina's old phone, which had remained logged into Molina's email and social media accounts. *Id.* But rather than investigating the abundance of exculpatory evidence before proceeding with an arrest, police relied on the geofence warrant to arrest Molina, interrogate him,

[3] Location History refers to the tool developed by Google that "appears to be the most sweeping, granular, and comprehensive tool—to a significant degree—when it comes to collecting and storing *location* data." *United States v. Chatrie*, 590 F. Supp. 3d 901, 907 (E.D. Va. 2022).

keep him in jail for several days, and even issue a press release naming him as the suspect. *Id.*

Zachary McCoy was also wrongfully identified as the lead suspect in a crime due to a geofence warrant. On January 14, 2020, McCoy received a notice from Google saying that police in Gainesville, Florida had sought information about his account. Schuppe, *supra*. Local police alighted on McCoy because a Google geofence warrant in a burglary case yielded location data that "seemed suspicious" to police, showing him passing near the burglarized home three times in an hour. *Id.* Yet McCoy had nothing to do with the burglary; he was an avid biker, and his frequent loops around the neighborhood—including near the burglarized house, which was less than a mile from his own—were captured on an exercise-tracking app that used Google's location services. *Id.* Upon identifying him as suspicious based on his device's trajectory, police then leveraged entirely innocent behavior to try to access a vast trove of personal and otherwise protected information: they sought access not only to the exercise-tracking app's data around the time of the burglary, but to *all* data associated with McCoy's Google account, including his use of products like Gmail and YouTube. *Id.* Although the Location History data placed McCoy near the scene of the crime, he was innocent.

The cases of Jorge Molina and Zachary McCoy are emblematic of the inherent problems with geofence warrants discussed below: the inclusion of innocent

people in broad nets of suspicion, cognitive biases that lead investigators to neglect traditional investigative techniques and ignore evidence of innocence, and reliance on misleading or ambiguous technological data. The true number of wrongful arrests and wrongful convictions arising from geofence warrants remains unknown due in part to courts' frequent sealing of such warrants. 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. However, these warrants have been widely used by federal and state law enforcement to investigate a variety of crimes including robberies, sexual assaults, arsons, and murders. *See id.* As law enforcement continues to rely on such warrants and companies like Google continue to collect more data, the risk of wrongful arrests and convictions grows as well.

B. Because Geofence Warrants Are Based Solely on Proximity of Date and Location, They Necessarily Cast Suspicion on Innocent People.

Geofence warrants differ fundamentally from traditional warrants because they do not rest on evidence establishing probable cause as to a particular person. Rather, as in this case, law enforcement entities typically seek geofence warrants precisely because they lack probable cause to suspect a particular person of criminal activity. *See, e.g.*, *United States v. Chatrie*, 590 F. Supp. 3d 901, 917

(E.D. Va. 2022) ("Having unearthed no further leads from his investigation, Det. Hylton then turned to geofence technology."). This inverts the constitutionally mandated warrant process, transforming a tool meant to be predicated on evidence into one that generates suspicion based on mere proximity to a crime scene.

Geofence warrants can be staggering in scope. The geofence warrant in this case compelled Google to search the company's entire "Sensorvault" database, which contained Location History data from hundreds of millions of users, to identify devices estimated to be within the boundaries of a given geofence. *See id.* at 908 ("Google has to compare all the data in the Sensorvault in order to identify users within the relevant timeframe of a geofence.").[4] Necessarily, this process requires searching the location histories of innocent people with no connection to the crime under investigation. And the consequences for those innocent individuals whose devices are determined to be within—or even near—the boundaries of a geofence can be very serious.

Even when considering only the devices estimated to fall within a geofence's geographic and temporal boundaries, these warrants can and often do encompass areas and time frames broad enough to capture Location History data from many people who neither were involved in nor witnessed a crime—as

[4] Google announced in 2023 that it would store Location History on users' devices instead of in the Sensorvault.

