No. 22-4489

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

UNITED STATES OF AMERICA,
***Plaintiff/Appellee*,**

v.

OKELLO T. CHATRIE,
***Defendant/Appellant*.**

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

BRIEF OF THE APPELLANT

MICHAEL W. PRICE
National Association of Criminal Defense Lawyers
Litigation Director, Fourth Amendment Center
1660 L Street NW, 12th Floor
Washington, DC 20036
(202) 465-7615
mprice@nacdl.org

GEREMY C. KAMENS
Federal Public Defender

Laura J. Koenig
Assistant Federal Public Defender
701 East Broad Street, Suite 3600
Richmond, VA 23219
(804) 565-0800
laura_koenig@fd.org

Counsel for Appellant

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Constitutional Provisions, Statutes, and Rules

No. 22-4489

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

UNITED STATES OF AMERICA,
Plaintiff/Appellee,

v.

OKELLO T. CHATRIE,
Defendant/Appellant.

On Appeal From the United States District Court
for the Eastern District of Virginia
Alexandria Division (The Hon. M. Hannah Lauck)

BRIEF OF THE APPELLANT

STATEMENT OF JURISDICTION

The district court had jurisdiction over this federal criminal case pursuant to 18 U.S.C. § 3231. That court entered the judgment of conviction and sentence against Okello Chatrie on August 19, 2022. J.A. 1449. Mr. Chatrie timely filed his notice of appeal on August 25, 2022. J.A. 1456; *see* Fed. R. App. P. 4(b)(1), (b)(6). Therefore, this Court has jurisdiction over this appeal pursuant to 28 U.S.C. § 1291.

STATEMENT OF THE ISSUES

I. Whether the good-faith doctrine applies to a "geofence" search where a state magistrate (1) abandoned his judicial role in issuing a warrant that was (2) so lacking in probable cause and (3) facially deficient that no objective officer could rely on it.

II. Whether a geofence search is a general warrant, to which the good-faith doctrine does not apply.

STATEMENT OF THE CASE

A. The Geofence Warrant

Someone robbed the Call Federal Credit Union in Richmond, Virginia, on May 20, 2019. There were plenty of witnesses and surveillance videos, but law enforcement still had no suspects nearly a month later. That was when investigators decided to try something radically different. The Chesterfield County Police Department, working with the FBI, asked a Virginia state magistrate to approve a new type of search—a "geofence warrant"—that forced Google to sleuth through "numerous tens of millions" of accounts and then allowed law enforcement to decide which accounts to search further. J.A. 1331; J.A. 1555.

A geofence warrant requires Google to produce data on all devices using Google "Location History" within a geographic area during a given window of time. According to Google, "roughly one-third of active Google users (i.e., numerous tens of millions of Google users)" had Location History enabled in 2019. J.A. 1555. But unlike a typical

warrant for location data, a geofence warrant does not identify individuals or suspects in any way. Instead, it operates in reverse: it requires Google to search an ocean of private data—the "Sensorvault"—and allows police the discretion to obtain private information from devices of interest.

Det. Joshua Hylton drafted the geofence warrant here, which drew a circle around the bank measuring 300 meters in diameter. That circle covered 17.5 acres of an urban area, and included not only the bank and parking lot, but also the entire Journey Christian Church nearby. J.A. 1351. The warrant did not account for the way Google estimates location, *see* J.A. 1334-1335; J.A. 1356-1358, or specify how to count which devices were in the circle. As a result, the search could have captured devices that were hundreds of feet outside the circle, including "several buildings (with an unknown number of floors), [] 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 (Hull Street and Price Club Boulevard), and what appear to be several residences." J.A. 1357. In fact, Mr. Chatrie identified at least one "false positive" in the results here. *See* J.A. 1358; J.A. 1370-1371. As the court determined, "this Geofence Warrant captured location data for a user who may not have been *remotely* close enough to the Bank to participate in or witness the robbery." J.A. 1370.

Det. Hylton brought the warrant to Chesterfield County Magistrate David Bishop, who had recently graduated from Pensacola Christian College and did not have a law degree. *See* J.A. 1385-1388. Magistrate Bishop completed his statutorily required probationary period three months before Det. Hylton presented him with the geofence warrant here. J.A. 1350. Magistrate Bishop asked no questions of Det. Hylton, did not seek to modify anything, and did not read the warrant in front of Det. Hylton. J.A. 1350. It was the first geofence warrant Magistrate Bishop had signed. J.A. 1350. And it outlined a novel, 3-step process, as detailed below.

1. Step 1

Step 1 required Google to provide "anonymized information" for devices "inside" the circle between 4:20 and 5:20 p.m. J.A. 1352. Google, however, "has no way to know ex ante which users may have [Location History] data indicating their potential presence in particular areas at particular times." J.A. 134. As a result, Step 1 required Google to "search across all [Location History] journal entries to identify users with potentially responsive [Location History] data, then run a computation against every set of coordinates to determine which [Location History] records match the time and space parameters in the warrant." J.A. 134-135. In other words, it required searching all of the "numerous tens of millions" of Google users who had Location History enabled. The warrant made no mention of this fact.

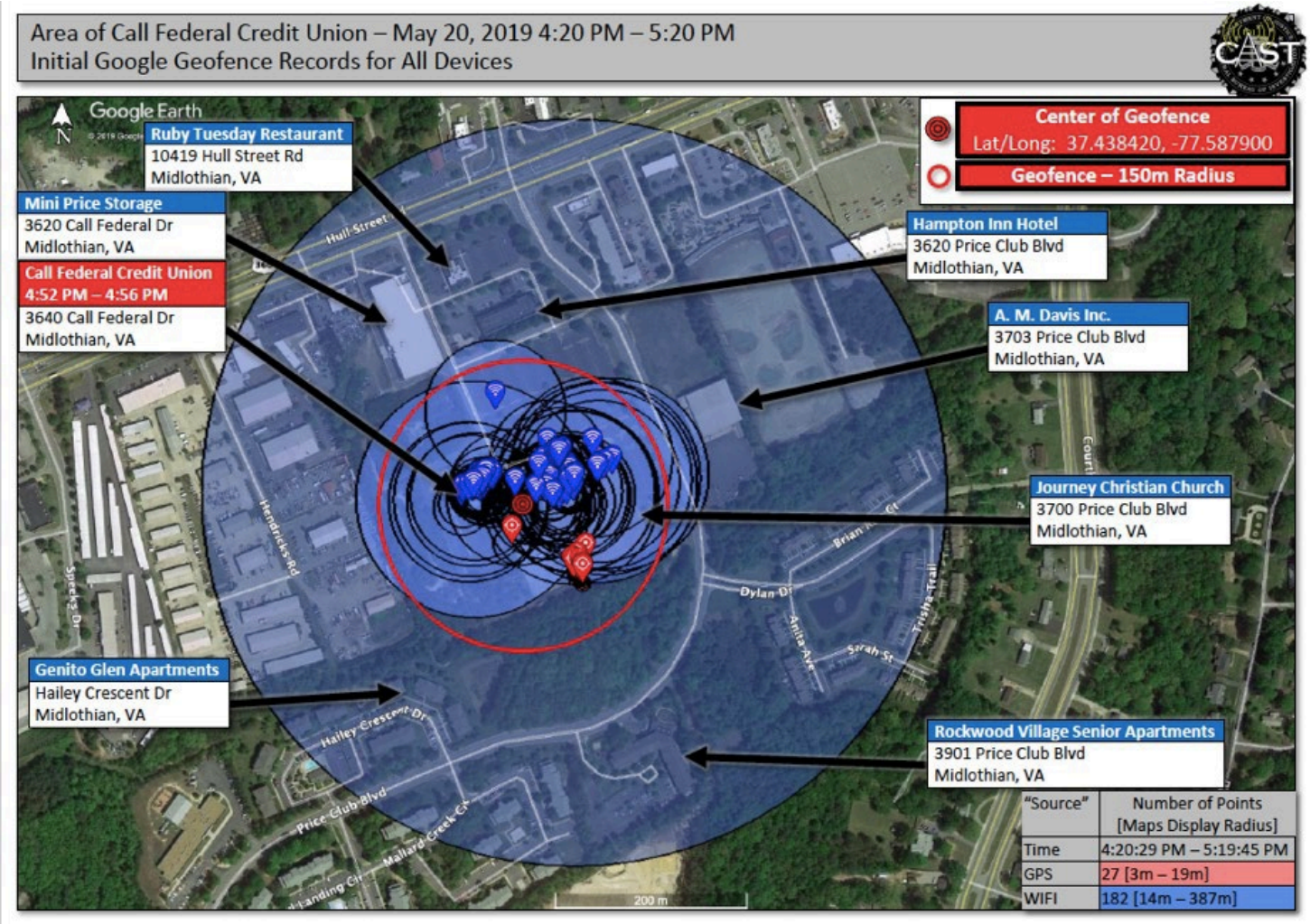
Similarly, Det. Hylton's affidavit cited his "training and experience" before describing how Google collects location data, noting that it is "derived from GPS data, cell site/cell tower information, Bluetooth connections, and Wi-Fi access points." J.A. 111. But Det. Hylton omitted that Location History is merely Google's *estimation* of a device's coordinates, and that Google's confidence in its estimation can vary significantly. As the district court explained, "When Google, through Location History, reports a device's estimated location by placing a point on a map, it also depicts around that point a 'confidence interval'—a circle of varying sizes—which indicates Google's confidence in its estimation." J.A. 1334. That confidence interval can be as small as three meters, but it can also be hundreds or thousands of meters. *See* J.A. 1334. Critically, Google is no more confident that a device is at the dot in the center of the circle as opposed to somewhere off near the edge. Consequently, when a confidence interval (also known as the "Map Display Radius") extends beyond the geofence, it is just as likely that a device was outside the geofence as inside it. Det. Hylton did not inform the court of this problem or take steps to mitigate it, such as only requesting devices whose confidence interval did not exceed the bounds of the geofence.[1]

