No. 22-4489

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

UNITED STATES,
Appellee,

v.

OKELLO CHATRIE,
Appellant.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA, RICHMOND DIVISION

BRIEF OF *AMICI CURIAE* AMERICAN CIVIL LIBERTIES UNION, AMERICAN CIVIL LIBERTIES UNION OF VIRGINIA, AND EIGHT FEDERAL PUBLIC DEFENDER OFFICES WITHIN THE FOURTH CIRCUIT IN SUPPORT OF APPELLANT AND REVERSAL

Jennifer Stisa Granick
American Civil Liberties Union Foundation
39 Drumm Street
San Francisco, CA 94111
Tel.: (415) 343-0758
jgranick@aclu.org

Eden B. Heilman
Matthew W. Callahan
American Civil Liberties Union Foundation of Virginia
P.O. Box 26464
Richmond, VA 23261
Tel.: (804) 523-2146
eheilman@acluva.org
mcallahan@acluva.org

Nathan Freed Wessler
Ashley Gorski
Patrick Toomey
Brandon Buskey
Trisha Trigilio
Laura Moraff
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
Tel.: (212) 549-2500
nwessler@aclu.org

(Additional Counsel for Amici Curiae listed on following page)

William F. Nettles, IV
Federal Public Defender
District of South Carolina
1901 Assembly Street
Suite 200
Columbia, SC 29201

Brian J. Kornbrath
Federal Public Defender
Northern District of West Virginia
230 West Pike Street
Suite 360
Clarksburg, WV 26301

G. Alan Dubois
Federal Public Defender
Eastern District of North Carolina
150 Fayetteville Street
Suite 450
Raleigh, NC 27601

John Baker
Federal Public Defender
Western District of North Carolina
129 West Trade Street
Suite 300
Charlotte, NC 28202

Louis Allen
Federal Public Defender
Middle District of North Carolina
301 N. Elm Street
Suite 410
Greensboro, NC 27401

James Wyda
Federal Public Defender
District of Maryland
100 South Charles Street
Tower II, 9th Floor
Baltimore, MD 21201

Juval O. Scott
Federal Public Defender
Western District of Virginia
210 First Street, SW
Suite 400
Roanoke, VA 24011

Wesley P. Page
Federal Public Defender
Southern District of West Virginia
300 Virginia Street East
Room 3400
Charleston, WV 25301

RULE 26.1 DISCLOSURE STATEMENT

The American Civil Liberties Union and the American Civil Liberties Union of Virginia are non-profit entities that do not have parent corporations. No publicly held corporation owns ten percent or more of any stake or stock in either organization.

The Federal Public Defender offices advocate on behalf of the criminally accused pursuant to 18 U.S.C. § 3006A, and are not corporations within the meaning of Fed. R. App. P. 26.1.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

INTEREST OF *AMICI CURIAE*[1]

The American Civil Liberties Union ("ACLU") is a nationwide, non-profit, non-partisan organization dedicated to defending the principles of liberty and equality embodied in the Constitution and our nation's civil rights laws. The ACLU of Virginia is a state affiliate of the ACLU. The protection of privacy as guaranteed by the Fourth Amendment, and the preservation of longstanding remedies for violations of that guarantee, are of special concern to *amici*.

Federal Defender *amici* are eight Federal Public Defender offices within the Fourth Circuit.[2] Each year, the Federal Defender *amici* collectively represent hundreds of indigent criminal defendants charged with violating various federal criminal laws, during the investigation of which the government routinely seeks search warrants for location data and seeks to apply the good-faith exception to the exclusionary rule pursuant to *United States v. Leon*, 468 U.S. 897 (1984), to those warrants. Federal Defender *amici* and their clients therefore have a strong interest in

---

[1] Pursuant to Federal Rule of Appellate Procedure 29(a)(4)(E), counsel for *amici curiae* certify that no person or entity, other than *amici curiae*, their members, or their counsel, made a monetary contribution to the preparation or submission of this brief or authored this brief in whole or in part. Appellant has consented to, and Appellee does not oppose, the filing of this brief.

[2] *Amici* are the Federal Public Defender offices for the District of Maryland, the Eastern, Middle, and Western Districts of North Carolina, the District of South Carolina, the Western District of Virginia, and the Northern and Southern Districts of West Virginia.

whether this Court finds that the good-faith exception to the exclusionary rule applies to geofence warrants and other novel surveillance techniques, which will control the outcome of Appellant Okello Chatrie's appeal.

SUMMARY OF ARGUMENT

This case presents the first opportunity for a federal court of appeals to decide whether it was objectively reasonable for a law enforcement officer to rely on a "geofence warrant." Geofence warrants purport to authorize officers to obtain information about an unknown and unlimited number of cell phone users. The actual scope of the search is determined after the warrant is issued, outside the presence of a judge, through opaque negotiations between law enforcement and Google. These warrants lack the predicate showing of probable cause and particularity, as well as the judicial oversight, required by the Fourth Amendment. They pose significant threats to privacy, because rather than identifying particular devices for which there is probable cause to search, geofence warrants allow officers to fish for relevant evidence from any and all devices estimated to have been within a geographical area. The ACLU and Federal Defender Offices agree with the defendant and other *amici* that this geofence warrant violated the Fourth Amendment.