Zachary McCoy's case illustrates. The warrant in this case, for example, involved "a geofence with a 150-meter radius—with a diameter of 300 meters, longer than three football fields—in an urban environment [that] included the Bank [at issue] and the nearby Journey Christian Church." *Id.* at 918. In other cases, law enforcement agencies have sought geofence warrants covering several acres, sometimes in densely populated cities, capturing businesses or residences entirely unrelated to the crime, or encompassing large and well-trafficked roads. *See, e.g.*, *In re the Search of Information that is Stored at the Premises Controlled by Google, LLC*, 542 F. Supp. 3d 1153, 1158 (D. Kan. 2021) (denying geofence warrant application where geographic boundary of geofence included two public streets and business unrelated to crime but located in target building); *In re the Search of Information Stored at Premises Controlled by Google*, Case No. 20 M 297, 2020 WL 5491763, at *1 (N.D. Ill. July 8, 2020) (denying geofence warrant application where requests covered two areas with 100-meter radii, including densely populated areas with restaurants, businesses, a residential complex, and medical offices). These expansive dragnets all but ensure that innocent individuals are swept into criminal investigations based solely on their proximity to a location at a particular time.

Zachary McCoy and Jorge Molina are just two examples of the thousands of innocent individuals each year whose location data places them within a geofence warrant zone and turns them into potential

suspects as a result. In one instance in Minnesota, "the name of an innocent man was released to a local journalist after it became part of the police record." Valentino-deVries, *supra*. He became a person of interest because a geofence placed him "within 170 feet of a burglary." *Id.* He later told a reporter that he "thought he might have appeared because he was a cabdriver." *Id.* In another instance, in New York City, the Manhattan district attorney sought information "for all devices used in parts of the Upper East Side"—purportedly to identify people involved in a brawl that took place in the area. Albert Fox Cahn, *Manhattan DA Cy Vance Made Google Give Up Info on Everyone in Area in Hunt for Antifa After Proud Boys Fight*, DAILY BEAST (Aug. 13, 2019, 12:03PM), https://www.thedailybeast.com/manhattan-da-cy-vance-made-google-give-up-info-on-everyone-in-area-in-hunt-for-antifa-after-proud-boys-fight/. In response to the search warrant, "Google provided information that investigators used—along with images given to a private facial recognition company—to target two people who turned out to be innocent bystanders." *Id.*; *see also* Alfred Ng, *Geofence Warrants: How Police Can Use Protesters' Phones Against Them*, CNET (June 16, 2020, 9:52 AM), https://www.cnet.com/news/geofence-warrants-how-police-can-use-protesters-phones-against-them. These cases exemplify that expansive geofence dragnets can and do sweep innocent persons into criminal investigations based solely on being in the wrong place at the wrong time.

Perhaps equally troubling, the inverse is also true: geofence warrants may fail to identify actual perpetrators while casting suspicion (and wasting investigative resources) on the innocent. Geofence searches can only return results for individuals who possess smartphones with Location History enabled and who had those devices with them at the relevant time. Perpetrators of crimes who do not own, or are not in possession of, smartphones, or who use devices that lack location services or for which such services have been disabled, would fall completely outside the scope of even the broadest geofence warrant. A sophisticated wrongdoer could simply leave their smartphone at home—or use a device without a traceable location service—to evade the detection of a geofence warrant. This perverse dynamic undermines the very investigative purpose geofence warrants purport to serve: these warrants generate false leads targeting innocent bystanders while allowing culpable parties to escape detection altogether.

II. Geofence Warrants Exacerbate Cognitive Bias and Rest on Unreliable Data, Two Factors Known to Contribute to Wrongful Convictions.

A. Geofence Warrants Contribute to Cognitive Bias, Leading Police to Ignore Alternative Suspects and Exculpatory Information.

Geofence warrants do not merely risk sweeping innocent people into the net of suspicion. They create conditions under which innocent people may be unable to escape suspicion. This Court has held 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. 85, 91 (1979) (citing *Sibron v. New York*, 392 U.S. 40, 62–63 (1968)). But geofence warrants depend entirely on such propinquity, even as they expose device users to arguably greater intrusions than the pat downs contemplated in *Ybarra*. *Compare Chatrie*, 590 F. Supp. 3d at 916 (noting that information released at Steps 2 and 3 can include "geographically unrestricted" location data "over an expanded time frame" and "account-identifying information" such as "name and email address") *with Ybarra*, 444 U.S. at 88–89, 96 (holding brief pat downs of bar patrons unconstitutional when warrant only authorized search of bartender and premises). And once a geofence warrant generates a pool of suspects, at least three forms of cognitive bias, which can lead criminal investigations astray, take hold: tunnel vision, confirmation bias, and automation bias.