Det. Hylton obtained the warrant on June 14, 2019, and served it to Google on June 20, 2019. J.A. 1352-1353. But, "[i]nexplicably, on June 19, 2019—*the day before*

[1] As the district court noted, the government has adopted a more conservative approach in other cases. J.A. 1375 (describing a warrant from D.D.C. that "sought only location data that fell *within* the geofence").

he sent the Warrant to Google—Det. Hylton submitted his return for the Warrant to the Chesterfield County Circuit Court." J.A. 1353. The return described the items seized as simply "Data," having not yet executed it. J.A. 1354.

In fact, Google provided the Step 1 results on June 28, 2019, in the form a ".csv" file (a spreadsheet). J.A. 2094. It included the Location History data for 19 unique Google users, yielding 209 location points over an hour. J.A. 2098-2104. For each of the 19 users, the data included columns indicating the "Device ID," "Date," "Time," "Latitude," "Longitude," "Source," and "Maps Display Radius" (the confidence interval). J.A. 2098; J.A. 1354. Law enforcement then imported this data into mapping software to render the depiction below. J.A. 1356.



The red circle represents the geofence drawn in the warrant. The blue and red icons represent the latitude and longitude coordinates. And the shaded blue circles represent the confidence interval for each of those points. The largest confidence interval is 387 meters, more than twice the size of the geofence. J.A. 1357. Critically, that device is equally likely to be anywhere in the largest shaded circle. As the district court explained:

> [T]hat person may have been dining inside the Ruby Tuesday restaurant nearby. The person may have been staying at the Hampton Inn Hotel, just north of the Bank. Or, he or she could have been inside his or her own home in the Genito Glen apartment complex or the nearby senior living

> facility. He or she may have been moving furniture into the nearby self-storage business. Indeed, the person may have been simply driving along Hull Street or Price Club Boulevard. Yet the government obtained the person's location data just the same.

J.A. 1370.

None of this information was returned to the Chesterfield County Circuit Court. J.A. 1354. Instead, without consulting a magistrate or judge, Det. Hylton proceeded to seek additional location data on all 19 users in Step 2.

2. Step 2

Step 2 required law enforcement to "narrow down" the list of devices, after which Google would produce additional, "contextual" data for that subset. J.A. 1352. According to the warrant, this would entail expanding the timeframe from one to two hours, with no geographical restrictions. J.A. 1352. In other words, it would allow law enforcement to see wherever a device traveled, for an hour before and an hour after the robbery. Google would then send law enforcement another spreadsheet containing this additional data. J.A. 110.

Det. Hylton did not follow this process, however. Instead, as the court found, the "record [] strongly suggests that he did not 'attempt to narrow down' the list of devices for which he requested further data." J.A. 1354. Without consulting Magistrate Bishop, Det. Hylton "requested 'additional location data' (Step 2 data) *and* 'subscriber information' (Step 3 data) 'for *all* 19 device numbers produced in [S]tep 1.'" J.A. 1354.

When he did not receive a response from Google, he left two voicemails and spoke to a Google "Legal Information Specialist" later the same day. J.A. 1038-1039; J.A. 1059.

Google specifically advised Det. Hylton that his request "did not appear to follow the three sequential steps or the narrowing required by the search warrant." J.A. 1355. According to the specialist, it did not appear Det. Hylton was familiar with the process outlined in the warrant, requiring her to explain the nature of the data to be turned over and emphasizing "the importance of [S]tep 2 in narrowing." J.A. 1355; J.A. 1584. Following that call, Det. Hylton emailed Google to request Step 2 data on *nine* of the 19 users. Google then created another database file on July 9, 2019, containing the "contextual" data for those nine users and sent it to the government. *See* J.A. 1355. This file included 680 location points over a total of two hours. *See* J.A. 2139. At no point did Det. Hylton contact Magistrate Bishop with respect to which users would be subject to this additional search and seizure. J.A. 1354.

The second spreadsheet, like the one before it, included only a numeric "Device ID" for each of the nine users—but this data was hardly anonymous. Through expert testimony, Mr. Chatrie demonstrated that it was possible to plot these data points, and using publicly available information, determine the likely identity of at least three individuals. J.A. 1358-1359. Furthermore, once law enforcement had a list of "anonymized" Device IDs, it could have obtained full subscriber information by simply issuing a subpoena to Google. *See In re Information Stored at Premises Controlled by*

Google ("Fuentes Opinion"), 481 F. Supp. 3d 730, 754 (N.D. Ill. 2020) (finding that there is "no practical difference between a warrant that harnesses the technology of the geofence, easily and cheaply, to generate a list of device IDs that the government may easily use to learn the subscriber identities, and a warrant granting the government unbridled discretion to compel Google to disclose some or all of those identities.").

3. Step 3

Step 3 required Google to provide "identifying account information/CSI" for a final subset of accounts, as determined by law enforcement. J.A. 1352. Det. Hylton requested and received this data for three device numbers. J.A. 1355-1356. But as the district court noted, "it is not apparent from the record whether Det. Hylton demonstrated to Google why he requested Step 3 data for these three accounts, nor did he seek the magistrate's approval before obtaining the data." J.A. 1356.

Furthermore, after receiving the Step 3 data, Det. Hylton requested "*additional* device or phone number information that could be associated with one of the accounts." J.A. 1356. As the court put it, "[t]his would have been an unauthorized Step 4" and as a result, Google did not produce further any further information under the geofence warrant. J.A. 1356.

B. Motion to Suppress

Based on the three geofence returns, law enforcement identified Mr. Chatrie as a suspect in the robbery, for which he was later arrested and indicted. Mr. Chatrie moved to suppress the results of the geofence warrant, as well as all fruits thereof. J.A.

25. Mr. Chatrie argued that the geofence warrant was an impermissible general warrant, and in the alternative, that it wholly failed to satisfy the Fourth Amendment's probable cause and particularity requirements. J.A. 27. Mr. Chatrie also argued that the *Leon* good-faith exception should not apply for three reasons: (1) the warrant affidavit lacked a substantial basis to determine probable cause; (2) it was so facially deficient that no officer could have reasonably presumed it was valid; and (3) the magistrate abandoned his judicial role.[2] *See* J.A. 48-49; J.A. 1110-1115; *United States v. Leon*, 468 U.S. 897, 923 (1984).

C. The Court's Opinion

Following extensive briefing and testimony, the district court issued a 63-page written opinion finding the geofence warrant "plainly violate[d]" the Fourth Amendment and was unconstitutional for lack of probable cause and particularity. J.A.

[2] This Court could also find that Det. Hylton recklessly omitted material information in violation of *Leon* and *Franks v. Delaware*. *See Leon*, 468 U.S. at 914 (citing *Franks*, 438 U.S. 154 (1978) (stating that the good faith exception does not apply where a warrant is based on knowing or recklessly false statements)). This rule "also applies when affiants omit material facts 'with the intent to make, or in reckless disregard of whether they thereby made, the affidavit misleading.'" *United States v. Colkley,* 899 F.2d 297, 300 (4th Cir.1990). Although Mr. Chatrie did not request a *Franks* hearing before the district court, the record below and testimony of Det. Hylton demonstrates that the detective acted with reckless disregard for the truth, failing to disclose the true nature and scope of the geofence search. As Mr. Chatrie repeatedly argued, these material omissions would have made it abundantly clear to a neutral magistrate that law enforcement lacked probable cause to search anyone's Location History, let alone "numerous tens of millions" or Mr. Chatrie's specifically. *See* J.A. 48-49; J.A. 390-391; J.A. 1115.