This brief addresses the applicability of the good-faith exception to the exclusionary rule. The exclusionary rule has a particularly important role in incentivizing candor and caution when the government seeks authorization to use novel surveillance techniques like geofence warrants. Here, the good-faith exception cannot apply because reliance on this warrant was not objectively reasonable.

Det. Hylton's reliance on this geofence warrant was objectively unreasonable because his application lacked the required indicia of probable cause and particularity: based on surveillance footage purportedly showing *one* unknown subject of interest with a cell phone before a bank robbery, Det. Hylton sought authority to conduct a novel search that would sweep in *all* devices that Google estimated to be in a 17.5-acre area during an hour-long period. J.A. 110, 112, 1351. No warrant could constitutionally authorize such an overbroad search, because "[g]eneral searches have long been deemed to violate fundamental rights. It is plain that the [Fourth] [A]mendment forbids them." *Marron v. United States*, 275 U.S. 192, 195 (1927).

Beyond these threshold defects, the warrant purported to authorize law enforcement and Google employees to determine the scope of their search while they were executing it—without returning to the magistrate to make any further assessment of probable cause. No valid warrant could cede to law enforcement officers the magistrate's constitutional duty to determine whether probable cause existed to obtain additional location and identification information for some of the cell phone users implicated in the first stage of the search. "It is the *magistrate's* responsibility to determine whether the officer's allegations establish probable cause and, if so, to issue a warrant comporting in form with the requirements of the Fourth Amendment." *United States v. Leon*, 468 U.S. 897, 921 (1984) (emphasis added).

Amici urge this Court to hold that it was objectively unreasonable to rely on the obviously deficient warrant in this case, and that suppression is necessary to incentivize caution and candor, especially when officers seek authorization to use novel surveillance techniques. Finally, *amici* urge this Court to decide the underlying Fourth Amendment issue before proceeding to the good-faith inquiry in order to provide magistrates and law enforcement officers with much-needed guidance on the use of geofence warrants and similar attempts to obtain authorization for overbroad general searches.

ARGUMENT

I. The government has a history of concealing information from magistrates when applying to use novel surveillance techniques, and must be deterred from continuing to do so.

It is axiomatic that in order for an officer's reliance on the magistrate's determination to be objectively reasonable, the officer must have supplied the magistrate with information "sufficient for a judge to exercise his independent judgment on issuing a search warrant." *United States v. Tate*, 524 F.3d 449, 457 (4th Cir. 2008). Warrant proceedings, which are conducted *ex parte*, demand a heightened duty of candor from police, because there is no adversarial process to bring omitted facts, inaccurate statements, or countervailing legal arguments to the magistrate's attention. *See Franks v. Delaware*, 438 U.S. 154, 169 (1978); *In re Accuracy Concerns Regarding FBI Matters Submitted to the FISC*, 411 F. Supp. 3d

333, 336 (FISA Ct. 2019) (observing that the government has a "heightened duty of candor . . . in *ex parte* proceedings . . . such as proceedings on electronic surveillance applications") (quotation marks omitted). This always-extant need for candor is especially acute when law enforcement officers and prosecutors seek permission to use novel and complex technologies that have rarely been the subject of judicial review. Yet when police seek to use novel surveillance techniques, they often fail to provide the magistrate with sufficient information to ensure the search meets the Fourth Amendment's requirements.

Take, for example, the years' worth of misleading applications seeking court orders to use cell site simulators to track and locate phones. Cell site simulators are police-operated devices that mimic cell phone towers, sending out signals that cause phones in the vicinity to transmit their unique serial number, which can be used to locate the phones. *See Andrews v. Balt. City Police Dep't*, 8 F.4th 234, 235 (4th Cir. 2020). The technology raises significant concerns under the Fourth Amendment because the devices collect information about bystanders who happen to be in the area and locate phones inside homes and other constitutionally protected spaces. *See id.* at 236–37.

For years, law enforcement agents and prosecutors sought authority to use cell site simulators by submitting applications that camouflaged this technology—often by completely omitting its novel capabilities and Fourth Amendment implications.

In Tacoma, Washington, for example, a press investigation revealed that police had used a cell site simulator more than 170 times over five years but had concealed their intent to do so from judges when seeking court orders.[3] In Charlotte, North Carolina, a similar investigation revealed that police had been deploying cell site simulators for eight years pursuant to pen register orders without disclosing that fact to courts.[4] In a Maryland case involving use of a cell site simulator where "prosecutors and police obtained an order under the Maryland pen register statute that failed to provide the necessary information upon which the court could make the constitutional assessments mandated," an appeals court explained that such concealment "prevents the court from exercising its fundamental duties under the Constitution" because "it is self-evident that the court must understand why and *how* the search is to be conducted." *State v. Andrews*, 134 A.3d 324, 338–39 (Md. Ct. Spec. App. 2016). After—and only after—such cases came to light, legislatures and courts began to expressly direct police to include full explanations of the technology in warrant applications so that magistrate judges could adequately assess whether to issue

[3] Adam Lynn, *Tacoma Police Change How They Seek Permission to Use Cellphone Tracker*, News Tribune (Nov. 15, 2014), https://www.thenewstribune.com/article25894096.html.