Cognitive bias is a well-documented phenomenon both in human cognition generally and in police and forensic investigations specifically. *See, e.g.*, Itiel E. Dror, *Biased and Biasing: The Hidden Bias Cascade and Bias Snowball Effects*, 15 BEHAV. SCI. 490 (2025). Rather than reflecting intentional bias or prejudice, cognitive bias is "an outcome, a by-product, of people's cognitive architecture and of how the brain processes information." *Id.* at 491. In the context of the criminal legal system, cognitive bias refers to the ways that "an

individual's pre-existing beliefs, expectations, motives, and situational context influence the collection, perception, and interpretation of evidence during the course of a criminal case." *Id.* (quoting Saul M. Kassin, et al., *The Forensic Confirmation Bias: Problems, Perspectives, and Proposed Solutions*, 2 J. APPLIED RSCH. MEM. & COGNITION 42, 45 (2013)). Far from being a rare phenomenon, cognitive bias has been extensively documented across forensic and investigative disciplines. *See, e.g.*, Itiel Dror, *Cognitive and Human Factors in Expert Decision Making: Six Fallacies and the Eight Sources of Bias*, 92 ANAL. CHEM. 7998 (2020); Itiel Dror & David Charlton, *Why Experts Make Errors*, 56 J. FORENSIC IDENTIFICATION 600 (2006).

Cognitive bias in forensics and police investigations has contributed to numerous wrongful convictions. *See* Vanessa Meterko, Innocence Project, *What is Cognitive Bias and How Does It Contribute to Wrongful Conviction* (Aug. 19, 2021), https://innocenceproject.org/news/what-is-cognitive-bias-how-it-contributes-to-wrongful-conviction/. Each form of cognitive bias can cause investigators to disregard evidence of innocence. *See generally* Keith A. Findley & Michael S. Scott, *The Multiple Dimensions of Tunnel Vision in Criminal Cases*, 2006 WIS. L. REV. 291 (2006); Kassin, et al., *supra*; Raja Parasuraman & Dietrich H. Manzey, *Complacency and Bias in Human Use of Automation: An Attentional Integration*, 52 HUM. FACTORS 381 (2010). As detailed below, these dynamics have contributed to

wrongful convictions, including cases in which innocent people were sentenced to death.

i. Geofence Warrants Can Lead to Tunnel Vision and Confirmation Bias, Known Factors in Wrongful Convictions.

Tunnel vision refers to "a rigid focus on one suspect that leads investigators to seek out and favor inculpatory evidence [against that suspect], while overlooking or discounting any exculpatory evidence." Kassin, et al., *supra*, at 45; *accord* Eitan Elaad, *Tunnel Vision and Confirmation Bias Among Police Investigators and Laypeople in Hypothetical Criminal Contexts*, 12 SAGE OPEN 1, 2 (Apr. 2022); Findley & Scott, *supra*, at 292. Tunnel vision is not intrinsically a function of bad faith, maliciousness, or indifference. Instead, it is "more often the product of the human condition as well as institutional and cultural pressures." Findley & Scott, *supra*, at 292. The fact that tunnel vision is unintentional, however, does not make it less dangerous to innocent suspects.