1328; *see also* J.A. 1361. The court made detailed findings of fact, much of which have been summarized above. The court also included a comprehensive description of how Location History functions, how it can be easily enabled, and how it can be difficult to stop or delete. J.A. 1331-1343.

1. Fourth Amendment Interest

The court began its analysis by addressing "standing"—*i.e.*, whether Mr. Chatrie "ha[d] a reasonable expectation of privacy in the data sought by the geofence warrant." J.A. 1361-1364. Although the court ultimately assumed, without holding, that the warrant constituted a Fourth Amendment "search," J.A. 1361-1362; J.A. 1368, the opinion provided sound reasoning for finding that Mr. Chatrie did have a privacy interest in his Location History data, regardless of the so-called "third-party doctrine." *See* J.A. 1362-1364; J.A. 1378-1380.

The court noted its "deep concern … that current Fourth Amendment doctrine may be materially lagging behind technological innovations" with respect to "both Fourth Amendment standing, and the third-party doctrine." J.A. 1362. Citing the Supreme Court's landmark decision in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), as well as this Court's *en banc* opinion in *Leaders of a Beautiful Struggle v. Baltimore Police Dep't,* 2 F.4th 330, 341 (4th Cir. 2021), Judge Lauck strongly suggested that Mr. Chatrie had a Fourth Amendment privacy interest in his Location History data. J.A. 1362-1364; J.A. 1378-1380. While the two hours of Location History

here was less than the seven days of cell site location information ("CSLI") at issue in *Carpenter*, the court recognized that Location History is more "powerful" than the information in *Carpenter*, *see* J.A. 1332; J.A. 1380, and more like the data in *Leaders*, J.A. 1362.

The court reached this view due, in part, to the "retrospective quality" of geofence data that "enables police to retrace a person's whereabouts, [without] know[ing] in advance whether they want to follow a particular individual, or when." J.A. 1358 (internal quotations omitted, quoting *Carpenter*, 138 S. Ct. at 2218). As the court explained, "although *law enforcement* limited the warrant's window to two hours, Google—despite efforts to constrain law enforcement access to its data—retains constant, near-exact location information for each user who opts in." J.A. 1362. As a result, law enforcement has "an almost unlimited pool from which to seek location data, and '[w]hoever the suspect turns out to be,' they have 'effectively been tailed' since they enabled Location History." J.A. 1362 (citing *Leaders*, 2 F.4th at 341). Indeed, Google "logs a device's location, on average, every two minutes," or about "720 times a day." J.A. 1332. And unlike the CSLI in *Carpenter*, Location History is "always on," even "if the person is not doing anything at all with [his or her] phone." J.A. 1334. As in *Leaders*, the court recognized that the ease of such "precise and essentially real-time location data was unimaginable"—until now. J.A. 1362. And it emphasized that such "expansive, detailed, and retrospective" monitoring is

fundamentally unlike traditional forms of surveillance, deserving of legislative if not judicial intervention. J.A. 1362-1364.

With respect to the third-party doctrine, the district court "expresse[d] its skepticism" in applying it to geofence technology. J.A. 1378. The government claimed that Mr. Chatrie could not have a privacy interest in two hours of location data because he "voluntarily disclosed" the information to Google, but "[t]he Court [thought] otherwise." J.A. 1379. Although Judge Lauck could not ascertain the precise circumstances whether or how Mr. Chatrie "gave consent," the court was "unconvinced that the third-party doctrine would render hollow Chatrie's expectation of privacy in his data." J.A. 1379. This remains true, the court concluded, "even for 'just' two hours" of location data. J.A. 1379. As the court explained, any "affirmative steps" Mr. Chatrie took to enable Location History "likely do not constitute a full assumption of the attendant risk of permanently disclosing one's whereabouts during almost every minute of every hour of every day." J.A. 1379 (noting the "limited and partially hidden warnings provided by Google."); *see also* J.A. 1380 ("[A] user simply cannot forfeit the protections of the Fourth Amendment for years of precise location information by selecting 'YES, I'M IN' at midnight while setting up Google Assistant, even if some text offered warning along the way.").[3]

[3] The court also appeared to recognize Mr. Chatrie's alternative argument that he had a Fourth Amendment property interest in his Location History data. *See* J.A. 1368 (likening it to a "defendant's property that he disclosed to a third party" and

2. Overbreadth

To justify "this sweeping warrant," law enforcement staked its alleged probable cause on "footage depicting the perpetrator holding a phone to his ear—and nothing else," which the district court held was "simply not '[]reasonable.'" J.A. 1370. Law enforcement—unable to locate the suspect despite access to camera footage, witness interviews, and two leads—"simply drew a circle with a 150-meter radius[.]" J.A. 1369-1370.

After stripping away the geofence warrant's "complexities," the court held that the warrant clearly "lacks sufficient probable cause." J.A. 1368. "Indeed," the court emphasized, "it is difficult to overstate the breadth of this warrant, particularly in light of the narrowness of the Government's probable cause showing." J.A. 1369. Supreme Court precedent is clear, the court stated: "warrants must establish probable cause that is 'particularized with respect to the person to be searched or seized.'" J.A. 1368 (quoting *Maryland v. Pringle*, 124 S. Ct. 795, 800 (2003)). But "[t]his warrant did no such thing." J.A. 1368. Rather than establish probable cause to search the "location information for *all* Google account owners who entered the geofence over the span of an hour, … the warrant simply did not include any facts to establish probable cause to collect such broad and intrusive data from each one of these individuals." J.A. 1368-1369. And in fact, it "swept in unrestricted location data for private citizens who had

---

stating that "users ultimately retain at least some joint interest in the location data their phones generate").

no reason to incur Government scrutiny," including one "user who may not have been *remotely* close enough to the Bank to participate in or witness the robbery." J.A. 1369-1370.

The court held that *United States v. McLamb*, 880 F.3d 685 (4th Cir. 2018), was inapposite because, there, "a user's 'mere propinquity' to the [child sexual abuse material] website *did* necessarily establish probable cause: any user visiting the site likely participated in the criminal conduct of viewing or sharing [CSAM]." J.A. 1372. Here, however, "a Google user's proximity to the bank robbery does not necessarily suggest that the user participated in the crime." J.A. 1372. Similarly, the court held that *United States v. James*, No. 18-cr-216 (SRN/HB), 2018 WL 6566000 (D. Minn. Nov. 26, 2018), which involved cellular tower dump data, was not on point because it "did not account for whether probable cause existed to search through [] *other* individuals' location information." J.A. 1373. Rather, *James* "stopped short of considering whether 'particularized' probable cause existed, and it is precisely that lack of narrowly-tailored probable cause that is fatal to this Geofence Warrant." J.A. 1373.

While the court ultimately did not decide "whether a geofence warrant may *ever* satisfy the Fourth Amendment's strictures," J.A. 1373, it held this geofence warrant could not stand because it relied "on precisely the same 'mere propinquity to others' rationale the Supreme Court has already rejected as an appropriate basis for a warrant." J.A. 1375. According to Judge Lauck, the government's "inverted probable cause

argument" was "unpersuasive": law enforcement was not permitted to "seek information based on probable cause that some unknown person committed an offense, and therefore search every person present nearby." J.A. 1375.

3. Particularity

The district court also found that Steps 2 and 3 of the geofence warrant were "undertaken with no judicial review whatsoever[,] improperly provid[ing] law enforcement and Google with unbridled discretion to decide which accounts will be subject to further intrusions." J.A. 1365; *see also* J.A. 1355 ("Neither Det. Hylton nor Google consulted with a magistrate or judge before Google disclosed this [Step 2] data."). And to the extent the government might argue the three-step process cured the warrant's particularized probable cause defects, "such an argument is unavailing." J.A. 1376 ("Steps 2 and 3 … leave the executing officer with *unbridled* discretion and lack any semblance of objective criteria to guide how officers would narrow the lists of users.").