[4] Fred Clasen-Kelly, *CMPD's Cellphone Tracking Cracked High-Profile Cases*, Charlotte Observer (Nov. 22, 2014), https://www.charlotteobserver.com/news/local/crime/article9235652.html.

warrants and what limitations to place on them. *See, e.g.*, 725 Ill. Comp. Stat. 137/15; Wash. Rev. Code § 9.73.260; *In re Application of the U.S. for an Ord. Relating to Tels. Used by Suppressed*, No. 15 M 0021, 2015 WL 6871289 (N.D. Ill. Nov. 9, 2015).

The government has exhibited a similar lack of candor in proceedings related to "upstream" surveillance of Internet communications.[5] The government first sought approval to conduct this surveillance under Section 702 of the Foreign Intelligence Surveillance Act ("FISA") in 2008, but it was not until 2011 that the government belatedly disclosed key facts about how this internet surveillance operates and results in significant intrusions on Americans' private communications. *See, e.g.*, [*Caption Redacted*], [Docket No. Redacted], 2011 WL 10945618, at *5, 27–41 (FISA Ct. Oct. 3, 2011) (describing the government's surveillance of "Internet transactions"). Even after the Foreign Intelligence Surveillance Court ("FISC") imposed new rules in response to these disclosures, the government did not report its repeated violations of those rules as part of its subsequent surveillance applications. In 2016, the FISC "ascribed the government's failure to disclose" these

[5] Upstream surveillance involves the bulk interception and searching of Americans' international Internet communications—including voice calls, emails, chats, and web-browsing traffic—as their communications travel the spine of the Internet between sender and receiver. *See Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* 7, Priv. & C.L. Oversight Bd. (July 2, 2014), https://irp.fas.org/offdocs/pclob-702.pdf.

violations "to an institutional 'lack of candor' on NSA's part and emphasized that 'this is a very serious Fourth Amendment issue.'" [*Caption Redacted*], [Docket No. Redacted], slip op. at 19 (FISA Ct. Apr. 26, 2017), https://perma.cc/7X2S-VAS7 (quoting an October 26, 2016 FISC hearing transcript at 5–6).

The government's control of what information to present to magistrates has also resulted in broad searches impacting the privacy of numerous non-suspects in the context of warrantless "cell tower dumps"—searches where the government obtains records revealing every phone that connected to one or more cell towers during a particular timespan. In one case, despite the government asserting that investigators had sought phone connection records from "rural locations in order to minimize the amount of extraneous telephone data that would likely be obtained," they received "in excess of 150,000 telephone numbers registering with these towers" pursuant to an order obtained from a magistrate judge. *See* Affidavit of Probable Cause at 11–12, *In re Application of the U.S. for an Ord. Authorizing a Mobile Tracking Device & Pen Reg.*, No. 10-6121 MB (D. Ariz. Mar. 3, 2010) (filed at ECF No. 43-1 in *United States v. Capito*, No. 3:10-cr-08050-NVW (D. Ariz)). Sometimes, law enforcement officers did not understand how tower dumps worked. *See, e.g.*, *In re Application of the U.S. for an Ord. Pursuant to 18 U.S.C. § 2703(d)*, 930 F. Supp. 2d 698, 699 (S.D. Tex. 2012) ("When discussing the technology with the assistant United States Attorney, it became apparent that he did not understand

it well."). However, when magistrate judges have pushed for further information, they have been able to craft orders narrowing the scope of the requests in order to protect the privacy of non-suspects, illustrating the importance of robust disclosures. *See, e.g.*, *In re Application of the U.S. for an Ord. Pursuant to 18 U.S.C. §§ 2703(c), 2703(d)*, 42 F. Supp. 3d 511, 519 (S.D.N.Y. 2014).

These examples underscore the need to incentivize candor when the government is applying to use novel surveillance techniques that pose significant threats to privacy. The exclusionary rule is necessary to counter the incentives for police to withhold information from courts about how those tools are being deployed. If it is considered "objectively reasonable" for an officer to rely on a warrant issued as a result of the officer's own inadequate presentation of facts, then police will continue to experiment with novel, powerful, and potentially unlawful forms of surveillance while shrouding their operations in secrecy.

In this case, Det. Hylton failed to adequately inform the magistrate judge of the scope and nature of the proposed search, thereby denying the magistrate an opportunity to make an informed, independent assessment as to whether the search was adequately supported by probable cause and sufficiently particularized. For example, Det. Hylton did not tell the magistrate that the search would require Google to compare *all* data in its location history repository to identify users within the geofence area, J.A. 1333, or that Google predicts the specific area a user was in with

only 68% accuracy, J.A. 1334–35. He did not warn the magistrate that law enforcement could easily identify users by combining the de-identified information Google provides in early stages of the geofence search with publicly available information such as tax records and social media accounts. J.A. 1359, 1371 & n.39. Nor did Det. Hylton inform the magistrate that the geofenced area was in a busy part of Richmond that included the Journey Christian Church. J.A. 1351, 1361; *see also* Appellant's Br. 32–33, ECF No. 22.

