

No. 22-4489

**IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH COURT**

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)**

JOINT APPENDIX

VOLUME 5 of 11 (pages 1071 - 1326)

JESSICA D. ABER
United States Attorney

Kenneth R. Simon, Jr., Ass't U.S. Attorney
Peter S. Duffey, Ass't U.S. Attorney
Counsel for Appellee
919 East Main Street, Suite 1900
Richmond, VA 23219
(804) 819-5400

Nathan P. Judish, Senior Counsel
Computer Crime & Intel. Property Section
Criminal Division
U.S. Department of Justice

GEREMY C. KAMENS
Federal Public Defender

Laura J. Koenig
Assistant Federal Public Defender
Counsel for Appellant
701 East Broad Street, Suite 3600
Richmond, VA 23219
(804) 565-0800

Michael W. Price, Litigation Dir.
NACDL Fourth Amendment Ctr.
1660 L Street NW, 12th Floor
Washington, DC 20036

This page intentionally left blank for double-sided pagination and printing

TABLE OF CONTENTS

VOLUME 1 (pages 1 - 176)

District Court Docket Sheet (as of Jan. 17, 2023)	1
Indictment (Sept. 17, 2019, Doc. 1).....	22
Defendant’s Motion to Suppress Evidence Obtained From a “Geofence” General Warrant (Oct. 29, 2019, Doc. 29)	25
Government’s Response in Opposition to Defendant’s Motion for Suppression of Evidence Obtained Pursuant to Google Geofence Warrant (Nov. 19, 2019, Doc. 41).....	51
Defendant’s Reply to Government’s Response [to] Motion to Suppress Evidence Obtained From a “Geofence” General Warrant (Dec. 9, 2019, Doc. 48).....	76
Exh. A (First Step 2 Request to Google) (Doc. 48-1)	98
Exh. B (Second Step 2 Request to Google) (Doc. 48-2)	100
Exh. C (Third Step 2 Request to Google) (Doc. 48-3)	102
Exh. D (Transcript, <i>Commonwealth v. Anderson</i> , No. CR17-4909-00F (Va. Cir. Ct., Jan. 4, 2019)) (Doc. 48-4).....	omitted from J.A.
Government’s Notice Regarding Attachment of Google Geofence State Search Warrant to Response in Opposition to Motion to Suppress (Dec. 18, 2019, Doc. 54)	104
Affidavit for search warrant and warrant, with attachments (Doc. 54-1)	107
Brief of Amicus Curiae Google LLC in Support of Neither Party Concerning Defendant’s Motion to Suppress Evidence From a “Geofence” General Warrant (Dec. 20, 2019, Doc. 59-1)	118
United States’ Response to Amicus Curiae Brief of Google LLC (Jan. 10, 2020, Doc. 71).....	148
Defendant’s Response to Google’s Motion to File Amicus Curiae Brief in Support of Neither Party (Jan. 10, 2020, Doc. 72)	158

VOLUME 2 (pages 177 - 416)

Transcript, Discovery Motion Hearing (Jan. 21, 2020, Doc. 81; <i>see</i> Doc. 77 (court minutes)).....	177
Preliminary matters.....	179
Def't witness Spencer McInville	
Direct examination.....	193
Cross examination.....	283
Redirect examination	306
Argument by the defense	318
Argument by the government	332
Rebuttal by the defense.....	350
Court's ruling.....	355
Defendant's Supplemental Motion to Suppress Evidence Obtained From a "Geofence" General Warrant (May 22, 2020, Doc. 104).....	363
United States' Response in Opposition to Defendant's Motion for Suppression of Evidence Obtained Pursuant to Google Geofence Warrant (June 12, 2020, Doc. 109).....	393

VOLUME 3 (pages 417 - 694)

Transcript, Suppression Motion Hearing, Day 1 (evidence) (Mar. 4, 2021, Doc. 201; <i>see</i> Doc. 198 (court minutes)).....	417
Preliminary matters.....	420
Def't witness Spencer McInville	
Direct examination.....	432
Cross examination.....	542
Redirect examination	586
Def't witness Marlo McGriff	
Direct examination.....	606

VOLUME 4 (pages 695 - 1070)

