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)

REPLY 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)

REPLY BRIEF OF THE APPELLANT

ARGUMENT

The government advances three arguments that ignore the realities of the digital age. *See* Gov't Br. 15-16. First, the government denies that people have a Fourth Amendment interest in their Google Location History, confusing personal data with business records and discounting the palpable privacy implications of revealing someone's whereabouts. Second, the government mistakes the needle for the haystack, insisting that a dragnet of "numerous tens of millions" of people is permissible so long as investigators can describe the needle. Finally, the government says police should

receive the benefit of "good faith" because they conferred with prosecutors working the same case, seeking a free pass to violate the Constitution. This Court should find the warrant unconstitutional, find the good-faith exception inapplicable, and remand to the district court.

A. Mr. Chatrie Had a Fourth Amendment Interest in His Location History

Although the government obtained a warrant here, they now claim that Mr. Chatrie lacked a Fourth Amendment interest in his Location History, suggesting no warrant was required. Gov't Br. 18. The government advances two arguments in support: 1) that police obtained "only" two hours of Mr. Chatrie's data, *id.* at 21, and 2) that Mr. Chatrie "voluntarily" disclosed his location information to Google, and therefore the government. *Id.* at 23, 27. The government is wrong on both the law and the facts. J.A. 31-40; J.A.76-85; J.A. 373-383; J.A. 1090-1102; J.A. 1164-1177.

1. Reasonable Expectation of Privacy

Mr. Chatrie had a reasonable expectation of privacy in his Location History under *Carpenter v. United States*, 138 S. Ct. 2206 (2018), and *United States v. Jones*, 565 U.S. 400 (2012), because Location History reveals the "privacies of life." 138 S. Ct. at 2218 (finding location tracking data "provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'") (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)). The precise and constant nature of

Location History makes it even more invasive and potent than CSLI, requiring less to achieve the same effect. J.A. 1379 ("Google Location History information—perhaps even more so than the cell-site location information at issue in *Carpenter*—is 'detailed, encyclopedic, and effortlessly compiled.'").

a) *Carpenter* Applies to Location History

The district court found that Location History is a "powerful" and "sweeping, granular, and comprehensive tool." J.A. 1331-1332. According to Google, it is "capable of estimating a device's location to a higher degree of accuracy and precision than is typical of CSLI" because it uses multiple inputs to estimate device location, including GPS and signals from nearby Wi-Fi networks. J.A. 1555. As a result, Location History can pinpoint a device inside constitutionally protected spaces like a home or church. It can do things that GPS cannot do, like determine a phone's elevation and identify the specific floor of a building. J.A. 1332. By contrast, CSLI may be sufficient to place a person "within a wedge-shaped sector ranging from one-eighth to four square miles." *Carpenter*, 138 S. Ct. at 2218. Additionally, cell phone service providers typically log CSLI when the phone connects to their network, by placing a phone call or receiving a text message, for example. *Id.* at 2211. By contrast, Google logs Location History every two minutes, even if its owner is asleep. J.A. 530-531; J.A. 1332.

Consequently, Location History can reveal private information in just minutes. Whereas it could take days of CSLI to capture enough detail to infer a device's location, two hours of Location History here easily revealed individuals inside the bank as well as nearby homes, apartment complexes, a hospital, and the Journey Christian Church. *See* J.A. 477-487; J.A. 1358-1359; *see also Matter of Search of Information Stored at Premises Controlled by Google*, No. 20 M 297, 2020 WL 5491763, at *5 n.7 (N.D. Ill. July 8, 2020) ("The government's inclusion of a large apartment complex in one of its geofences raises additional concerns … that it may obtain location information as to an individual who may be in the privacy of their own residence"). Furthermore, using this supposedly "anonymized" data, a defense expert determined the likely identities of at least three of these individuals. *Id.* (describing the paths for "Mr. Green," "Mr. Blue," and "Ms. Yellow"). Indeed, Google treats this sensitive data as user "content" under the Stored Communications Act, 18 U.S.C. § 2703, calling it a "digital journal" of users' movements and requiring a warrant to search it. J.A. 138.