Here, exclusion is appropriate because "the deterrence benefits of suppression outweigh the 'substantial social costs' of excluding the evidence." *United States v. Rush*, 808 F.3d 1007, 1010 (4th Cir. 2015). Suppression would deter law enforcement officers from omitting plainly material facts from warrant applications when seeking authorization to use novel surveillance techniques, and conducting vastly overbroad searches limited only by the capabilities of a private company.

II. The good-faith exception does not apply to Det. Hylton's reliance on the geofence warrant here.

Geofence warrants like this one purport to authorize sweeping searches of an unidentified number of devices without particularized probable cause and without sufficient judicial oversight. "Ordinarily, when a search violates the Fourth Amendment, the fruits thereof are inadmissible under the exclusionary rule, 'a judicially created remedy designed to safeguard Fourth Amendment rights generally

through its deterrent effect.'" *United States v. Doyle*, 650 F.3d 460, 466 (4th Cir. 2011) (quoting *United States v. Calandra*, 414 U.S. 338, 348 (1974)). The Supreme Court has created an exception where police rely in objective "good faith" on a judicially authorized, facially valid warrant that is later determined to be defective. *Leon*, 468 U.S. at 920–21. But the good-faith exception applies only when "the officer's reliance on the magistrate's probable cause determination and on the technical sufficiency of the warrant" was "*objectively reasonable*." *Id.* at 922 (emphasis added).

In establishing this good-faith exception, the *Leon* Court specified that it would be unreasonable for police to rely on a warrant "based on an affidavit 'so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable'"; or "so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid"; or "where the issuing magistrate wholly abandoned his judicial role." 468 U.S. at 923 (quoting *Brown v. Illinois*, 422 U.S. 590, 610–11 (1975) (Powell, J., concurring in part)). The geofence warrant in this case failed in each of these three respects. Because reliance on the warrant was objectively unreasonable, the good-faith exception does not apply.

A. The warrant was so lacking in indicia of probable cause that it was unreasonable to presume it was valid.

The Fourth Amendment is designed to "eliminate altogether searches not based on probable cause," and "those searches deemed necessary should be as limited as possible." *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971). Thus "a warrant to search a place cannot normally be construed to authorize a search of each individual in that place." *Ybarra v. Illinois*, 444 U.S. 85, 92 n.4 (1979). Because geofence warrants seek "to cause the disclosure of the identities of various persons whose Google-connected devices entered the geofences, the government must satisfy probable cause as to those persons." *In re Search of: Info. Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 750–51 (N.D. Ill. 2020) (rejecting a geofence warrant application).

Here, the warrant authorized a search of every device likely to be in or near a 17.5-acre area surrounding a crime scene during an hour-long period. Yet Det. Hylton made no attempt to establish probable cause linking every phone in the area to the alleged crime. Instead, Det. Hylton attempted to establish that there was probable cause to obtain data about *one* unknown subject's phone, J.A. 112 ("[P]rior to the robbery . . . the [unknown subject] had a cell phone in his right hand and appeared to be speaking with someone on the device."), knowing the geofence search would gather information about an unlimited number of other phones.

The good-faith exception does not apply "where a reasonable officer would know that a probable cause determination could not be rendered without information conspicuously absent from his application for a warrant." *Doyle*, 650 F.3d at 476. For example, this Court declined to apply the good-faith exception where a warrant that was "chiefly based . . . on finding three marijuana stems in the trash . . . empowered the police to seize a host of things seemingly unconnected to marijuana possession," including "any computers, toiletries, or jewelry, and the search of every book, record, and document in the home." *United States v. Lyles*, 910 F.3d 787, 795 (4th Cir. 2018). "Nothing in the affidavit supported a search for entirely lawful items," so "no reasonable officer would have believed that this warrant was valid." *United States v. Lyles*, No. TDC-17-0039, 2017 WL 5633093, at *7 (D. Md. Nov. 20, 2017), *aff'd,* 910 F.3d 787 (4th Cir. 2018).

Similarly, evidence that one suspect was using a cell phone before a robbery cannot justify indiscriminately gathering information about every nearby cell phone. No reasonably well-trained officer would rely on a magistrate's authorization to obtain data from an unlimited number of devices when the affidavit only addresses one of those devices. Indeed, a court in the Northern District of Illinois recently rejected a geofence warrant, in part because "the government ha[d] not established probable cause to believe that evidence of a crime will be found in the location history and identifying subscriber information of persons *other than the Unknown*

Subject," and yet "[t]he warrant s[ought] to gather evidence on potentially *all* users of phones in the geofence." *In re Search*, 481 F. Supp. 3d at 744, 746, 751; *see also In re Search of Info. that is Stored at the Premises Controlled by Google*, 542 F. Supp. 3d 1153, 1157 (D. Kan. 2021) ("If a geofence warrant is likely to return a large amount of data from individuals having nothing to do with the alleged criminal activity . . . the sheer amount of information lessens the likelihood that the data would reveal a criminal suspect's identity, thereby weakening the showing of probable cause.").