Transcript, Suppression Motion Hearing, Day 2 (evidence) (Mar. 5, 2021, Doc. 202; <i>see</i> Doc. 199 (court minutes)).....	695
Preliminary matters.....	698
Def’t witness Marlo McGriff, cont’d Direct examination.....	699
Cross examination.....	791
Redirect examination	841
Def’t witness Sarah Rodriguez Direct examination.....	862
Cross examination.....	902
Redirect examination	916
Gov’t witness Jeremy D’Errico Direct examination.....	923
Cross examination.....	967
Redirect examination	1010
Gov’t witness Joshua Hylton Direct examination.....	1016
Cross examination.....	1040
Redirect examination	1063
Concluding matters	1064

VOLUME 5 (pages 1071 - 1326)

Defendant’s Post-Hearing Brief on “Geofence” General Warrant (May 3, 2021, Doc. 205).....	1071
Government’s Response in Opposition to Defendant’s Motion for Suppression (May 21, 2020, Doc. 214; <i>see</i> Doc. 207-2).....	1117
Defendant’s Reply to Government’s Response in Opposition to Motion for Suppression (June 4, 2020, Doc. 213)	1164
Transcript, Suppression Hearing (arguments) (June 24, 2021, Doc. 217; <i>see</i> Doc. 215 (court minutes)).....	1185

Argument by the defense	1187
Argument by the government	1231
Rebuttal by the defense.....	1313
Concluding matters	1322

VOLUME 6 (pages 1327 - 1456)

Memorandum Opinion (denying suppression motion) (Mar. 3, 2022, Doc. 220).....	1327
Order (denying suppression motion) (Mar. 3, 2022, Doc. 221)	1390
Criminal Information (May 6, 2022, Doc. 224)	1391
Transcript, Change of Plea Hearing (May 9, 2022, Doc. 247; <i>see</i> Doc. 226)	1394
Plea Agreement (May 9, 2022, Doc. 228)	1428
Statement of Facts (May 9, 2022, Doc. 229)	1444
Judgment in a Criminal Case (Aug. 19, 2022, Doc. 239).....	1449
Notice of Appeal (Aug. 25, 2022, Doc. 241).....	1456

VOLUME 7 (pages 1457 - 1810) – DOCUMENT EXHIBITS

Exhibits Admitted at Discovery Motion Hearing (Jan. 21, 2020)

Def't Exh. 1: Geofence Warrant & Application (same as Doc. 54-1, minus ECF header)	<i>see</i> J.A. 107
Def't Exh. 2: Google Amicus Brief (Doc. 59-1)	<i>see</i> J.A. 118
Def't Exh. 3: PDF of Raw Data (sealed)	<i>see</i> J.A. 2093
Def't Exh. 4: Activation Video.....	omitted from J.A., available on request
Def't Exh. 5: Three Paths Video (sealed)	<i>see</i> J.A. 2139
Def't Exh. 6: First Step 2 Request to Google	1457
Def't Exh. 7: Second Step 2 Request to Google.....	1459
Def't Exh. 8: Third Step 2 Request to Google	1461

Def't Exh. 9: Step 3 Request to Google	1463
--	------

Exhibits Admitted at Suppression Motion Hearing (Mar. 4-5, 2021)

Def't Exh. 1: Geofence Warrant & Application (same as Doc. 54-1, minus ECF header)	<i>see</i> J.A. 107
Def't Exh. 2: Google Amicus Brief (Doc. 59-1)	<i>see</i> J.A. 118
Def't Exh. 3: PDF of Raw Data (sealed)	<i>see</i> J.A. 2093
Def't Exh. 5: Three Paths Video (sealed)	<i>see</i> J.A. 2139
Def't Exh. 6: Spencer McInville Report	1464
Def't Exh. 7: Spencer McInville Supplemental Report	1469
Def't Exh. 8: CSV Google Data File (.csv file)	<i>see</i> J.A. 2139
Def't Exh. 9: Unique in Crowd Study	1475
Def't Exh. 11: September 2018 Oracle Submission	1480
Def't Exh. 18: Federal Search Warrant Application & Attachments	1502
Def't Exh. 19: State Search Warrants & Attachments	1534
Def't Exh. 21: McGriff Declaration 1 (Doc. 96-1)	1551
Def't Exh. 23: McGriff Declaration 3 (Doc. 147)	1562
Def't Exh. 24: Rodriguez Declaration (Doc. 96-2)	1579
Def't Exh. 27: Every Step You Take	1587
Def't Exh. 30: AZ Ex. 18 (admitted portions only)	1631
Def't Exh. 31: AZ Ex. 19 (admitted portions only)	1633
Def't Exh. 32: AZ Ex. 20	1639
Def't Exh. 33: AZ Ex. 24	1644
Def't Exh. 34: AZ Ex. 202	1667
Def't Exh. 36: AZ Ex. 209	1777
Def't Exh. 38: AZ Ex. 219	1781
Def't Exh. 40: AZ Ex. 236	1797
Def't Exh. 41: AZ Ex. 260	1804