As the court determined, the warrant lacked "language objectively identifying *which* accounts" officers could search; it did not "provide objective guardrails by which officers could *determine* which accounts" to search; nor did it "limit the *number* of devices" to be searched. J.A. 1376. Instead, it "provided law enforcement unchecked discretion to seize more intrusive and personal data with each round of requests—

without ever needing to return to a neutral and detached magistrate for approval." J.A. 1376.

Steps 2 and 3 plainly "'put[] no limit on the [G]overnment's discretion to select the device IDs from which it may then derive identifying subscriber information.'" J.A. 1378 (citation omitted). And as a result, they "fail to provide the executing officer with clear standards from which he or she could 'reasonably … ascertain and identify … the place to be searched [or] the items to be seized.'" J.A. 1378. Therefore, the court held, the government cannot rely on Steps 2 and 3 to provide the lacking particularized probable cause, they "independently fail under the Fourth Amendment's particularity requirement." J.A. 1378.

4. Good Faith

Although the district court agreed that the geofence warrant was unconstitutional for lack of particularity and probable cause, it nonetheless denied Mr. Chatrie's motion to suppress on good-faith grounds. J.A. 1361. The court held the good-faith exception was generally applicable where there was a lack of judicial guidance regarding a novel investigative technique and where law enforcement sought advice from counsel before applying for a warrant that uses the new tool. *See* J.A. 1382 ("[C]ourts generally decline to hold a warrant 'facially deficient where the legality of an investigative technique is unclear and law enforcement seeks advice

from counsel before applying for the warrant.'" (quoting *United States v. McLamb*, 880 F.3d 685, 691 (4th Cir. 2018))).

Det. Hylton—"rel[ying] on his past experience seeking geofence warrants" that had been approved by magistrates and prosecutors—"sought 'advice from counsel before applying for the warrant.'" J.A. 1382-1383 (quoting *McLamb*, 880 F.3d at 691). Because of this case's "complexities," along with Det. Hylton's "prior acquisition of three similar warrants, and his consultation with Government attorneys before obtaining those warrants," the court could not say Det. Hylton's "reliance on the instant warrant was objectively unreasonable" and said suppression would not "'meaningfully deter' improper law enforcement conduct." J.A. 1383 (citation omitted).

The court also did not find that that Magistrate Bishop "wholly abandoned his role as a detached magistrate." J.A. 1384. While he perhaps "*should have* considered the implications of the Warrant more carefully," J.A. 1384, no evidence was produced to show that he "did not read the affidavit"; "that he read it so cursorily as to have wholly abandoned his neutral and detached role"; or that he "acted in a partisan manner or aligned himself with the police." J.A. 1384 (citations omitted).

The court disagreed with Mr. Chatrie's argument that the "magistrate's utter lack of concern regarding the obvious flaws in the warrant," J.A. 1384, should be analyzed under second *Leon* exception (regarding the magistrate's alleged

abandonment of his or her judicial role). Instead, it held the Fourth Circuit has instructed such an allegation should be analyzed under the third *Leon* exception (regarding the supporting affidavit's being "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable"), J.A. 1382 (citation omitted), and decided "that exception does not warrant suppression either." J.A. 1385.

As to Magistrate Bishop's qualifications, the court held his undergraduate "degree likely suffice[d]" to be a magistrate under Virginia law, J.A. 1387, even though he graduated from a school that—while accredited in 2013 by the Transnational Association of Christian Colleges and Schools ("TRACS")—was neither "officially licensed in Florida," nor "accredited by a regional higher-education accrediting agency." J.A. 1386. And even though he "signed this sweeping and powerfully intrusive Geofence Warrant" only three months after he began "serving as a non-probationary magistrate," J.A. 1385-1386, "Virginia sufficiently trains its magistrates to determine probable cause"; and Magistrate Bishop had satisfied the state's requirements to become one. J.A. 1387.

But the court was "not clear … that *any* person just three years out of college should be burdened with the responsibility of approving or rejecting a warrant of this complexity and magnitude." J.A. 1387. Due to "the myriad ways that geofencing instigates a massive intrusion into individual rights, … without notice to potentially

thousands of persons with phones within it," the court felt it was "less than evident that all law enforcement officers" or "most magistrates, with or without a law degree," "have a clear understanding of the invasive scope of these warrants." J.A. 1387-1388. Ultimately, though, the court held that "even if Magistrate Bishop's degree or lack of experience did not qualify him to make this consequential finding, the good faith exception would still apply" because "suppression based on a technical defect of the magistrate's credentials would not serve to deter improper law enforcement conduct." J.A. 1388.

D. Plea and Sentencing

Following the court's denial of his motion to suppress, Mr. Chatrie pleaded guilty to two related counts, filed via criminal information, pursuant to a conditional plea agreement on May 9, 2022. J.A. 1432. The court imposed a sentence of 57 months' incarceration on the first count, and 84 months on the second count, to be served consecutively, followed by three years of supervised release. J.A. 1450-1451. This appeal follows.

SUMMARY OF ARGUMENT

The good-faith doctrine should not apply to the geofence warrant in this case. First, it was so plainly lacking in probable cause that no officer could have reasonably relied on it. *See United States v. Doyle*, 650 F.3d 460, 467 (4th Cir. 2011). Second, it was facially deficient in failing to particularize the data to be searched

and seized, explicitly granting law enforcement the discretion to choose who to target in Steps 2 and 3. And third, the magistrate who signed it wholly abandoned his judicial role in authorizing law enforcement to negotiate with Google over which users to search. Indeed, the geofence warrant was so overbroad and so unparticularized that it is a modern-day general warrant, to which the good-faith doctrine must not apply. The district court erred in finding that consultation with prosecutors could inoculate law enforcement officers' actions, and the court erred in not finding that suppression would produce deterrent benefits. Suppression is appropriate here to ensure that new technologies do not make an end run around the Fourth Amendment.

STANDARD OF REVIEW

When evaluating the applicability of the good-faith exception in the context of a motion to suppress, this Court reviews the district "court's legal conclusions *de novo* and its factual findings for clear error." *See United States v. Lyles*, 910 F.3d 787, 796 (2018) (quoting *United States v. McKenzie-Gude*, 671 F.3d 452, 461 (4th Cir. 2011)).

ARGUMENT

A. The Warrant Lacked a Substantial Basis to Determine Probable Cause

The Fourth Circuit has identified at least four types of cases where the good-faith exception does not apply. One of them is: "if the affidavit supporting the warrant

is so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable." *Doyle*, 650 F.3d at 467 (internal quotations and citation omitted); J.A. 1382. Here, as the court determined, the "warrant simply did not include any facts to establish probable cause," and it was "completely devoid of any suggestion that all—or even a substantial number of—the individuals searched had participated in or witnessed the crime." J.A. 1369. But in contradiction, the court found that it was not "*so* lacking in indicia or probable cause as to render official belief in its existence entirely unreasonable," J.A. 1383, due in large part to the novelty of the technology and the nature of the warrant.

Mr. Chatrie disagrees. The good-faith exception offers no refuge to the government where, as here, a warrant is "completely devoid" of probable cause. The warrant here is a "bare bones" warrant, to which the good-faith doctrine does not apply. *See United States v. Wilhelm*, 80 F.3d 116, 121 (4th Cir. 1996) (finding that the good-faith exception should not apply to a "bare bones" affidavit); *United States v. Griffith*, 867 F.3d 1265, 1278-79 (D.C. Cir. 2017) (declining to apply good-faith exception to evidence seized pursuant to a "bare bones" affidavit); *United States v. Underwood,* 725 F.3d 1076, 1085 (9th Cir. 2013) (equating a "bare bones" affidavit with an affidavit "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable" (quoting *United States v. Leon*, 468 U.S. 897, 923 (1984))); *United States v. Craig*, 861 F.2d 818, 821 (5th Cir. 1988) (referring to

the third *Leon* exception as the "bare bones affidavit exception"); *see also Burns v. United States*, 235 A.3d 758, 779 (D.C. 2020) ("[F]ederal courts have consistently viewed 'bare bones' search warrant affidavits as fitting squarely within the third exception to the good faith exception recognized in *Leon*."). That rule should not change because a warrant is "cloaked" in new technology. J.A. 1383. If anything, law enforcement should be held to a more stringent duty of candor with respect to new surveillance technologies and, as the Supreme Court has suggested, be held to a more "demanding standard of reasonableness" when confronted with the prospect of searching many people unrelated to the crime being investigated. *Maryland v. Garrison*, 480 U.S. 79, 97 (1987).