Moreover, any officer would logically understand that where, as here, a geofence in an urban area has a diameter longer than three football fields, it will sweep in an overwhelming number of people and devices for which there is no probable cause to search. *See In re Search*, 542 F. Supp. 3d at 1158 (rejecting a geofence warrant application in part because the warrant failed to address that the geofenced area included a business unrelated to the alleged crime); *In re Search*, 481 F. Supp. 3d at 752 ("Here, the proposed warrant would admittedly capture the device IDs . . . for all who entered the geofences, which surround locations as to which there is no reason to believe that anyone—other than the Unknown Subject—entering those locations is involved in the subject offense or in any other crime.").

Det. Hylton described the geographical area targeted as "[a]n area encompassing the Call Federal Credit Union and an adjacent business the UNSUB

fled towards following the robbery," J.A. 111, but he failed to inform the magistrate that the credit union was "located in a busy part of the Richmond metro area," J.A. 1361, or that the geofenced area included the Journey Christian Church and its parking lot, J.A. 1351. As federal magistrate judges have observed, in "busy urban areas . . . where the geofences already extended at least slightly into areas where uninvolved persons might have traversed, even small-scale expansions of the geofences increased the likelihood of capturing the identities and locations of uninvolved persons, providing another reason why the warrant was overbroad." *In re Search*, 481 F. Supp. 3d at 745; *accord In re Search of: Info. Stored at Premises Controlled by Google*, No. 20 M 297, 2020 WL 5491763, at *5 (N.D. Ill. July 8, 2020). An objectively reasonable officer would know not to rely on a warrant purportedly authorizing such an overbroad search.[6]

[6] The only published opinions in which federal magistrate judges have approved geofence warrants involve geofenced areas that were purposefully narrowed "to ensure that location data, with a fair probability, will capture evidence of the crime only." *In re Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d 345, 357 (N.D. Ill. 2020); *accord In re Search of Info. that Is Stored at the Premises Controlled by Google*, 579 F. Supp. 3d 62, 85 (D.D.C. 2021) ("[I]n contrast to the other published cases on geofence warrants, the request for location information here does not have the potential of sweeping up the location data of a substantial number of uninvolved persons."). While the Middle District of Alabama applied the good-faith exception to admit evidence obtained from a geofence warrant, the radiuses of the geofences there were 40 meters and 100 meters, as opposed to the 150-meter radius here, and the court there engaged in remarkably little analysis as it sought to avoid the "journey into the quagmire of geofence search warrants." *United States v. Davis*, No. 2:21-cr-

To the extent the government argues that Det. Hylton attempted to establish that there was probable cause to obtain information associated with other devices, any reasonably well-trained officer would recognize such an attempt as futile. Det. Hylton's affidavit states that "location data can assist investigators in forming a fuller geospatial understanding and timeline related to a specific criminal investigation; and may tend to identify potential witnesses and/or suspects," and "[s]uch information can also aid investigators in possibly inculpating or exculpating persons of interest." J.A. 113. The most generous reading of this language "resembles an argument that probable cause exists because those users were found in the place to be searched, i.e., the place as to which probable cause exists to believe the offense happened." *In re Search*, 481 F. Supp. 3d at 751. No reasonable officer could think that an affidavit provides sufficient indicia of probable cause to locate numerous devices when his only rationale is "mere propinquity to others independently suspected of criminal activity." *See Ybarra*, 444 U.S. at 91; *Owens ex*

101-MHT-JTA, 2022 WL 3009240, at *9 (M.D. Ala. July 1, 2022), *report and recommendation adopted,* No. 2:21CR101-MHT, 2022 WL 3007744 (M.D. Ala. July 28, 2022). The District Court for the District of Columbia denied a defendant's motion to suppress when law enforcement relied on a geofence warrant to obtain information about people at the Capitol building on January 6, 2021, but explained that "January 6 was a unique event in a geographically unusual place such that the scope of probable cause was uncommonly large," and the geofence warrant there contained an extra safeguards at each step of the search to limit the government's discretion. *United States v. Rhine*, No. 21-0687 (RC), 2023 WL 372044, at *29 (D.D.C. Jan. 24, 2023).

rel. Owens v. Lott, 372 F.3d 267, 277, 279 (4th Cir. 2004) (warrant authorizing search of "all persons" at a residence is unconstitutional unless it establishes probable cause to believe "all persons present at [the subject residence] would be involved in criminal activity") (alteration in original); Appellant's Br. 26–27.

Because it was objectively unreasonable to rely on a warrant that made no attempt to establish probable cause for all but one of the devices that would be swept up in the search, exclusion remains the appropriate remedy.

B. The warrant was so facially deficient in failing to particularize the place to be searched and information to be seized that a reasonable officer would not presume it to be valid.

The good-faith exception cannot apply where a warrant is "so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid." *Leon*, 468 U.S. at 923. A warrant is facially deficient unless it "identifies the items to be seized by their relation to designated crimes" and "the description of the items leaves nothing to the discretion of the officer executing the warrant." *United States v. Williams*, 592 F.3d 511, 519 (4th Cir. 2010). Without this particularized description, individuals are not "secure in their persons, houses, papers, and effects from intrusion and seizure by officers acting under the unbridled authority of a general warrant." *Stanford v. Texas*, 379 U.S. 476, 481 (1965).