Carpenter involved seven days of CSLI, which is why the Supreme Court required a warrant to search seven days or more of CSLI. *See* 138 S. Ct. at 2267 (Gorsuch, J., dissenting). It was not a magic number, indicating a higher constitutional significance. *Carpenter* does not suggest that warrantless searches for shorter periods of time are permissible or imply some *de minimis* exception to the Fourth Amendment. Rather, *Carpenter* explicitly declined to determine "whether there is [any sufficiently]

limited period [of time] for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny." *Id.* at 2217 n.3; *see also Matter of Search of Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 756 (N.D. Ill. 2020) ("Fuentes Opinion") ("[T]here is much to suggest that *Carpenter*'s holding, on the question of whether the privacy interests in CSLI over at least seven days, should be extended to the use of geofences involving intrusions of much shorter duration.").

As Justice Gorsuch wrote: "[W]hat distinguishes historical data from real-time data, or seven days of a single person's data from a download of *everyone's* data over some indefinite period of time?" 138 S. Ct. at 2267 (Gorsuch, J., dissenting). There is no principled distinction to draw. The Court's concern in *Carpenter* and *Jones* was the risk of exposing "indisputably private" information, "'the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on.'" *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring); *Carpenter*, 138 S. Ct. at 2215. A geofence warrant can do just that, placing devices in both the church next door and a nearby hospital. J.A. 477-487; J.A. 1358-1359.

Moreover, the Supreme Court has repeatedly found that precise, short-term searches run afoul of the Fourth Amendment where, as here, they reveal information

inside a constitutionally protected space. *See United States v. Karo*, 468 U.S. 705, 716-17 (1984) (finding using a beeper to track an object inside private residence a search of information "withdrawn from public view"); *Kyllo v. United* States, 533 U.S. 27, 30, 37 (2001) (finding using thermal imaging to peer through walls of a home a search, even though scan "took only a few minutes" and could not show much detail inside). Specifically, the *Karo* Court remarked that "[i]ndiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests in the home to escape entirely some sort of Fourth Amendment oversight." *Karo*, 468 U.S. at 716.

This Court's decision in *Leaders of a Beautiful Struggle v. Baltimore Police Department*, 2 F.4th 330 (4th Cir. 2021) (*en banc*), is highly instructive. In *Leaders*, a private contractor conducted persistent ariel surveillance of Baltimore, which blurred people and vehicles. *Id.* at 334. When certain crimes occurred, police received a report with responsive data from before and after the crime. *Id.* These reports included the "tracks" of "vehicles and people present at the scene" as well as the locations before and after. *Id.* Critically, these "tracks" were "often shorter snippets of several hours or less." *Id.* at 342. Nonetheless, this Court found *Carpenter* applied because the tracks were culled from the contractor's 45-day repository. *Id.* at 341-42. The length of the "track" was not decisive, but that police could essentially "travel back in time" and observe someone's movements, or "tail[]" a suspect "for the prior six weeks" was

determinative. *Id.* at 341. "People understand that they may be filmed by security cameras on city streets, or a police officer could stake out their house and tail them for a time … [b]ut capturing everyone's movements outside during the daytime for 45 days goes beyond that ordinary capacity." *Id.* at 345. It "enables police to 'retrace a person's whereabouts,' granting access to otherwise 'unknowable' information." *Id.* at 342.

Similarly, a geofence warrant "transcends mere augmentation of ordinary police capabilities," and is akin to a time machine with no analog before the digital age. *Id.* at 345; J.A. 1362 ("this expansive, detailed, and retrospective nature of Google location data [] is unlike, for example, surveillance footage"). Here, as the district court found, the geofence entailed "accessing" an "almost unlimited pool" of "constant, near-exact location information for each user" with Location History enabled.[1] J.A. 1362. "Numerous tens of millions" of users were searched. J.A. 1555. Without the ability to search this enormous cache of accounts, the government would not have identified Mr. Chatrie or the other devices present. J.A. 1362; *Leaders*, 2 F.4th at 342 ("[T]he government can deduce such information only because it recorded *everyone's* movements.").