State inquiries into the causes of wrongful convictions have repeatedly identified tunnel vision as a significant contributor to wrongful convictions. In 2002, former Illinois Governor George Ryan's Commission on Capital Punishment examined the thirteen cases in which innocent people were sentenced to death before being exonerated, finding that "[a]ll 13 cases were characterized by relatively little solid evidence connecting the charged

defendants to the crimes." State of Ill., *Report of the Governor's Commission on Capital Punishment* 7 (2002). The Commission identified "the dangers of tunnel vision or confirmatory bias" as a critical factor in these wrongful convictions. *Id.* at 21. In Virginia, similarly, the Innocence Commission examined the state's known wrongful convictions and found that tunnel vision caused police to "too quickly jump to the conclusion that a particular suspect is guilty" and to "focus solely on one person to the exclusion of other viable suspects." Innocence Comm'n for Va., *A Vision for Justice: Report and Recommendations Regarding Wrongful Convictions in the Commonwealth of Virginia* 69 (2005). These findings are not isolated incidents, but patterns that recur during criminal investigations, even when law enforcement is confronted with proof of innocence.

Steven Avery's case starkly illustrates the danger that police tunnel vision can pose to innocent people. In 1985, Avery was convicted of a brutal rape in Manitowoc County, Wisconsin, based primarily on an eyewitness identification later shown to be unreliable. Findley & Scott, *supra*, at 299–300. Local sheriff's deputies focused on Avery not because any evidence connected him to the crime, but because he was accused of another crime at the time and the sheriff thought he matched the victim's description. Innocence Project, *Case Profiles: Steven Avery*, https://innocenceproject.org/cases/steven-avery/.
After Avery was identified by the victim in a suggestive eyewitness identification procedure, the

sheriff's office and assigned prosecutor never investigated any other suspects—even though the actual perpetrator also matched the description and was a suspect in a series of sexual assaults in the area, and both the local police department and at least two employees in the district attorney's office suggested that he might be the true perpetrator. *Id.*; Findley & Scott, *supra*, at 299–301. At trial, Avery presented sixteen alibi witnesses who confirmed his whereabouts, including two entirely unbiased store employees, but he was still convicted. Findley & Scott, *supra*, at 301–02. Tunnel vision led to Avery serving more than eighteen years in prison for a crime he did not commit before he was finally exonerated by DNA.

Tunnel vision is related to the phenomenon of confirmation bias—the universal human tendency to favor "information that confirms an individual's preconceptions or hypotheses independently of the information's truthfulness or falsity." Elaad, *supra*, at 2. While tunnel vision involves a narrowing of focus onto a specific individual, so that alternate suspects are not considered, confirmation bias involves a broader tendency to "seek or interpret evidence in ways that support existing beliefs, expectations or hypotheses." Findley & Scott, *supra*, at 309. Confirmation bias has been shown to afflict experts in a variety of domains, including "fingerprint comparisons, toxicology, and other forensic science judgments." Itiel E. Dror, et al., *Cognitive Bias in Forensic Pathology Decisions*, 66 J. FORENSIC SCI. 1750, 1752 (2021). In one classic study, expert

fingerprint examiners were asked to examine a set of fingerprints that they themselves had previously declared a "match" but were told they were from a high-profile case of a wrongful match; four out of five examiners changed their opinion that the fingerprints were a match. Itiel E. Dror, et al., *Contextual Information Renders Experts Vulnerable to Making Erroneous Identifications*, 156 FORENSIC SCI. INT'L 74, 76 (2006). Similarly, researchers have found that false confessions can "corrupt other evidence": For instance, when polygraph examiners are told a suspect confessed, they are more likely to determine that the suspect was deceptive, and when eyewitnesses are told a suspect confessed, they are more likely to identify that suspect—even if they had initially identified someone else. Kassin, et al., *supra*, at 46.

Jorge Molina's case makes clear how tunnel vision and confirmation bias can play out with geofence warrants. When police lock onto a suspect identified via a geofence warrant, these cognitive phenomena can lead them to ignore alternate leads, disregard exculpatory evidence, and over-weight evidence that appears to confirm the suspect's guilt. For Molina, this meant several days of wrongful incarceration despite strong alibi evidence, the presence of a much more compelling suspect, and clear indications that his Location History data might not reflect his true whereabouts. *See* O'Connor, *supra*. This is particularly concerning with geofence warrants because once a device or devices are identified via

Location History, law enforcement is granted the power to bypass particularized, individualized showings of probable cause—the kind of individualized showings that might force law enforcement to reckon with contradictory or exculpatory evidence—supplanting the gatekeeping role of a neutral and detached magistrate. *Cf. Ybarra*, 444 U.S. at 107. Once investigators identify a set of devices present in or near the boundaries of a geofence, the geofence warrant process leaves the choice of which devices and users to pursue for further investigation to the discretion of law enforcement and private companies, without judicial oversight. *See Chatrie*, 590 F. Supp. 3d at 916 (describing Steps 2 and 3 of Google's response process). This creates precisely the kind of investigative environment ripe for tunnel vision and confirmation bias.

ii. Geofence Warrants Can Produce Automation Bias, Which Can Contribute to Convicting the Innocent.