The geofence warrant in this case was a general warrant. *See* Appellant's Br. 36, 48–49. It indiscriminately authorized a search of any and all devices that were likely near a 17.5-acre area at some point during an hour-long period. It provided no details about the particular places to be searched and data to be seized, and made no attempt to identify a relationship between the many phones that would be subject to search and the alleged crime. Similar to a geofence warrant application that was rejected by a district court in Kansas, Det. Hylton's warrant application "d[id] not explain the extent to which the geofence, combined with the margin of error, is likely to capture uninvolved individuals from . . . surrounding properties." *In re Search*, 542 F. Supp. 3d at 1158.

The warrant states that, at Step 1, Google will return anonymized information that includes "a numerical identifier for the account, the type of account, time stamped location coordinates and the data source that this information came from if available." J.A. 110. Conspicuously missing from this list is another crucial piece of information that Google provides at Step 1: a confidence interval for each data point. J.A. 1345–46. The confidence interval is a circle around each location data point that "indicates Google's confidence in its estimation." J.A. 1334. Google provides these confidence intervals, because it cannot pinpoint locations "with absolute precision." *Id.* Instead, "'Google aims to accurately capture roughly 68 percent of users' within its confidence intervals." J.A. 1334–35 (quoting J.A. 629). "'[I]n other words, there

[is] a 68 percent likelihood that a [Google] user is somewhere inside' the confidence interval." J.A. 1335 (first and second alteration in original) (quoting J.A. 629). Thus, there is a 32 percent likelihood that a user was not inside the confidence interval—and, in some cases, not inside the geofenced area at all. Indeed, the largest confidence interval that was provided in response to the instant geofence warrant had a radius more than twice as large as the original geofence area, meaning Google was 68% certain that the user was somewhere within a 470,513-square-meter area that overlapped with the 70,686-square-meter geofence area. J.A. 1357. The geofence warrant therefore authorized the government at Step 2 to "obtain[] two hours of unrestricted location data for an individual who perhaps had only driven within the outer vicinity of the crime scene," J.A. 1371, an area that included "several buildings (with an unknown number of floors), including a Ruby Tuesday restaurant, a Hampton Inn Hotel, several units of the Genito Glen apartment complex, a self-storage business, a senior living facility, two busy streets . . . , and what appear to be several residences," J.A. 1357.

When the District Court finally learned about these facts through extensive litigation, it opined that "the notion that geofences *can* capture information from users who are not even in the vicinity of the relevant area troubles the Court and evinces how broad a sweep these warrants may have." J.A. 1357 n.29. Because the

magistrate was not fully informed, the officer's reliance on that warrant was unreasonable.

Moreover, an objectively reasonable officer would recognize the warrant in this case as facially deficient because, far from leaving no discretion to the executing officers, *Williams*, 592 F.3d at 519, the officer had "unlimited discretion . . . with respect to learning the identities of the persons whose devices showed up on the anonymized list(s) in the second stage of the protocol." *In re Search*, 481 F. Supp. 3d at 746. The process was "completely devoid of any meaningful limitation," and "did not satisfy the Fourth Amendment's particularity requirement because it gave law enforcement agents unbridled discretion to obtain identifying information about each device detected in the geofences." *Id.*

Here, the warrant specified only that the officer would "*attempt to* narrow down the list" of account information provided in Step 1 "by reviewing the time stamped location coordinates for each account and comparing that against the known time and location information that is specific to this crime." J.A. 110 (emphasis added). The premise of the warrant is that the officer and Google employees—without a magistrate—work together to determine whose information will be disclosed. "As such, the warrant puts no limit on the government's discretion to select the device IDs from which it may then derive identifying subscriber information from among the anonymized list of Google-connected devices that

traversed the geofences." *In re Search*, 481 F. Supp. 3d at 754. The district court thus correctly determined that Steps 2 and 3 "improperly provided law enforcement and Google with unbridled discretion to decide which accounts will be subject to further intrusions," J.A. 1365, a defect obvious on the face of the warrant.

The geofence warrant therefore plainly violated the requirement that, "[a]s to what is to be taken, nothing is left to the discretion of the officer executing the warrant." *Marron*, 275 U.S. at 196. "Given that the particularity requirement is set forth in the text of the Constitution, no reasonable officer could believe that a warrant that plainly did not comply with that requirement was valid." *Groh v. Ramirez*, 540 U.S. 551, 563 (2004).

C. The good-faith exception is inapplicable because the government's search process represented a patent departure from the magistrate's prescribed role under the Fourth Amendment.