[1] At the time, Google retained Location History indefinitely and Mr. Chatrie had 341 days of data stored in his account. *See* Response to Government's Notice of Supplemental Authority, *United States v. Chatrie*, 3:19cr130, ECF No. 218 at 3 n.1 (E.D. Va. July 16, 2021).

b) The Third-Party Doctrine Does Not Apply

The government counters that the third-party doctrine dictates a different result, arguing that Mr. Chatrie "voluntarily disclosed information about the location of his phone to Google to obtain location-based services." Gov't Br. 23. But Location History is qualitatively different than the "business records" that fall into the third-party exception, like bank deposit slips or telephone numbers dialed. *See United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979). As the Supreme Court recently articulated, digital is different: any extension of old rules to digital data "has to rest on its own bottom." *Riley v. California*, 573 U.S. 373, 393 (2014) (observing that likening a physical search to the search of a cell phone is akin to "saying a ride on horseback is materially indistinguishable from a flight to the moon"); *Jones*, 565 U.S at 417 (Sotomayor, J., concurring) (describing the third-party doctrine as "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks"). Accordingly, the Supreme Court has instructed lower courts not to "mechanically" apply old rules to new technologies. 138 S. Ct. at 2219. Yet that is precisely what the government asks this Court to do.

Location History is unlike the "invited informant" in *Hoffa v. United States*, 385 U.S. 293, 302 (1966), where "every conversation which he heard was either directed to him or knowingly carried on in his presence," because it runs constantly and

imperceptibly in the background. It is unlike the bank records in *United States v. Miller*, where "negotiable instruments" used in commercial transactions were distinguishable from otherwise "confidential communications." 425 U.S. 435, 438 (1976). And Location History is unlike the digits dialed on a landline telephone in *Smith v. Maryland*, where callers were actively aware that the phone company tracked calls and sent bills showing the information collected. *Id.* at 742-45. Here, Mr. Chatrie enabled Location History only once—seemingly unknowingly. There is no evidence that Google sent a notice or reminders to Mr. Chatrie about Location History. J.A. 745; J.A. 777. And unlike *Smith*, Google does not bill users for Location History.

The government points to an opt-in process for Location History as evidence that Mr. Chatrie intended to relinquish forever all privacy in his physical location. Gov't Br. 27. But the district court recognized that that process provided only "the guise of consent" that "few people know how to disable." J.A. 1364; *see also* Fuentes Opinion, 481 F. Supp. 3d at 737 ("The Court finds it difficult to imagine that users of electronic devices would affirmatively realize, at the time they begin using the device, that they are providing their location information to Google in a way that will result in the government's ability to obtain—easily, quickly and cheaply—their precise geographical location at virtually any point in the history of their use of the device."). Here, Mr. Chatrie encountered a single pop-up screen (a "consent flow") while setting up Google Assistant that did not adequately describe Location History or how to

manage it. J.A. 1364. 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." J.A. 1380.

Finally, the government relies on Google's privacy policy to argue that Mr. Chatrie voluntarily conveyed his location information to Google and law enforcement in return for mapping and traffic updates. Gov't Br. 26. But the Supreme Court has never allowed such agreements to define the Fourth Amendment. *See Smith*, 442 U.S. at 745 ("We are not inclined to make a crazy quilt of the Fourth Amendment."). Indeed, the *Carpenter* majority did not rely on the cell company's contract or terms of service. It mattered not that the CSLI was "generated for commercial purposes," *id.* at 2217, and often sold in aggregate to data brokers for advertising. *Id.*

The government may believe that Location History is not as "indispensable to participation in modern society" as phone calls, but "numerous tens of millions" of people still use it. J.A. 1555. It is nonsensical to deem this data unworthy of Fourth Amendment protection unless everyone uses it. Yet that is the line the government seeks to draw. Modern smartphones serve many critical functions beyond making calls. *See Riley*, 573 U.S. at 393 ("They could just as easily be called cameras, … televisions, maps, or newspapers."). For many users, these functions are essential as owning the phone in the first place.