The use of geofence warrants can also lead to automation bias, which refers to the human tendency to "over-rely on automation." Kate Goddard, et al., *Automation Bias: A Systematic Review of Frequency, Effect Mediators, and Mitigators*, 19 J. AM. MED. INFORM. ASSOC. 121, 121 (2011). Automation bias tends to produce "decisions that are not based on a thorough analysis of all available information but that are strongly biased by the automatically generated

advice." Parasuraman & Manzey, *supra*, at 391. In other words, it can induce individuals, including police officers, to accept technological outputs uncritically.

Decades of controlled studies across domains as varied as aviation, medicine, process control, and military command have established that humans systematically over-rely on computer-generated outputs, even when those outputs are demonstrably wrong. *Id.* at 392–95. Automation bias "(a) can be found in different settings, (b) occurs in both naïve and expert . . . participants, (c) seems to depend on the . . . overall reliability of an aid, (d) cannot be prevented by training or explicit instructions to verify the recommendations of an aid, (e) seems to . . . depend on how accountable users of an aid perceive themselves for overall performance, and (f) can affect decision making in individuals as well as in teams." *Id.* at 397. Automation bias can persist even when lives are at stake: one study found, for instance, that the detection rate for cancers dropped from 68% when mammogram reviewers were unaided by technology to 52% when an automated aid failed to perform its intended function. E. Alberdi, et al., *Effects of Incorrect Computer-Aided Detection (CAD) Output on Human Decision-Making in Mammography*, 11 ACAD. RADIOLOGY 909, 909–18 (2004).

Automation bias is known to lead to both errors of omission, where the user fails to notice problems because the automation does not alert them, and

errors of commission, where users follow automated recommendations that are incorrect. Parasuraman & Manzey, *supra*, at 392. In geofence investigations, omission errors occur when investigators fail to notice the data's limitations, and commission errors occur when investigators act on location matches that are wrong or misleading.

Google's Location History data is computer-generated and carries the imprimatur of one of the world's most sophisticated technology companies. But, as discussed in Part II.B, *infra*, such data is not always accurate and can be highly imprecise depending on what type of location data is used. See Andrea Macarulla Rodriguez, et al., *Google Timeline Accuracy Assessment and Error Prediction*, 3 FORENSIC SCI. RES. 240, 241–42, 249 (2018) (providing an overview of the various positioning methods used for Location History and documenting substantially less precision and substantially greater error for location sources such as Wi-Fi and 2G and 3G cell networks compared to GPS). Yet automation bias can induce investigators to disregard these nuances and accord less precise forms of Location History data more weight than they deserve. Automation bias can also lead investigators to ignore the fact that the true perpetrator might be entirely absent from the Location History data produced in response to a geofence warrant. Investigators inclined to trust the objective-seeming data may simply focus instead on the most suspicious-looking candidate among the devices and users that *are* included, even if that

person is innocent—just as the police did with Zachary McCoy.

The Government may contend that geofence warrants are merely investigative tools that develop individualized suspicion through subsequent narrowing steps. But the Fourth Amendment requires that probable cause be established before the search, not manufactured afterward through steps that provide "law enforcement and Google with unbridled discretion to decide which accounts will be subject to further intrusions." *Chatrie*, 590 F. Supp. 3d at 927. This is especially so when the individuals exercising that discretion are vulnerable to automation bias and insufficiently sensitive to the potential for the automatically generated data to be misleading.