At bottom, this geofence warrant, like every other warrant, boils down to basics: probable cause and particularity. Every officer is trained to follow these constitutional requirements for obtaining a valid warrant. They are not new concepts. And while police may try new investigative techniques, they should not be allowed to mask constitutional shortcomings in "the complexities of novel technology" and expect a free pass. J.A. 1368.

The search of millions of Google users at once renders the warrant here so overbroad that no reasonably objective officer could have thought it valid. Det. Hylton did not establish probable cause to search even one person's Location History, let alone *everyone's* Location History. Any reasonable officer should have

recognized that such an astoundingly broad search could not be justified based on boilerplate assumptions about cell phone use.

However, even without stating that the warrant would be a digital dragnet of millions, it was still objectively unreasonable to search everyone within 150 meters of a bank in Richmond. Any reasonably well-trained officer would have known that it is necessary to establish probable cause based on the individual facts of a case. *See Doyle*, 650 F.3d at 472 (finding that good-faith exception did not apply when the police searched a house for contraband with a warrant that contained "remarkably scant evidence … to support a belief that [the defendant] *in fact* possessed" it (emphasis added)); *see also United States v. Winn*, 79 F. Supp. 3d 904, 924 (S.D. Ill. 2015) ("[T]he warrant was so facially and grossly overbroad in its description of the items to be seized that '[a] reasonably well-trained officer would have known the search was illegal despite the issuing judge's authorization.'" (quoting *Leon*, 468 U.S. at 923 n.23)); *cf. United States v. Seerden*, 916 F.3d 360, 367-68 (4th Cir. 2019) (finding good-faith exception did apply where the affidavit contained allegations and admissions of the actual crime for which evidence was sought). Likewise, they would have known that it is necessary to limit the scope of any search to that probable cause. *See United States v. Hurwitz*, 459 F.3d 463, 473 (4th Cir. 2006) ("[A] warrant must be 'no broader than the probable cause on which it is based.'" (quoting *United States v. Zimmerman*, 277 F.3d 426, 432 (3d Cir. 2002))).

This is not a new requirement. It is well-established that law enforcement must demonstrate "a reasonable ground for belief of guilt … *particularized* with respect to the person to be searched or seized." J.A. 1367 (quoting *Maryland v. Pringle*, 124 S. Ct. 795, 800 (2003)). As the Supreme Court recognized more than 40 years ago, it is not constitutional to search everyone in a public place without probable cause to believe that everyone there is involved in criminal activity. *See Ybarra v. Illinois*, 444 U.S. 85, 91 (1979). Probable cause must be "particularized," and 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." *Id.*; *see also* J.A. 1367.

Thus, in the case of warrants authorizing the search of "all persons on [a] premise[s]," this Circuit has established that an officer must show probable cause "to believe that *all* persons on the premises at the time of the search are involved in the criminal activity." *Owens ex rel. Owens v. Lott*, 372 F.3d 267, 276 (4th Cir. 2004); *see also United States v. Curry*, 965 F.3d 313, 330-31 (4th Cir. 2020) (*en banc*) (finding unconstitutional the search of a group of men walking in a public area less than a minute after the sound of gunshots near an apartment complex).

Here, the search involved a public space encompassing, at the very least, the whole of a bank and a nearby church. A reasonable officer would have known that such a warrant would require a broad search of many individuals, and that it would return information about many people uninvolved in the robbery. As the district

court saw it, the geofence warrant was akin to an "all persons" warrant for the area around the bank, including a large church and possibly many other businesses and multi-unit residential buildings. J.A. 1368. The warrant failed, however, to particularize probable cause with respect to any—let alone *all*—of the Google users whose data would be searched and seized. J.A. 1368 ("This warrant did no such thing."). Instead, it sought for information on "*all* Google account owners who entered the geofence over the span of an hour" plus "contextual data" for another hour with "*no* geographical restriction." J.A. 1368.

Similarly, when the place to be searched is a room or apartment in a multi-unit building, a valid warrant must generally identify the subunit to be searched. *See Manley v. Commonwealth*, 211 Va. 146, 151 (1970) (recognizing the rule that "a search warrant directed against a multiple-occupancy structure is invalid if it fails to describe the particular sub-unit to be searched …."); *Brown v. Commonwealth*, 212 Va. 672, 674 (1972) (same). While there is an exception if the building appears to be a single-occupancy structure, it does not apply where officers realize the building is multi-unit, even if they do not know how many units there are. On the contrary, as the Supreme Court warned in *Maryland v. Garrison*, officers "should be on notice … that they must clearly distinguish the target unit from the others in order to avoid infringing upon the Fourth Amendment rights of other occupants of the building." 480 U.S. 79, 95 n.4 (1987). Or in other words, officers drawing such a warrant

"should be put to *a more demanding standard* of reasonableness to justify any mistake than is required for those who rely on a reasonable failure to recognize at all the multiunit nature of a structure." *Id*. (emphasis added).

Here, although the warrant ostensibly sought data about people around the bank at the time of the robbery, it actually identified Google's headquarters as the place to be searched, almost a month after the robbery. J.A. 110. But Google's Location History "Sensorvault" is like an apartment building with "numerous tens of millions" of units, containing the Location History data belonging to each user. Det. Hylton must have known that he was asking to search the data from more than one user in the Sensorvault, even if he did not know it would be "tens of millions" of them. He must have known that the search would cover at least the users in the bank and the church, if not the Ruby Tuesday, the hotel, or the Genito Glen apartment complex.

It was therefore insufficient for the warrant to merely identify "1600 Amphitheater Parkway" as the place to be searched, as the affidavit did not establish probable cause for each of the "tens of millions" of accounts housed on Google's servers. Once again, 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. Any reasonable officer would have known they did not have

probable cause to search every apartment in a multi-million-unit building, but that is the digital equivalent of what Det. Hylton did. Any reasonable officer would have known that such a search is impermissible, even if approved by a magistrate.

Even if Det. Hylton thought the warrant would only search and seize the data belonging to people in the geofence, he must have known that he did not have probable cause to search all of them. He did not even know how many users would be returned in Step 1, so he could not have had probable cause ahead of time to search all 19 of them. The geofence was a dragnet, plain and simple. There was no particularized probable cause at all. Det. Hylton simply used the same template he had used three times before, plugged in a summary of the crime, and changed the date and location. J.A. 1048. There was no evidence that the robber "in fact" had a smartphone, had used Android or Google services, had opted-in to Location History, or had not deleted the data in question. There was no evidence that the robber's data was "in fact" in Google's Sensorvault. *See Doyle*, 650 F.3d at 472; J.A. 64. There was no attempt to even exclude devices associated with the Journey Christian Church. All the government offered here were generalized assumptions about cell phone users. Statistics, however, are no substitute for particularized probable cause. The alternative would mean there is no reason that the police could not obtain a geofence warrant in every single case. Instead, this Court should hold that any belief in the

existence of probable cause for this geofence warrant was entirely unreasonable. *See Doyle*, 650 F.3d at 471; *United States v. Leon*, 468 U.S. 897, 923 (1984).

While the workings of Location History and geofence warrants may be somewhat complex, it was Det. Hylton who invited this complexity and asked the magistrate to rely on his "training and experience" in approving such a radically different type of warrant. J.A. 111. Simply put, Det. Hylton represented that he knew what he was talking about. But even though he had obtained three geofence warrants in the past, he had never received any training at all on applying for or using them. J.A. 1044-1045. Furthermore, Det. Hylton had received no training on geofence warrants for a very good reason: there were no law enforcement procedures to follow, and there were no trainings to take. J.A. 969-970. In fact, neither the Chesterfield County Police nor the FBI, who quickly became involved in this case, trained their investigators on seeking geofence warrants. *See* J.A. 968-969.[4]

But Det. Hylton did not mention any of this in his warrant application. Instead, he used a "go-by"—a template—with a 3-step process seemingly developed in secret during discussions between Google and the Computer Crime and Intellectual Property Section ("CCIPS") of the United States Department of Justice. *See* J.A. 1344; J.A. 1369. Of course, there is nothing inherently wrong with using a warrant

[4] Perhaps this is also for a very good reason: geofence warrants are impermissible general warrants. *See infra*, Section F.

template. But it is still necessary to tailor its scope to the facts of the case. Generalized assumptions about cell phone use do not suffice.

Moreover, for the good-faith doctrine to reasonably apply, an officer should at least be required to understand what he is asking for. Det. Hylton appeared to have no real understanding of geofence warrants, despite having obtained one three times before. According to Google, Det. Hylton seemed unaware of how the process was supposed to work or what data he could expect to receive. J.A. 1355; J.A. 1584-1585. He did not even follow the process as outlined in the warrant he prepared. Instead, he "returned the warrant before it was served, improperly requested Step 2 and 3 information simultaneously, failed at first to narrow his request at Step 2, and incorrectly tried to add a Step 4 to the process." J.A. 1377.