VOLUME 8 (pages 1811 - 2090) – DOCUMENT EXHIBITS, CONT'D

Exhibits Admitted at Suppression Motion Hearing (Mar. 4-5, 2021), cont'd

Def't Exh. 43: May 2018 Privacy Policy – Redline	1811
Def't Exh. 43a: May 2018 Privacy Policy – Redline (with internet source information)	1840
Def't Exh. 44: Jan. 2019 Privacy Policy – Redline	1865
Def't Exh. 45: Oct. 2019 Privacy Policy – Redline	1895
Def't Exh. 46: McGriff Blog 1	1926

Def't Exh. 47: McGriff Blog 2	1929
Def't Exh. 48: 2018 Quartz Article	1934
Def't Exh. 49: 2018 AP Article 1	1941
Def't Exh. 51: 2019 NYT Article	1948
Def't Exh. 53: Blumenthal-Markey Letter to FTC	1957
 Gov't Exh. 1: CAST PowerPoint Presentation.....	1981
Gov't Exh. 2: Geofence Warrant (Doc. 54-1)	<i>see</i> J.A. 107
Gov't Exh. 3: Declaration of Marlo McGriff (Mar. 11, 2020) (same as Def't Exh. 21 (Doc. 96-1))	<i>see</i> J.A. 1551
Gov't Exh. 3a: Declaration of Sarah Rodriguez (Mar. 11, 2020) (same as Def't Exh. 24 (Doc. 96-2))	<i>see</i> J.A. 1579
Gov't Exh. 3b: Supplemental Declaration of McGriff (June 17, 2020) (Doc. 110-1).....	2032
Gov't Exh. 3c: Third Declaration of Marlo McGriff (Aug. 7, 2020) (same as Def't Exh. 23 (Doc. 147)).....	<i>see</i> J.A. 1562
Gov't Exh. 4: Joshua Hylton emails with Google	2034
Gov't Exh. 5: Google Privacy Policy	2048
Gov't Exh. 5a: Google Terms of Service	2081
Gov't Exh. 6: Special Agent D'Errico's C.V.	2088
Gov't Exh. 12: "Got to Be Mobile" Video	<i>see</i> J.A. 2091

VOLUME 9 (pages 2091 - 2092) – DIGITAL MEDIA EXHIBIT

Gov't Exh. 12: "Got to Be Mobile" Video (admitted only at suppression motion hearing).....	(.mp4 file)
---	-------------

VOLUME 10 (pages 2093 - 2138) – SEALED DOCUMENT EXHIBIT

Def't Exh. 3: PDF of Raw Data (<i>see</i> Doc. 69 (sealing order)) (admitted at both discovery motion hearing and suppression motion hearing).....	2093
--	------

VOLUME 11 (pages 2139 - end) – SEALED DIGITAL MEDIA EXHIBITS

Def't Exh. 5: Three Paths Video (admitted at both discovery motion hearing and suppression motion hearing)	(.mp4 file)
Def't Exh. 8: CSV Google Data File (admitted only at suppression motion hearing)	(.csv file, viewable in Excel)

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division**

UNITED STATES OF AMERICA)	
)	
)	Case No. 3:19cr130
)	
OKELLO T. CHATRIE,)	
Defendant)	

MR. CHATRIE’S POST-HEARING BRIEF ON “GEOFENCE” GENERAL WARRANT

At the government’s direction, Google searched the Location History (“LH”) data of “numerous tens of millions” of people in an effort to generate suspects in the robbery. *See* Def. Ex. 21 at 4. It was a dragnet of epic proportions. The warrant seeks to dress up this search in a “three-step” process crafted by Google and the FBI, but that process is no more than a legal fig leaf obscuring the magnitude of the privacy invasion at work. This epic dragnet gave free reign to Google and the government to single out which accounts to search further in steps two and three. It was so overbroad and lacking in particularity that it was the digital equivalent of a general warrant and therefore impermissible under the Fourth Amendment. Mr. Chatrie seeks to suppress all evidence obtained as a result of the geofence warrant, and all fruits thereof.