This Court has emphasized that the probable cause requirement "cannot be undercut or avoided by simply pointing to the fact that coincidentally there exists probable cause to search or seize another or to search the premises where the person may happen to be." *Ybarra*, 444 U.S. at 91. Yet geofence warrants do precisely that. They cast suspicion on everyone who happens to have been near a location. And once suspicion has set in, cognitive biases make it extraordinarily difficult for innocent people to clear their names. The result is a digital dragnet from

which the innocent, once ensnared, may never fully escape.

B. Geofence Warrants Target Location History Data That, Despite How Detailed and Extensive It Can Be, Is Also Often Unreliable.

Even when Location History data is broadly accurate, it can produce both false positives and false negatives: someone not in the targeted area may be reported as present, and someone present may not be captured at all. *See Chatrie*, 590 F. Supp. 3d at 923. Location data sources that vary in accuracy and precision, confidence intervals calibrated to capture only a subset of devices' true locations, the possibility of users' Google accounts being active on multiple devices, and the prerequisites for inclusion in the Sensorvault Location History database all contribute to the prevalence of false positive and false negatives.

First, although Location History data can in some cases estimate a device's location with extreme accuracy, it is not always reliable, and different sources of Location History data vary widely in precision. Location History draws from several sources of data, including the Global Positioning System (GPS), Bluetooth beacons, nearby Wi-Fi networks, cellular towers, and Internet Protocol address information. *Id.* at 908. Some of this data can be precise. Under certain circumstances, Google can estimate a device's location within three meters or determine which floor of a multi-story building it is on using Location History data. *Id* at 908–09. Generally,

GPS is the most accurate source of location data. *See* Rodriguez, et al., *supra*, at 245 (noting that among Google location methods, GPS had "highest hit ratio" for correctly capturing a device's true location within the listed margin of error).

Other sources of Location History data can be considerably less accurate, and coordinates presented to four decimal places may still reflect a location estimate that is off by hundreds of meters. One study found that when GPS is unavailable, Google's hit rate (the proportion of cases in which the true location fell within the confidence interval Google provided) was only 38% for 3G networks and 33% for 2G networks. *Id.* Cell tower data can be especially imprecise, particularly in rural areas, where such data might provide estimates of an individual's location miles away from their true location. *Id.* at 249–50.

Because Location History data can be imprecise and its accuracy can vary based on its source, Google generates a confidence interval for each set of estimated location coordinates. Google's responses to geofence warrants contain estimated latitude and longitude coordinates for each device believed to lie within the perimeter of the geofence as well as a confidence interval for that data point. *Chatrie*, 590 F. Supp. 3d at 909, 915. The confidence interval is provided in the form of a circle around the identified coordinates, which represents a margin of error for the device's true location. *Id.* at 909. The smaller the radius of the confidence interval, the more precise

Google believes the location estimate to be—the larger the radius, the less precise the estimate.

When Google cannot identify a device's location with precision and provides coordinates with a large confidence interval, the true location of a device might be hundreds of meters outside the geofence, which itself might already span a large area. *See id.* at 918 n.26 (noting that the total area of the geofence here was 70,686 square meters). As such, geofence warrants can include people who were nowhere near the target location. Indeed, as the District Court noted, the geofence warrant here captured a user whose true location "may not have been remotely close enough to the Bank to participate in or witness the robbery" because the "confidence intervals stretched to 387 meters," more than twice the radius of the geofence itself. *Id.* at 922, 930. The area within the confidence intervals for that user included residences, a church, a hotel, a senior living facility, and two busy streets, any of which could have been the user's true location. *Id.* at 922–23.

Second, because Google's reported confidence intervals are not designed to capture all users or devices, the true location of the device can fall outside of the confidence interval. Google sets its confidence intervals with the goal of capturing approximately 68 percent of users within them. *Id.* at 909. This means that, for a given confidence interval, there is a 32 percent chance that the device's true location falls outside the listed radius. As discussed above, the

radius of these confidence intervals can already be as large as hundreds of meters, encompassing residences, hotels, restaurants, and places of worship. *Id.* at 922–23. There is around a one-in-three chance that the true location of a device is even farther away, despite appearing within the geofence.