Mr. Chatrie did not meaningfully volunteer his location history to Google. Like many Google users, he did not knowingly or intentionally "opt-in" to Google's Location History service. Although the district court did not decide this question, it concluded that Mr. Chatrie "likely could not have, in a 'meaningful sense, voluntarily "assumed the risk" of turning over a comprehensive dossier of his physical movements' to law enforcement." J.A. 1380.

2. Property Interest

The most significant difference between Location History and the CSLI in *Carpenter* or the GPS data in *Jones* is who owns it. Regardless of the duration of the search or the significant privacy interests at stake, Location History data fits into a simpler scheme: the Fourth Amendment protects it because it belongs to the users who created it. It is their digital papers and effects, their personal "journal" stored in their accounts, just like their Gmail, Google Docs, or Google Photos. J.A. 131; J.A. 138; J.A. 374; J.A. 1330; J.A. 1555. It is user-generated content, not Google's "business records." Companies do not allow customers to delete the company's business records, unlike Location History. J.A. 1340-1343. Google did not possess a list of people near the bank until the government ordered one made. Rather, Google is a bailee of private data that belongs to each individual user. Consequently, the government can only search and seize it with a valid warrant. J.A. 39-40; J.A. 160-161.

Through this lens, even the smallest incursion is a Fourth Amendment search. The question is not how "private" the information is. *See, e.g.*, *Jones*, 565 U.S. at 406-07 ("[A defendant's] Fourth Amendment rights do not rise or fall with the *Katz* formulation.… [F]or most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates. *Katz* did not repudiate that understanding."); *Carpenter*, 138 S. Ct. at 2267-68 (Gorsuch, J., dissenting) ("[T]he traditional approach [to asserting a Fourth Amendment claim] asked if a house, paper or effect was *yours* under law. No more was needed to trigger the Fourth Amendment.").

Mr. Chatrie has briefed this argument repeatedly. J.A. 39-40; J.A. 83-85; J.A. 382-383; J.A. 1102; J.A. 1172-1173. The government, however, has not responded to its substance or introduced evidence to the contrary. Instead, they simply dismiss it as "rooted in Justice Gorsuch's solo dissent in *Carpenter*," J.A. 62, ignoring jurisprudence applying it as an independent test. *See, e.g.*, *Jones*, 565 U.S. at 409 ("[A]s we have discussed, the *Katz* reasonable-expectation-of-privacy test has been *added to,* not *substituted for,* the common-law trespassory test."); *Kyllo v. United States*, 533 U.S. 27, 40 (2001) ("[W]ell into the 20th century, our Fourth Amendment jurisprudence was tied to common-law trespass."); *Soldal v. Cook County*, 506 U.S. 56, 62 (1992) ("[O]ur cases unmistakably hold that the Amendment protects property as well as privacy."). This Court should find the government has conceded Mr. Chatrie's property

interest in his Location History and conclude that accessing it infringed on his Fourth Amendment rights.

B. Overbreadth

The government contends there was "ample basis" for finding probable cause but offers mostly generalizations about phones that would be universally applicable. Gov't Br. 30 (e.g., most phones are smartphones, which likely have an associated Google account and location data). The only case-specific fact they muster was that "the robber held a cell phone to his ear." *Id.*; J.A. 1370. But there was absolutely nothing in the warrant connecting Mr. Chatrie to the robbery. It did not identify him or his Google account at all. Had the government wanted to obtain *only* Mr. Chatrie's Location History data with this warrant, there clearly was no probable cause to do.

No Fourth Amendment exception exists to search "numerous tens of millions" of people simultaneously. The government's logic would mean that every time a crime occurs, and a cell phone is involved, probable cause exists to search the Location History of millions of Google users and seize the data of everyone nearby. J.A. 1375. This "inverted probable cause argument" therefore "cannot stand," J.A. 1375, and cannot justify a search of Mr. Chatrie's data. As the district court correctly determined, "probable cause '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.'" J.A. 1375 (quoting *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979)).

The government contends that *Ybarra* and its progeny are an "exception to the general rule for search warrants" and that probable cause need only be particularized for searches of people, not things. Gov't Br. 34. But *Ybarra* suggests no such thing and provides no rationale for treating "persons" differently from their "houses," "papers," and "effects." U.S. Const. art. IV.