The good-faith exception does not apply where "the magistrate fails to perform a 'neutral and detached' function." *United States v. Gary*, 528 F.3d 324, 329 (4th Cir. 2008). Here, the magistrate issued a warrant that improperly delegated to Google and the police the decision of which accounts should be subject to de-anonymization. J.A. 1365. In other words, the officer asked and the magistrate agreed to leave it to non-judicial officers to determine whether there was probable cause for further searches of each account that had been captured and examined in Steps 1 and 2. This is a clear abdication of the magistrate's responsibility, and one

that any "reasonably well trained officer," *Leon*, 468 U.S. at 923, would recognize, as it is well established that probable cause determinations must be overseen by a magistrate. *See United States v. E.D. Mich.* (*Keith*), 407 U.S. 297, 316 (1972) ("[T]he very heart of the Fourth Amendment directive" is that a search requires "*both* the efforts of the officer to gather evidence . . . *and* the judgment of the magistrate that the collected evidence is sufficient to justify invasion of a citizen's private premises or conversation.") (emphasis added).

"[O]ur basic constitutional doctrine" holds that "individual freedoms will best be preserved through a separation of powers and division of functions among the different branches and levels of Government." *Id.* at 317. Google is not one of those branches, and neither it nor the police possess the "objective mind" needed to "weigh the need to invade that privacy in order to enforce the law." *See McDonald v. United States*, 335 U.S. 451, 455 (1948). "When the right of privacy must reasonably yield to the right of search is, as a rule, to be decided by a judicial officer." *Johnson v. United States*, 333 U.S. 10, 14 (1948). As a Virginia judge put it when rejecting a geofence warrant application, "[t]he police want to unilaterally tell Google which cell phones it wants to unmask to obtain the owner's personal information. The Court may not give police this judicial discretion." *In re Search of Info. Stored at the Premises Controlled by Google*, No. KM-2022-79, 2022 WL 584326, at *9 (Va. Cir. Ct. Feb. 24, 2022).

Moreover, the geofence warrant application that Det. Hylton presented to the magistrate consisted of little more than boilerplate language.[7] Indeed, police have been submitting virtually identical applications for warrants across the country, in investigations ranging from a hospital employee's stolen wallet, to a string of neighborhood vehicle burglaries, to arson.[8] Boilerplate language indicates that police are not tailoring their applications to the particular facts of the case, and are rotely reproducing the provisions asking magistrates to abdicate their judicial role and delegate judicial functions to police and Google.

"Prior review by a neutral and detached magistrate is the time-tested means of effectuating Fourth Amendment rights." *Keith*, 407 U.S. at 318. Here, the warrant instead left law enforcement and Google to decide, mid-search amongst themselves, with no questions asked, whether there was a reason to track and/or identify users. J.A. 1376. In doing so, the warrant ensured that the magistrate abdicated his responsibility and did not "perform his neutral and detached function," making the

[7] Det. Hylton used a "go by," which is a "template document[] that outline[s] 'specific information that [Google] need[s] in order to process the search warrant,'" J.A. 1369 n.36 (third and fourth alteration in original) (quoting J.A. 969–70).

[8] *See, e.g.*, Affidavit for Search Warrant No. 2344001 (Utah 2d Dist. Ct. Nov. 8, 2021); Affidavit for Search Warrant No. 2351121 (Utah 2d Dist. Ct. Nov. 22, 2021); Affidavit for Search Warrant, *In re Accounts Associated with Devices that Were Inside the Area* (Wake Cty. N.C. Super. Ct. May 5, 2017), *available at* https://www.documentcloud.org/documents/4388574-20170505-arson-warrant.html.

good-faith exception inapplicable. *Smith v. Munday*, 848 F.3d 248, 255 (4th Cir. 2017) (quoting *Leon*, 468 U.S. at 914); J.A. 1350.

III. Regardless of whether the good-faith exception applies, the Court should address whether the geofence warrant violates the Fourth Amendment.

Before determining whether the good-faith exception applies, this Court should decide whether the geofence search violated the Fourth Amendment. This will provide law enforcement officers and magistrate judges with much-needed guidance, and guard against future unconstitutional searches. When a case presents a "novel question of law whose resolution is necessary to guide future action by law enforcement officers and magistrates, there is sufficient reason for the Court to decide the violation issue *before* turning to the good-faith question." *Illinois v. Gates*, 462 U.S. 213, 264, 265 n.18 (1983) (White, J., concurring) (citing *O'Connor v. Donaldson*, 422 U.S. 563 (1975)); *see also United States v. Dahlman*, 13 F.3d 1391, 1397 (10th Cir. 1993) ("[A] close reading of *Leon* reveals that, while the Supreme Court intended to vest lower courts with discretion, the preferred sequence is to address the Fourth Amendment issues before turning to the good faith issue unless there is no danger of 'freezing' Fourth Amendment jurisprudence or unless the case poses 'no important Fourth Amendment questions.'" (quoting *Leon,* 468 U.S. at 924–25)). This case unquestionably poses novel and important Fourth Amendment questions. Geofence warrants present "a complex topic, requiring a

detailed, nuanced understanding and application of Fourth Amendment principles." J.A. 1383. The number of geofence warrant requests has been dramatically increasing, J.A. 1343, and their highly intrusive nature calls out for the application of clear judicial standards.