As discussed in Part I.B, *supra*, the information provided to law enforcement officials in response to geofence warrants will inevitably include the data of innocent people who were simply going about their daily lives within geofence boundaries around the time of a crime. This itself is cause for concern. However, because the data can be imprecise and because there is a significant chance that a device was not located within the confidence interval, there is substantial danger that geofence warrants will envelop not only those innocent individuals who happen to have actually been within the arbitrary geofence area drawn by law enforcement, but also innocent individuals who were never anywhere near the area specified in the warrant. These individuals may have been hundreds of meters away—and yet geofence warrants put their data into law enforcement's hands. That this tool can sometimes be extraordinarily accurate in some cases increases its danger, potentially luring officials to overestimate its accuracy in other cases where it may be inaccurate or imprecise. Location History data invites officials to rely on potentially misleading data to justify investigations and arrests, creating a serious risk that innocent people will be unreasonably surveilled,

investigated, and falsely accused or convicted—even if they never set foot near a crime scene.

Third, even when the location data does accurately capture a device's location, the presence of a device in the vicinity of a crime scene does not necessarily mean the account owner was there. Location History tracks logged-in Google accounts, not individuals, and Google allows users to be logged into their accounts on multiple devices simultaneously. *Chatrie*, 590 F. Supp. 3d at 909 ("Location History tracks a user's location across every app and every device associated with the user's account."). A law enforcement official therefore might pursue suspects based on the incorrect assumption that a device's presence at the scene of a crime necessarily indicates that the account owner was also present, even though it might have been their family member, friend, roommate, or even a stranger who picked up a lost phone.

This type of error is precisely what exposed Jorge Molina to a wrongful accusation of homicide and police's public broadcasting of his name and face as the murder suspect. O'Connor, *supra*. Although Molina ultimately was not charged and avoided a wrongful conviction, he was arrested at work and subsequently lost his job, lost his car, and had to drop out of school. *Id.* He has had to live with the psychological ramifications of his wrongful arrest for a crime punishable by death: nightmares about "sitting alone in that jail cell," where he was held for six days, and fear that "his phone may track him to

another crime scene" or that he might "be treated as a killer by people who recognize his widely spread mugshot." *Id.* And he has said that the arrest has made it difficult for him to find a new job ever since, as his record remains unsealed. *Id.* Geofence warrants' potential to first point law enforcement to innocent people, and then blind them to exculpatory evidence, makes such outcomes virtually inevitable.

Finally, even if the technology itself were entirely accurate and reliable, and even if device locations perfectly corresponded with account owners' locations, a geofence warrant might still in some cases point police only to innocent people. If the true suspect is not a Google user or has not activated Location History then, by definition, everyone whose device shows up in Location History results for the geofence warrant will be innocent. In such a circumstance, even though all devices located by a geofence warrant would belong to people unconnected to the crime, their presence in the search results will nonetheless expose them to a pall of suspicion and potentially illegal searches and seizures. This is particularly true given that law enforcement officials have turned to geofence warrants in the absence of individualized suspicion. *See, e.g.*, *Chatrie*, 590 F. Supp. 3d at 917 ("Having unearthed no further leads from his investigation, Det. Hylton then turned to geofence technology.").

Reaching for this technology with no independent, individualized basis for suspicion, government officials are primed to rely upon location data to draw

rushed conclusions, even if the true suspect does not use Location History and all returned data therefore targets innocent people. Coupled with the cognitive biases of tunnel vision, confirmation bias, and automation bias, geofence warrants create conditions ripe for wrongful arrests and convictions.

CONCLUSION

For the foregoing reasons, *amici curiae* urge this Court to hold that the execution of the geofence warrant violated the Fourth Amendment.

Respectfully submitted,

M. CHRIS FABRICANT
MATTHEW A. WASSERMAN
INNOCENCE PROJECT, INC.
40 Worth Street, Suite 701
New York, NY 10013

JAMES C. DUGAN
Counsel of Record
FERDINAND G. SUBA JR.
CORINNE D. CATHCART
WILLKIE FARR
& GALLAGHER LLP
787 Seventh Avenue
New York, NY 10019
(212) 728-8000
jdugan@willkie.com

Counsel for Amici Curiae

March 2, 2026