"Astoundingly," the government's response was that they had "established probable cause to obtain *all* information (Steps 1, 2, and 3) from *all* users within the geofence without any narrowing measures." J.A. 1368-1369. Or to put it another way, the government admitted that the 3-step process existed solely to appease Google. J.A. 1369 ("[I]t appears that law enforcement implemented narrowing measures in this Warrant at the behest of Google."). But, as the district court determined, "the warrant simply did not include any facts to establish probable cause to collect such broad and intrusive data from each one of these individuals." J.A. 1369. Rather, the 3-step process was a legal fig leaf. The warrant application made

no mention of such sweeping authority, but instead obscured the true scope of the search and seizure through the empty 3-step process that it detailed.

Officers owe a duty of candor to the judiciary. *See Taylor v. Hughes*, 26 F.4th 419, 422 (7th Cir. 2022) ("Police officers owe judges candor when seeking search warrants."); *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1178 (9th Cir. 2010) (Kozinski, C.J., concurring) ("[O]mitting such highly relevant information altogether is inconsistent with the government's duty of candor in presenting a warrant application."); U.S. Const. amend. IV ("[N]o Warrants shall issue, but upon probable cause, *supported by Oath or affirmation* ...") (emphasis added). It violates this duty to file warrants they do not understand. It violates this duty to seek new types of warrants involving new technologies, while failing to learn or apprise the court of how they work. And it violates this duty to represent that law enforcement will follow specific procedures, when the government apparently believed that they are superfluous and did not intend to follow them.

Det. Hylton did not meet his duty of candor. He proposed the new tactic, so he had a duty to explain it. If he did not know how it would work, he should have said so and not misrepresented his training and experience. If he did know, then he concealed material facts from the issuing magistrate.[5] Had he been more forthright—had the magistrate known that the warrant he signed authorized Google to search the

[5] *See supra* page 11, note 2.

private daily "journals" of "numerous tens of millions of people"—he would have surely refused to sign such a warrant. J.A. 128 (stating that Location History is not a "business record" but a "journal that Google users can choose to create, edit, and store to record their movements and travels.").

Had the magistrate known that the warrant he signed simultaneously authorized a search of a church, a hotel, a restaurant, a mini storage facility, and two apartment complexes, he would have laid his pen on his desk and sent the affiant away empty-handed. To not include those facts demonstrates at least recklessness with regard to the true nature of the search the affiant proposed. Det. Hylton failed to include these critical facts that should have highlighted the unique overbreadth of the search for the reviewing magistrate—namely, the true scope of the number of people to be searched and the true boundaries of the "geofence." Including these facts would have only highlighted the warrant's deficiencies. *See Doyle*, 650 F.3d at 476 ("[W]here a reasonable officer would know that a probable cause determination could not be rendered without information conspicuously absent from his application for a warrant, reliance on the resulting warrant is not objectively reasonable.").

This case is, at bottom, a question of Fourth Amendment basics. The issues may be "cloaked" in new technologies and police tactics, but the same old rules still apply. Probable cause is not such a "complex topic" requiring an understanding that "police officers are not and cannot be expected to possess." J.A. 1383. And Det.

Hylton knew he did not have probable cause to search anyone, including Mr. Chatrie. Indeed, that absence of suspects is precisely why he applied for a geofence warrant. And that is why it was "so lacking in indicia of probable cause" to search Mr. Chatrie's data that "official belief in its existence [was] entirely unreasonable." *See Leon*, 468 U.S. at 923 (internal citations and quotations omitted). The warrant's deficiencies were "so extreme and apparent that a reasonably well-trained police officer, with reasonable knowledge of what the law prohibits, would have known the warrants were invalid notwithstanding their approval by a judge." *Burns*, *Burns v. United States*, 235 A.3d 758, 767 (D.C. 2020). The good-faith exception therefore should not apply, and the district court should have granted Mr. Chatrie's motion to suppress all evidence and fruits obtained from the geofence warrant.

B. The Warrant Was Unparticularized and Facially Deficient

The good-faith exception also does not apply when a warrant is so facially deficient that no objective officer could rely on it. Here, the geofence warrant was profoundly lacking in particularity because it failed to limit the data searched and seized, leaving the scope entirely up to police. The 3-step process was no cure, the court determined. J.A. 1376. Instead, it showed a "clear lack of particularity" that left "the executing officer with *unbridled* discretion." J.A. 1376. Specifically, the court found that Steps 2 and 3 "lack[ed] any semblance of objective criteria to guide how officers would narrow the lists of users." J.A. 1376. Once again, however, the court

found that the good-faith doctrine applied under *United States v. McLamb*, 880 F.3d 685 (4th Cir. 2018), because of Det. Hylton's "prior acquisition of three similar warrants, and his consultation with Government attorneys before obtaining those warrants." J.A. 1383.

Mr. Chatrie maintains that the existence of previous similar warrants, even if obtained in consultation with prosecutors, is not sufficient to merit application of the good-faith exception in this case. Like probable cause, particularity is a fundamental part of drafting warrants. It is not a new requirement. It is not an obscure requirement. And it is not a technical legal requirement. Rather, it is axiomatic that a warrant must "limit[] the authorization to search to the specific areas and things for which there is probable cause to search." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987).

Indeed, the Founders created the particularity requirement in response to one of the chief evils of their time: "general warrants," which "allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity," and were one of the direct causes of the American revolution. *Riley v. California*, 573 U.S. 373, 403 (2014). General warrants were despised because they "specified only an offense … and left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched." *Steagald v. United States*, 451 U.S. 204, 220 (1981). Moreover, where there are significant First Amendment concerns, the particularity requirement takes on heightened importance.

See Stanford v. Texas, 379 U.S. 476, 485 (1965); *Marcus v. Search Warrant of Property*, 367 U.S. 717, 729 (1961); *A Quantity of Copies of Books v. Kansas*, 378 U.S. 205, 212 (1964). In such circumstances, particularity demands that "nothing is left to the discretion of the officer executing the warrant." *Stanford*, 379 U.S. at 485.

This geofence warrant, however, did nothing of the sort. Instead, it explicitly gave officers the authority to decide what data to search and what to seize. It was up to Google and the government to determine how to count responsive devices in Step 1. And it was up to Google and the government to decide which accounts would be subject to further scrutiny in Steps 2 and 3. At every step along the way, the warrant gave law enforcement "unchecked discretion to seize more intrusive and personal data," all "without ever needing to return to a neutral and detached magistrate for approval." J.A. 1377. In sum, the geofence warrant was facially deficient due to its complete lack of particularity, and Mr. Chatrie maintains that Det. Hylton's reliance on it was objectively unreasonable.

The district court erred in citing *McLamb* to conclude that the good-faith doctrine should nevertheless apply. This case is unlike *McLamb*, where the issue was a complicated jurisdictional question involving statutory construction: whether Rule 41 of the Federal Rules of Criminal Procedure permitted a magistrate judge to issue a warrant for a "network investigative technique" that exceeded the geographic boundaries of their jurisdiction. *McLamb*, 880 F.3d at 691. At the time, it was

"unclear" whether such extraterritorial warrants were permissible. *Id*. As a result, this Court determined that it was reasonable to rely on consultation with government attorneys when confronted by such an obscure and technical legal question. *Id.*

Here, by contrast, the very reason police resorted to a geofence warrant was because they did not have any suspects. The warrant was useful *because* it was unparticularized, permitting Det. Hylton to pick and choose which accounts to search and the amount of data to seize, without judicial supervision. Any reasonable officer, however, should have known that valid warrants do not work that way. It was not "unclear" that warrants must be particularized. *See Groh v. Ramirez*, 540 U.S. 551, 563 (2004) ("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." (citing *Harlow v. Fitzgerald,* 457 U.S. 800, 818-19 (1982))). Indeed, it is a basic principle that "Fourth Amendment direction must be confined to the signing magistrate, not the executing officers or a third party." J.A. 1377. And while Det. Hylton had obtained geofence warrants in the past, obtaining one deficient warrant should not mechanically entitle him to obtain another.