BACKGROUND

In March 2021, this Court held an evidentiary hearing on Mr. Chatrie’s motion to suppress the geofence warrant. *See* ECF 29. Mr. Chatrie had filed that suppression motion in October 2019, based on the sparse facts available to him at that time. What little defense counsel knew about geofence warrants came primarily from newspaper articles and online reports. *See id.* at 4-5. Over the past 18 months, however, investigation revealed significant new facts that have both merited corrections and strengthened Mr. Chatrie’s legal arguments.

Specifically, Google filed an *amicus* brief (Def. Ex. 2), unsolicited, as well as four written declarations (Def. Ex. 21; ECF No. 96-2; ECF No. 110-1; Def. Ex. 23) in response to two defense subpoenas *duces tecum* (ECF No. 82; ECF No. 123). In addition, two Google representatives, Marlo McGriff and Sarah Rodriguez, testified in person over the course of two days. Tr. 190–275 282–424, 445–499.¹ The Commonwealth of Virginia provided some information about the qualifications of the magistrate judge who issued the warrant. *See* ECF No. 156. And defense counsel benefited from the expertise of Spencer McInville, who forensically examined Mr. Chatrie’s phone, prepared two written reports (Def. Ex. 6; Def. Ex. 7), and testified twice in person. *See* Tr. 16–170; 1/21/20 Tr. 17—139. Furthermore, counsel for Mr. Chatrie cross-examined the Virginia state investigator responsible for obtaining and executing the geofence warrant, Det. Joshua Hylton, Tr. 623–46, and FBI Special Agent Jeremy D’Errico, who offered expert testimony for the government. Tr. 550–93. Finally, three federal magistrates, all in the Northern District of Illinois, have issued opinions, *sua sponte*, regarding geofence warrants. *In re Search Warrant Application for Geofence Location Data Stored at Google* (“Harjani Opinion”), No. 20 M 525, 2020 WL 6343084 (N.D. Ill. Oct. 29, 2020); *In re Information Stored at Premises Controlled by Google* (“Fuentes Opinion”), 481 F. Supp. 3d 730 (N.D. Ill. 2020); *In re Information Stored at Premises Controlled by Google* (“Weisman Opinion”), No. 20 M 297, 2020 WL 5491763 (N.D. Ill. July 8, 2020). Two of the three found the warrants invalid. *See* Fuentes Opinion, 481 F. Supp. 3d at 757; Weisman Opinion, 2020 WL 5491763 at *8. All three of them, however, did so without the benefit of adversarial briefing or the full factual record now before this Court.

Mr. Chatrie submitted a supplemental brief to the Court in May 2020. *See* ECF No. 104. Most significantly, by then, Google clarified that the geofence warrant required searching

¹ All cites to “Tr.” refer to the March 4–5, 2021, hearing unless otherwise noted.

“numerous tens of millions” of people, not just the 19 who happened to be near to the bank. *See* Def. Ex. 21 at 4. Google subsequently confirmed this fact at the March hearing and provided additional context that supports Mr. Chatric’s argument in favor of suppression. Mr. Chatric’s arguments have evolved accordingly, and defense counsel has sought to keep the Court abreast of these developments. *See, e.g.*, ECF No. 104 at 2, 4; ECF No. 82 at 2–3. But in the interest of clarity, Mr. Chatric summarizes the relevant facts as they are currently known.

FACTS

Someone robbed the Call Federal Credit Union in Richmond, Virginia, on May 20, 2019. *See* Def. Ex. 1 at 11. The Chesterfield County Police Department had no suspects. There were plenty of witnesses and surveillance videos, Tr. 607–08, but instead of pursuing traditional investigative techniques, the government turned to Google. Det. Joshua Hylton drafted an application for a “geofence” warrant, a novel digital search that required Google to identify all electronic devices in the area at the time of the robbery, and then provide even more data on devices of interest at the government’s discretion. *See* Def. Ex. 1.