Rather, *Ybarra* applied the basic principles of probable cause, concluding that a person's mere proximity to a crime, without more, is insufficient to justify their search or seizure. 444 U.S. at 91. Just as probable cause to search a house will not justify a search of the neighbors, the district court found that this reasoning applies equally to searches of individual Google accounts and the Location History therein. J.A. 1372; *see also* Fuentes Opinion, 481 F. Supp. 3d at 753 ("The Seventh Circuit's treatment of *Ybarra* teaches us that . . . that at least some evidence of a person's involvement in the suspected crime is required, in order for the Fourth Amendment to allow . . . the seizure of that person's things, such as location information, in which the person has a constitutionally protected expectation of privacy.").

The government counters that *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978), allows a warrant to establish only that the things to be searched for are at the property to which entry is sought. Gov't Br. 32. But *Zurcher* is not analogous to the geofence

here. *Zurcher* involved a search for photographs a newspaper employee took of unidentified demonstrators who had allegedly assaulted police. 436 U.S. at 551. Unlike Location History data, those photographs did not belong to individual demonstrators; they belonged to the newspaper. Unlike here, the warrant established a nexus between the crime and what police sought: published photographs from the protest-turned-crime-scene from the photographer who was present at the protest. *Id*. By contrast, the geofence warrant offers no evidence that Mr. Chatrie possessed relevant Location History data. As the district court found, it was also "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. The facts in *Zurcher* would be analogous to this case only if the newspaper happened to store private pictures belonging to tens of millions of non-employees.

The government cites *Illinois v. Lidster*, 540 U.S. 419 (2004), which involved stopping motorists to investigate a hit-and-run and is likewise inapposite. Those stops relied on the diminished expectation of privacy in automobiles and were permissible only because they sought the public's voluntary cooperation. 540 U.S. at 424-25. By contrast, checkpoints intended to reveal that a motorist has committed some crime are unconstitutional. *See City of Indianapolis v. Edmond*, 531 U.S. 32, 40-44 (2000). Thus, because the search here sought to identify the robber, the better analogy is to an unconstitutional checkpoint that stopped every car near the bank during rush hour and

demanded drivers unlock their phones and allow police to see their location history. As *Edmond* teaches, such a checkpoint would be impermissible for the same reason that the geofence warrant also fails: "A search or seizure is ordinarily unreasonable in the absence of individualized suspicion of wrongdoing." 531 U.S. at 42.

Finally, the government's reliance on *United States v. James*, 3 F.4th 1102 (8th Cir. 2021), involving a cell phone tower dump, is unpersuasive. The Fourth Circuit has never found tower dumps constitutional, and *Carpenter* explicitly declined to bless them. 138 S. Ct. at 2220. Moreover, the number of people a typical tower dump searches is far smaller than the "numerous tens of millions" a geofence warrant searches. J.A. 469. What these searches have in common is the absence of particularized probable cause, which *James* failed to consider. J.A. 1373; *see also* Fuentes Opinion at 751-52.

C. Lack of Particularity

Ordinarily, a warrant is required to search any single Google account. To obtain such a warrant, the police must identify the account to be searched. That does not mean that police must identify an account by the owner's name; they can provide a username or account number. But the warrant must identify the account to be searched in some way. Ordinarily, a warrant missing such information violates the Fourth Amendment's particularity requirement because it invites impermissible officer discretion on which accounts to search. Yet that is what happened here. The government asks this Court to

dispense with that particularity requirement if police want to search "numerous tens of millions" of accounts simultaneously.

The government counters that the warrant "specified with precision the items to be seized," Gov't Br. 37, but the scope of the search lacked any limit. Searching for a needle in a haystack, even if described precisely, still requires searching the whole haystack. The warrant did not specify Mr. Chatrie's account as the place to be searched, or any other account. Instead, it identified Google's headquarters at 1600 Amphitheater Parkway, the equivalent here of every haystack in the world. *See* Appellant's Br. 28.