On the contrary, while past warrants and consultation with counsel may be "prima facie evidence" of good faith, these factors must not insulate the government from its basic obligation to particularize warrants. *See United States v. Winn*, 79 F. Supp. 3d 904, 923-24 (S.D. Ill. 2015) (refusing to find good faith where two officers

had 15 years of experience between them and obtained a warrant that "gave them unbridled discretion to search for and seize whatever they wished"). Rather, the government's "recklessness" and complete disregard for the particularity requirement should negate any claim of good faith in this case. *See id*.

C. The Magistrate Abandoned His Judicial Role

Finally, the district court erred in finding that Magistrate Bishop had not wholly abandoned his judicial role as a detached magistrate. *See* J.A. 1384. The Fourth Circuit has established that the good-faith exception does not apply where the magistrate acted as a "rubber stamp" in approving a "bare bones" affidavit. *United States v. Wilhelm*, 80 F.3d 116, 121 (4th Cir. 1996). And as discussed above, the affidavit here was "completely devoid" of probable cause. J.A. 1369. It relied entirely on generalized assumptions about cell phone use that could apply in any case and therefore did not "provide the magistrate with a substantial basis for determining the existence of probable cause." *Wilhelm*, 80 F.3d at 123.

The district court faulted Mr. Chatrie because he "produced no evidence to show that the magistrate did not read the affidavit or that he read it so cursorily as to have wholly abandoned his neutral and detached role." J.A. 1384. But no amount of reading could have led the magistrate to find probable cause in this warrant. There were simply no facts to do so. As a result, "the state magistrate could not have acted as other than a 'rubber stamp' in approving such an affidavit." *Wilhelm*, 80 F.3d at

121; *see also Winn*, 79 F. Supp. 3d at 924 (finding that a judge acted as rubber stamp "when he signed off on a warrant despite the facially overbroad nature of the list of items to be seized"); *United States v. Decker*, 956 F.2d 773, 777-78 (8th Cir. 1992) (finding judge did not fulfill role of neutral and detached reviewer by approving warrant with glaring omissions).

Magistrate Bishop further abandoned his judicial role in granting such immense discretion to Det. Hylton to decide which users' data to search and seize in Steps 2 and 3. As in *Lo-Ji Sales v. New York*, the magistrate abdicated his authority by leaving the determination of what to seize up to the executing officers. 442 U.S. 319, 326-27 (1979). The Fourth Amendment, however, "does not permit such action," nor such "open-ended warrants." *Id*. at 325.[6] Rather, it demands that a neutral and detached magistrate make decisions about what to search and what to seize. This constitutional function may not be outsourced to Google or to the police. But that is what Magistrate Bishop did here. He abandoned his judicial role, and the good-faith exception should therefore not apply.

[6] Among other problems, this grant of discretion prevents the magistrate from "verify[ing] that the inventory prepared by the police … accurately reflected what he had ordered seized." *Lo-Ji Sales*, 442 U.S. at 327. Indeed, the warrant return in this case, which was filed prior to the warrant's execution, contained just one word: "Data." J.A. 1354.

D. Consultation With Prosecutors Does Not Immunize Det. Hylton

The district court erred in finding that Det. Hylton's "consultation with Government attorneys" before obtaining three similar warrants rendered reasonable his reliance on the warrant here. J.A. 1383. While officers may be encouraged to discuss warrant applications with prosecutors, such consultation in no way shields an officer who unreasonably relies on an unconstitutional warrant. *See, e.g.*, *United States v. Lyles*, 910 F.3d 787, 796 (4th Cir. 2018) (finding that while a prosecutor's and police supervisor's review of warrant application is relevant to good-faith analysis, because those parties share the officer's incentives to ferret out crime, such review is not dispositive); *see also Messerschmidt v. Millender*, 565 U.S. 535, 554 (2012) ("And because the officers' superior and the deputy district attorney are part of the prosecution team, their review also cannot be regarded as dispositive."). Otherwise, "police departments might be tempted to immunize warrants through perfunctory superior review, thereby displacing the need for 'a neutral and detached magistrate' to make an independent assessment of an affidavit's probable cause." *Lyles*, 910 F.3d at 796-97 (citing *Riley*, 573 U.S. at 382 (emphasizing constitutional importance of warrant review by neutral and detached magistrate)).

Here, the district court erred by placing too much weight on Det. Hylton's prior consultation with prosecutors on three "mostly similar" geofence warrants. J.A. 1022. First, Det. Hylton did not consult with government attorneys before obtaining the

geofence warrant in this case. J.A. 1021. Rather, he had consulted with prosecutors about three other geofence warrants before seeking the warrant in this case. J.A. 1021. During those earlier consultations, no one had ever explicitly told Det. Hylton that geofence warrants were illegal. J.A. 1021. But, Det. Hylton had never received any data in response to the warrants, J.A. 1023, and thus, there was no data disclosed to challenge or sufficient scrutiny applied to the search itself.

Second, the district court relied heavily on this Court's decision in *McLamb* to find that Det. Hylton's prior consultations with prosecutors on three geofence warrants—that had yielded no returns—rendered reasonable his reliance on the warrant in this case. The legal question in *McLamb* was the validity of executing a warrant that reached beyond a magistrate's particular jurisdiction. *See* 880 F.3d at 689. The warrant application itself accurately described the digital tool used and the scope of the intended search. *Id.* at 690. The affiant officer, concerned about the legality of executing a warrant using a digital tool that extended beyond the issuing magistrate's district, consulted with attorneys within the Department of Justice and the FBI. *Id.* at 689. It was in that context that this Court observed: "We are disinclined to conclude that a warrant is 'facially deficient' where the legality of an investigative technique is unclear and law enforcement seeks advice from counsel before applying for the warrant." *Id.* at 691.

Here, while certainly geofence warrants were a relatively novel surveillance tool in 2019, there was nothing novel—or constitutional—about the unfettered discretion that the warrant in this case gave to police through the multi-stage search process or the warrant's complete disregard for the Fourth Amendment's probable cause and particularity requirements. Det. Hylton knew he would be searching the private location data of a large number of people, even if he was not certain exactly how many innocent persons would be searched. He knew he did not have probable cause for the untold number of innocent persons who would be searched. He knew the warrant gave him complete discretion to choose whose privacy to further invade in later stages of the search. J.A. 2037 (seeking more invasive second stage data on everyone in the geofence).

Any objectively reasonable officer would have known, or should have known, that such a warrant violates the basic precepts of the Fourth Amendment, regardless of consultation with counsel or approval by an inexperienced magistrate. *See Lyles*, 910 F.3d at 796 (recognizing that the "magnitude of the intrusion … 'is of central relevance to determining reasonableness,'" especially "when 'any and all' is the warrant's insistent refrain" (quoting *Maryland v. King*, 569 U.S. 435, 446 (2013))); *see also Winn*, 79 F. Supp. 3d at 923-24.

E. Suppression Would Produce Deterrent Benefits

Finally, Mr. Chatrie disagrees with the district court's conclusion that "exclusion here likely would not 'meaningfully deter' improper law enforcement conduct." J.A. 1383. On the contrary, the geofence warrant here demonstrated a culpable disregard for the most basic Fourth Amendment requirements that cannot be saved by magistrate approval or consultation with the prosecution. *See United States v. Qazah*, 810 F.3d 879, 887 (4th Cir. 2015) ("When the police exhibit deliberate, reckless, or grossly negligent disregard for Fourth Amendment rights, the deterrent value of exclusion is strong and tends to outweigh the resulting costs.").

Mr. Chatrie is mindful that the purpose of the exclusionary rule "is to deter future Fourth Amendment violations" and that exclusion is appropriate only when "the deterrence benefits of suppression ... outweigh its heavy costs." *Davis v. United States,* 564 U.S. 229, 237 (2011). But this is one of those cases. Det. Hylton knew or should have known that valid warrants do not permit the dragnet search of millions. And Det. Hylton knew or should have known that they do not authorize police officers to decide who to search and what to seize. Suppression would discourage law enforcement from seeking such blatantly overbroad and unparticularized warrants in the future.

Even though Magistrate Bishop signed the warrant, Det. Hylton was the one responsible for preparing it. *See Groh v. Ramirez*, 540 U.S. 551, 564 (2004)

("[B]ecause petitioner himself prepared the invalid warrant, he may not argue that he reasonably relied on the Magistrate's assurance that the warrant contained an adequate description of the things to be seized and was therefore valid."). Moreover, Det. Hylton was the one who asked the court to rely on his "training and experience"—of which he had none and very little, respectively, when it came to geofence warrants. *See* J.A. 1353; J.A. 113. In truth, Det. Hylton had received no training on geofence warrants from either the Chesterfield County Police or the FBI because neither agency had any policies or procedures to follow for such a constitutionally subversive search and seizure. *See supra* Section A; J.A. 968-970; J.A. 1044-1045.