As the Sixth Circuit has recognized, "[i]f every court confronted with a novel Fourth Amendment question were to skip directly to good faith, the government would be given *carte blanche* to violate constitutionally protected privacy rights." *United States v. Warshak*, 631 F.3d 266, 282 n.13 (6th Cir. 2010). "[P]olice officers might shift the focus of their inquiry from 'what does the fourth amendment require?' to 'what will the courts allow me to get away with?'" Potter Stewart, *The Road to* Mapp v. Ohio *and Beyond: The Origins, Development and Future of the Exclusionary Rule in Search-and-Seizure Cases*, 83 Colum. L. Rev. 1365, 1403 (1983).

This appeal presents a well-developed record following extensive discovery by the defense, permitting the Court to provide an informed answer to the Fourth Amendment question. Given the government's history of concealing material facts about novel surveillance techniques from the courts, *supra,* Section I, this Court should not withhold much-needed guidance on the constitutional status of geofence warrants.

Additionally, robust development of Fourth Amendment law is crucial for ensuring that constitutional rights remain protected as law enforcement techniques evolve. While courts typically discuss the exclusionary rule's deterrence function with respect to police practices, "[a] failure by the appellate courts to accurately assess Fourth Amendment interests in the course of announcing the law has the same impact as the failure of the police to follow the law." Orin S. Kerr, *Good Faith, New Law, and the Scope of the Exclusionary Rule*, 99 Geo. L. J. 1077, 1090 (2011). Whether a constitutional violation arises from a police officer's own misunderstanding or irreverence for constitutional rights, or insufficient guidance from the courts as to which police practices are unconstitutional, constitutional rights are left unprotected and more-readily violated in the future.

Finally, reaching the merits here is necessary to provide guidance to magistrate judges, who rely on Fourth Amendment precedent to determine whether to issue a warrant based on an officer's application. *See, e.g.*, J.A. 1330 ("There is a relative dearth of case law addressing geofence warrants"); *In re Search*, 542 F. Supp. 3d at 1154 ("The court issues this written order not only to address the subject application, but also to provide guidance for future search warrant applications involving geofence technology given the relatively sparse authority on this issue.").

This Court should hold that the magistrate's issuance of the geofence warrant in this case was in error so that magistrates do not continue to enable constitutional

violations against defendants like Mr. Chatrie—and against the countless innocent individuals swept up in geofence searches.

CONCLUSION

For these reasons, the Court should first hold that the geofence search violated the Fourth Amendment and then that the good-faith exception does not apply.

January 27, 2023

Respectfully submitted,

/s/ Nathan Freed Wessler

Jennifer Stisa Granick
American Civil Liberties Union Foundation
39 Drumm Street
San Francisco, CA 94111
Tel.: (415) 343-0758
jgranick@aclu.org

Eden B. Heilman
Matthew W. Callahan
American Civil Liberties Union Foundation of Virginia
P.O. Box 26464
Richmond, VA 23261
Tel.: (804) 523-2146
eheilman@acluva.org
mcallahan@acluva.org

William F. Nettles, IV
Federal Public Defender

Nathan Freed Wessler
Ashley Gorski
Patrick Toomey
Brandon Buskey
Trisha Trigilio
Laura Moraff
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
Tel.: (212) 549-2500
nwessler@aclu.org[9]

Brian J. Kornbrath
Federal Public Defender
Northern District of West Virginia
230 West Pike Street
Suite 360
Clarksburg, WV 26301

[9] Counsel thank ACLU law-graduate fellow Kimberly Saltz for her assistance in preparing this brief.

District of South Carolina
1901 Assembly Street
Suite 200
Columbia, SC 29201

G. Alan Dubois
Federal Public Defender
Eastern District of North Carolina
150 Fayetteville Street
Suite 450
Raleigh, NC 27601

Louis Allen
Federal Public Defender
Middle District of North Carolina
301 N. Elm Street
Suite 410
Greensboro, NC 27401

Juval O. Scott
Federal Public Defender
Western District of Virginia
210 First Street, SW
Suite 400
Roanoke, VA 24011

John Baker
Federal Public Defender
Western District of North Carolina
129 West Trade Street
Suite 300
Charlotte, NC 28202

James Wyda
Federal Public Defender
District of Maryland
100 South Charles Street
Tower II, 9th Floor
Baltimore, MD 21201

Wesley P. Page
Federal Public Defender
Southern District of West Virginia
300 Virginia Street East
Room 3400
Charleston, WV 25301

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Fed. R. App. P. 32(a) because it contains 6,499 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f).
2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type-style requirements of Fed. R. App. P. 32(a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Word 2010 in 14-point Times New Roman.

Dated: January 27, 2023

/s/ Nathan Freed Wessler

Nathan Freed Wessler
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
Tel.: (212) 5249-2500
nwessler@aclu.org

Counsel of Record for Amici Curiae

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 27th day of January, 2023, the foregoing Brief of *Amici Curiae* was filed electronically through the Court's CM/ECF system. Notice of this filing will be sent by email to all parties by operation of the Court's electronic filing system.

Dated: January 27, 2023

/s/ Nathan Freed Wessler
Nathan Freed Wessler
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
Tel.: (212) 5249-2500
nwessler@aclu.org

Counsel of Record for Amici Curiae