Det. Hylton had never received training on geofence warrants. Tr. 627–28. There was no training because there were no law enforcement procedures to follow. Tr. 552–53. In fact, neither the Chesterfield Police nor the FBI, who quickly became involved in this case, trained their investigators on seeking geofence warrants. *Id.*; Tr. 552. Agent D’Errico assisted in the investigation and testified as the government’s expert on geofence warrants. Tr. 506–50. Yet, like Det. Hylton, Agent D’Errico admitted he has never received specific training on geofence warrants, from the FBI or from Google. Tr. 551.

This lack of training and absence of procedures does not mean that police conjured the geofence warrant here. The basic contours of a geofence warrant were the unofficial product of

repeated discussions between Google and the Computer Crimes and Intellectual Property Section (“CCIPS”) of the Department of Justice in 2018.² Tr. 456-57. Google required a warrant because it considers Location History data to be “content” under the Stored Communications Act, 18 U.S.C. § 2703, which requires a warrant to access it. *See* Def. Ex. 2 at 16.³

Eventually, Agent D’Errico obtained a “go by” from CCIPS, which “assists” investigators “in the language needed to obtain a geofence search warrant” from Google. Tr. 552; *id.* at 553 (“[W]e follow the steps that [CCIPS and Google] have laid out in order to ... make sure that Google understands what we are requesting and that we understand what we’ll receive back”). Agent D’Errico does not recall providing this “go by” to Det. Hylton, at least in this case. Tr. 553. But somehow or another—he does not recall—Det. Hylton got one too. Tr. 635. In fact, Det. Hylton had sought a state geofence warrant once before using a local “go by” from another officer, so he used the same template, plugged in the new date and location, and did it again. Tr. 631.

I. Location History

The warrant outlined a three-step process for Google to search users’ location data and provide information about nearby devices around the time of the robbery. The warrant did not instruct Google to exclude any types of location data from the search. Rather, it called for searching “each type of Google account,” regardless of the device configuration. Def. Ex. 1 at 4, 9. Instead, Google searched one of its three databases: the so-called “Sensorvault” database, which is the repository for “Location History” data. *See* Tr. 211-12; ECF No. 104 at 6-7.

² Tr. 456-57 (“CCIPS is an agency that ... our counsel engages with to discuss sort of certain procedures that may be relevant for the way that ... Google will need to handle these types of requests, especially with reverse Location History being a relatively new type of request”); 476 (repeated “engagement” between CCIPS and Google “help[ed] to socialize the concept of these types of warrants”); *see also* Tr. 552-53 (discussing the relationship with CCIPS).

³ The government disputes Google’s characterization of Location History data as user “content,” *see* ECF No. 109 at 9; ECF No. 71 at 8, but it has yet to cite to a single case where a subpoena or court order have been sufficient to obtain Location History data.

Location History is a Google feature that logs device location data and creates a timeline on a map of where a user has been with that device. Def. Ex. 21 at 2; Tr. 355. Google likens Location History data to a virtual “journal” of where users have been (with their devices). Def. Ex. 2 at 6; Tr. 204. When Google saves this data, it associates it with unique user accounts it keeps in the “Sensorvault.” Def. Ex. 21 at 3; Tr. 130, 314. If a user has the Google Location History enabled, then Google estimates the user’s device location using Global Positioning System (“GPS”) data, the signal strength of nearby Wi-Fi networks, Bluetooth beacons, cell phone location information (“CSLI”) from nearby cellular towers, and Internet Protocol (“IP”) address information. Tr. 18–19; Def. Ex. 21 at 4, 8–9. Location History is not an “app”; it is a setting on the Google account associated with a device. Once enabled, it records that device’s location as often as every two minutes, at all times regardless of whether any app is open or closed, the phone is in use, or the device is in a public or private space. Tr. 20, 114–15, 436–37, 513. Approximately one-third of all active Google users have Location History enabled on their accounts. Def. Ex. 21 at 4; Tr. 205. Google has been unable or unwilling to say exactly how many users this was in 2019, but Google acknowledges that it was at least “numerous tens of millions” of people. *Id.*