Furthermore, Det. Hylton had not received data from Google in any of the three previous geofence warrants he obtained, testifying that none of those cases "were immediately concerning the public's welfare and safety." J.A. 1023. Like relying on an informant with no credibility, Det. Hylton failed to disclose the frailty of his knowledge and experience. *See United States v. Doyle*, 650 F.3d 460, 476 (4th Cir. 2011) ("[W]here a reasonable officer would know that a probable cause determination could not be rendered without information conspicuously absent from his application for a warrant, reliance on the resulting warrant is not objectively reasonable."). And Det. Hylton did so to secure a dragnet of immense proportions that would be conducted at the sole discretion of police. In short, the grave

constitutional defects in this warrant were Det. Hylton's doing. *Cf. Massachusetts v. Sheppard*, 468 U.S. 981, 990 (1984) ("[I]t was the judge, not the police officers, who made the critical mistake.").

Moreover, it has become apparent that this case was not an isolated instance of negligence, but part of a growing trend that is just now coming to light. As the district court explained:

> In recent years, the number of geofence warrants received by Google has increased exponentially. Google received its first in 2016. After that, Google "observed over a 1,500% increase in the number of geofence requests it received in 2018 compared to 2017; and the rate ... increased over 500% from 2018 to 2019." In 2019, Google received "around 9,000 total geofence requests." And Google now reports that geofence warrants comprise more than twenty-five percent of all warrants it receives in the United States.

J.A. 1343-1344 (internal citations and footnotes omitted). Despite this increasing frequency, it is only now that geofence warrants are facing scrutiny in criminal prosecutions like this one. Given Google's statistics, however, it is hard to imagine that this is the first case where a geofence warrant played a significant role. It is more likely that the use of geofence warrants has not been disclosed in countless other cases, concealing a conscious concern with the constitutionality of such searches. And in such circumstances, the exclusionary rule plays another important role in deterring such "recurring or systemic negligence." *United States v. McLamb*, 880 F.3d 685, 690 (4th Cir. 2018) (quoting *Herring v. United States*, 555 U.S. 135, 144 (2009)).

This is the first opportunity for a federal court of appeals to address law enforcement's secretive geofence habit. And this Court should send a strong message to law enforcement that the Fourth Amendment will not tolerate it. Any objectively reasonable officer knows that a warrant must satisfy the Fourth Amendment's probable cause and particularity requirements. There is no 3-step dance around it. Law enforcement should not continue to think that such discretion belongs to anyone but the judiciary.

Law enforcement's conduct in this case is culpable enough to yield "meaningfu[l]" deterrence that would be "worth the price paid by the justice system." *Herring*, 555 U.S. at 144. Det. Hylton violated the Fourth Amendment with "deliberate, reckless, or grossly negligent conduct" in a pattern of law enforcement behavior that demonstrates "recurring or systemic negligence." *Id.* Culpability lies with the police, and suppression would deter future geofence warrants with such breadth and discretion. The warrant here was simply not "objectively reasonably law enforcement activity," and this Court should deter similar conduct by applying the exclusionary rule. *United States v. Leon*, 468 U.S. 897, 919 (1984); *see also United States v. Wilhelm*, 80 F.3d 116, 123 (4th Cir. 1996).

F. General Warrants Deserve No Good Faith

There is no such thing as relying on a general warrant in good faith. *See Groh v. Ramirez*, 540 U.S. 551, 558 (2004). To hold otherwise would invite the kind of

"systematic error" and "reckless disregard of constitutional requirements" that the Supreme Court has cautioned against. *Herring*, 555 U.S. at 144; *see also United States v. Krueger*, 809 F.3d 1109, 1123 (10th Cir. 2015) (Gorsuch, J., concurring) (finding that when a warrant is void, "potential questions of 'harmlessness'" do not matter); *United States v. Winn*¸ 79 F. Supp. 3d 904, 926 (S.D. Ill. 2015) ("Because the warrant is a general warrant, it has no valid portions."). Should this Court find that this geofence warrant was an unconstitutional general warrant, then no balancing test is required. The good-faith doctrine does not apply.

While the good-faith exception is relatively new, the prohibition on general warrants is not. General warrants were a catalyst for the American Revolution and the inspiration behind the Fourth Amendment. And as a result, the Constitution forbids them. Because *Leon* was not decided until 1984—nearly 200 years after the Fourth Amendment outlawed general warrants in this country, fewer courts have had occasion to consider whether the good-faith rule has any bearing on a general warrant. But consistently, courts have found that the good-faith exception is inapplicable to general warrants. *See, e.g.*, *Groh*, 540 U.S. at 558 (finding that a warrant "so obviously deficient" in particularity must be regarded as "warrantless" within the meaning of our case law); *United States v. Ninety-Two Thousand Four Hundred Twenty-Two Dollars and Fifty-Seven Cents ($92,422.57)*, 307 F.3d 137, 149 (3d Cir. 2002) (finding general warrants to be "so plainly in violation of the

particularity requirement that the executing officers could not have reasonably trusted in its legality"); *United States v. George*, 975 F.2d 72, 77-78 (2d Cir. 1992); *United States v. Medlin*, 842 F.2d 1194, 1199 (10th Cir. 1988); *United States v. Crozier*, 777 F.2d 1376, 1381 (9th Cir. 1985); *see also United States v. Minnick*, No. TDC-14-055, 2016 WL 3461190, at *5 (D. Md. June 21, 2016) (considering the good-faith exception's applicability to suppression *after* rejecting the claim that what issued was a general warrant); *Winn*, 79 F. Supp. 3d at 926; *United States v. Fleet Mgmt. Ltd.*, 521 F. Supp. 2d 436, 445-46 (E.D. Pa. 2007) ("[W]e read Third Circuit precedent to prohibit the use of the good faith exception in connection with general warrants." (citing *United States v. Christine*, 687 F.2d 749, 758 (3d Cir. 1982) ("It is beyond doubt that all evidence seized pursuant to a general warrant must be suppressed."))).

The geofence warrant here was a general warrant. It "did *not* describe in 'specific and inclusive generic terms' what was to be seized," but rather "vest[ed] the executing officers with 'unbridled discretion' to search for and seize whatever they wished.'" *Fleet Mgmt. Ltd.*, 521 F. Supp. 2d at 443. It provided no particularized probable cause for the "all persons" search in Step 1, and it granted law enforcement "unbridled discretion" to search and seize more data in Step 2 and Step 3. J.A. 1365. If the Fourth Amendment means anything, it is a safeguard against this type of dragnet search and discretionary seizure of private data. It does not

contemplate this sort of general rummaging, even if conducted by computers. On the contrary, geofence warrants are the digital equivalent of the very thing the Fourth Amendment was designed to prevent.

The Fourth Circuit has never applied the good-faith doctrine to a general warrant, and it should not start now. This Court should therefore find that the geofence warrant is an affront to the Fourth Amendment and suppress all evidence and fruits thereof.

CONCLUSION

For the reasons stated above, this Court should reverse the judgment of the district court denying Mr. Chatrie's motion to suppress.

Respectfully submitted,

MICHAEL W. PRICE
National Association of Criminal Defense Lawyers

s/ Michael W. Price
Litigation Director, Fourth Amendment Center
1660 L Street NW, 12th Floor
Washington, DC 20036
(202) 465-7615
mprice@nacdl.org

GEREMY C. KAMENS
Federal Public Defender

s/ Laura J. Koenig
Laura J. Koenig
Assistant Federal Public Defender
701 East Broad Street, Suite 3600
Richmond, VA 23219
(804) 565-0800
laura_koenig@fd.org

Dated January 20, 2023

REQUEST FOR ORAL ARGUMENT

Counsel for the appellant assert that the issues raised in this brief may be more fully developed through oral argument, and respectfully request the same.

CERTIFICATE OF COMPLIANCE

1. This Brief of the Appellant has been prepared using Word for Office 365 software, Times New Roman font, 14-point proportional type size.

2. EXCLUSIVE of the table of contents, table of authorities, signature block, statement with respect to oral argument, and this certificate of compliance, this brief contains no more than 13,000 words, specifically 11,614 words.

I understand that a material misrepresentation can result in the Court's striking the brief and imposing sanctions. If the Court so requests, I will provide an electronic version of the brief and/or a copy of the word or line print-out.

January 20, 2023
Date

s/ Laura J. Koenig
Laura J. Koenig
Assistant Federal Public Defender