With respect to the data seized in Steps 2 and 3, the warrant left "the executing officer with *unbridled* discretion and lack[ed] any semblance of objective criteria to guide how officers would narrow the lists of users." J.A. 1365. It explicitly eliminated judicial oversight to "narrow down" the results and determine which accounts to search further. J.A. 1352. Indeed, the warrant so clearly delegated this discretion to investigators that the government admits that the three-step process was a pretense, claiming now that the warrant authorized the seizure of two hours of Location History, deanonymized, for every device identified in the initial search. Gov't Br. 39-40; J.A. 1368-1369. The warrant, however, did not identify any of these people and "simply did not include any facts to establish probable cause to collect such broad and intrusive data from each one of these individuals," including Mr. Chatrie. J.A. 1369.

This admission demonstrates why severance is inappropriate. J.A. 89. Step 1 is the ballgame: once the government seizes the first round of data, investigators can obtain subscriber information for any Device ID through a subpoena to Google. *See* 18 U.S.C. 2703(d); *see also* Fuentes Opinion, 481 F. Supp. 3d at 754 (finding that there is "no practical difference between a warrant that … generate[s] 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"). As the government acknowledges, "first-step information alone was sufficient for investigators to recognize" the likely robber's account. Gov't Br. 41. The "narrowing measures" lack significance and cannot save the warrant's lack of particularity. Severance would only condone the digital equivalent of a general warrant that lacked particularity from the outset. *See*, *e.g.*, *United States v. Sells*, 463 F.3d 1148, 1158 (10th Cir. 2006) (noting that "every court to adopt the severance doctrine has further limited its application to prohibit severance from saving a warrant that has been rendered a general warrant by nature of its invalid portions despite containing some valid portion").

Finally, the government misrepresents the record in suggesting that a geofence warrant is like Google's advertising practices. Gov't Br. 42. There is no other circumstance where Google searches for such information or provides it to outsiders. J.A. 849-850. Google "never share[s] anyone's location history with a third party"

advertiser. J.A. 613. Likewise, advertisers cannot return to Google and ask for more information about where certain devices were before or after seeing an ad or visiting a store. J.A. 615. Advertisers simply cannot get any identifiable information about individual Google users. J.A. 615; J.A. 439 (explaining that data in warrant returns is "much different" than that accessible to advertisers).

D. The Good-Faith Exception Does Not Apply

The government claims that the good-faith exception should apply to a digital dragnet that searched "numerous tens of millions" of people, without identifying a single account to search, and without probable cause for any account searched. The government should have known better. The prohibition on general warrants is the Fourth Amendment's most basic commandment, not a "new rule." Gov't Br. 52. Yet this warrant searched the Location History of millions without identifying one. It was unsanctioned by the Chesterfield County Police and the FBI, neither of which had any policies, procedures, or trainings on geofence warrants. J.A. 969-970. And the Supreme Court has never come close to blessing anything remotely like it.

General warrants like this one are the antitheses of probable cause and particularity; they cannot be reasonably believed to be constitutional. *See Groh v. Ramirez*, 540 U.S. 551, 565 (2004) (quoting *United States v. Leon*, 468 U.S. 897, 923 (1984)) ("[A] warrant may be 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."). The mere fact that a government attorney said otherwise must not dictate the outcome. It certainly does not cure the lack of specificity in the place to be searched or somehow create a nexus between the crime and the accounts to be searched.

The good-faith exception assumes the existence of an approved warrant. That ever-present fact does not relieve the government of its continuing obligation to exercise reasonable professional judgment, especially where, as here the affidavit failed to alert the issuing magistrate to its true scope. *See, e.g.*, *Messerschmidt v. Millender*, 565 U.S. 535, 554 (2012); *id.* at 559 (Kagan, J., concurring in part and dissenting in part) (citation omitted) ("*Malley*[*v. Briggs*] made clear that qualified immunity turned on the officer's own 'professional judgment,' considered separately from the mistake of the magistrate."); *United States v. Dutton*, 509 F. App'x 815, 818 (10th Cir. 2013) (quoting *United States v. Gonzales*, 399 F.3d 1225, 1231 (10th Cir. 2005)) ("'Exclusion is appropriate in such circumstances because "reasonably well-trained" officers, exercising their own professional judgment, will be able to recognize the deficiency. Here, the warrant was "so lacking," and the officer's reliance upon it was not objectively reasonable.'"); *Malley v. Briggs*, 475 U.S. 335, 345-46 (1986) ("We find it reasonable to require the officer applying for the warrant to minimize this danger by exercising reasonable professional judgment.").

No objectively reasonable officer would have believed that such a warrant satisfied the Fourth Amendment, even if a prosecutor rubber stamped it. The absence of particularized probable cause was apparent because the application obviously failed to connect Mr. Chatrie (or anyone else) to the crime in any way. The only case-specific fact alleged was that the suspect spoke into a cell phone, which provides no meaningful limit. An objectively reasonable police officer has been trained to know what probable cause looks like. This was not it.

Likewise, no reasonable officer could believe this geofence warrant satisfied the Fourth Amendment's particularity requirement. The crux of particularity involves eliminating officer discretion, but this warrant left abundant discretion to Google and the police. The three-step process did not cure this defect. J.A. 1376. Rather, it now appears that the three-step process was intended to either appease Google or deceive the issuing magistrate. This absence of particularity is appalling, especially where, as here, the data searched can reveal protected activities ranging from participation in a protest to accessing healthcare. *See Stanford v. Texas*, 379 U.S. 476, 485 (1965); Amici Curiae Tech. L. & Pol'y Clinic at N.Y.U. Sch. of L. & Elec. Frontier Found. Br. 23-26; Amicus Curiae The Reporters' Comm. for Freedom of the Press Br. 5-15.

If "scrupulous exactitude" means anything, *Stanford*, 379 U.S. at 485, it must compel rigorous compliance with the particularity requirement in these circumstances. It cannot mean that almost *every* crime would justify a geofence warrant simply

because many people own smartphones. Based on the government's logic, there would be probable cause to seek location data every time something illegal occurs, regardless of the crime's connection to a suspect's smartphone or location data. It would mean anyone using Location History "has effectively been tailed every moment of every day," allowing the government to "call upon the results of that surveillance" whenever it wants. *Carpenter*, 138 S. Ct. at 2218.

Lastly, the government relies on *United States v. McLamb*, 880 F.3d 685 (4th Cir. 2018), to bolster its claim that the investigator's "consult[ation] with prosecutors about geofence warrants" meant "he behaved reasonably for an investigator seeking to employ a new investigative technique." Gov't Br. 54. *McLamb* stands for the idea that the good-faith exception was appropriate "where the legality of an investigative technique is unclear" and law enforcement seeks advice from counsel. 880 F.3d at 691. But as Mr. Chatrie has explained, probable cause and particularity are not novel requirements. Appellant's Br. 24. Rather, they are bedrock principles on which the Fourth Amendment was built.

As the district court recognized, those requirements do not change when "cloaked by the complexities of novel technology," J.A. 1368, especially when the government fails to describe the nature of the search accurately. *See* 880 F.3d at 690 (noting that *McLamb* "devoted several pages [of its supporting affidavit] to explaining the" new investigative technique, providing a "detailed description of the [Network

Investigative Technique that] was sufficient to inform the magistrate judge of the scope of the warrant sought"). The rapid rise of new technologies should not insulate the government's actions from their consequences. *See* Amici Curiae ACLU, ACLU of Va., and Eight Fed. Pub. Def. Offs. within the Fourth Cir. Br. 6-11. While there is no "bureaucratic" requirement that officers undergo training, Gov't Br. 54, crediting non-existent training is a material misrepresentation that cannot establish good faith. *See* J.A. 1353. Here, the affidavit did not mention the geofence warrant's scope or even suggest that it would search the Location History data of "numerous tens of millions" of Google users. No magistrate or prosecutor ever should have approved of and no officer ever should have relied on a warrant allowing for the search of every haystack around the world and conferring on the police unfathomable discretion to execute it.

CONCLUSION

For the reasons stated above and in the opening brief, 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 May 15, 2023

CERTIFICATE OF COMPLIANCE

1. This reply brief 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 6,500 words, specifically 5,440 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.

May 15, 2023
Date

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