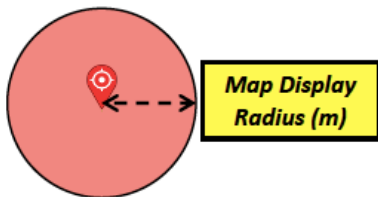
II. Location History Accuracy

The accuracy of Location History information varies depending on which sources of location data are available to the device at a given time. For example, location data based on GPS signals is usually more accurate than location derived from Wi-Fi signals. *See* 1/21/20 Tr. at 64. Google, however, has a preference. Google relies on Wi-Fi signals first, followed by GPS, then Bluetooth, and finally CSLI. Even though GPS data is generally more accurate than Wi-Fi, GPS consumes more resources on the device, diminishing battery life and making it impractical to use frequently. Tr. 519. As a result, Location History data often comes from Wi-Fi data, and that is what happened

in this case. Here, 88% of the coordinates at issue were derived from Wi-Fi signals; the remainder came from GPS. *See* 1/21/20 Tr. at 64. None were derived from Bluetooth, CSLI, or IP address information. *Id.*; *see also* Tr. 173.

Location History data is Google’s **estimation** of where a device is. Tr. 212. It is not hard data, but is instead Google’s best guess at device location based on available information. *See* Def. Ex. 2 at 10–11 n.7 (“In that respect, LH differs from CSLI, which is not an estimate at all, but simply a historical fact: that a device connected to a given cell tower during a given time period. An LH user’s Timeline, however, combines and contextualizes numerous individual location data points ...”). As Google puts it, Location History is a “probabilistic estimate,” and each data point has its own “margin of error.” *Id.* Google uses an unknown algorithm to make this estimation, which Google did not disclose when subpoenaed. *See* ECF No. 82 at 10; ECF No. 85 at 2. Indeed, Location History is different from other types of location data that courts have previously considered and emerges from Google’s black box with a fluctuating margin of errors. *See* Tr. 178, 590–91.

When Google reports a set of estimated latitude/longitude coordinates, it also reports a “confidence interval,” or “Map Display Radius,” to indicate Google’s confidence in its estimation. Tr. 38, 212, 530–31. On a map, Google visualizes the coordinates as a “blue dot” and the Display



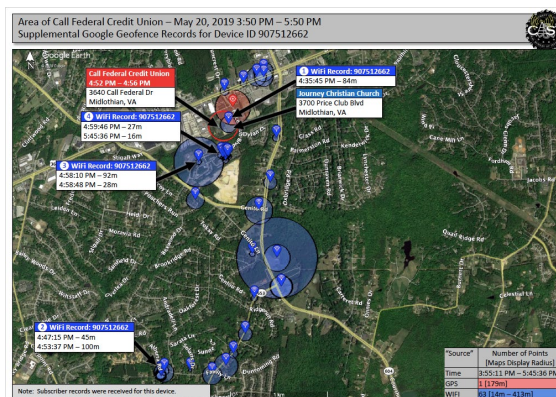
Radius as a “shaded circle” around the dot. *See* Tr. 213; Def. Ex. 21 at 9. The government illustrates this concept (in red) in a report Agent D’Errico prepared, as shown in Figure 1. *See* Gov’t Ex. 1 at 18.

Figure 1

Importantly, Google is equally confident that a device could be anywhere within the Display Radius, *i.e.*, the shaded circle. *See* Tr. 214. The estimated coordinates, recorded as

latitude/longitude, are simply the center point of that circle. *See* Tr. 531 (“If I could, I would draw maps without a center point in it and just a bubble because that’s a better representation.”). It is equally likely that the device is at the center point as anywhere else in the shaded circle, even off toward the edge. *See* Google, *Find and Improve your Location's Accuracy* (last visited Apr. 26, 2021) (“The blue dot shows you where you are on the map. When Google Maps isn’t sure about your location, you’ll see a light blue circle around the blue dot. You might be anywhere within the light blue circle.”).⁴ Indeed, Google users may be familiar with this phenomenon, as “in the common scenario of realizing that your cell phone GPS position is off by a few feet, often resulting in your Uber driver pulling up slightly away from you or your car location appearing in a lake, rather than on the road by the lake.” *Harjani Opinion*, 2020 WL 6343084 at *9.

The Map Display Radius expands and contracts in accordance with Google’s confidence in its location estimation. As a result, the accuracy of Location History data varies over time, as illustrated by the varying size of the shaded circles in the government’s rendition of user data in this case, as shown in Figure 2 below. **Figure 2**



Google always aims to be 68% confident that a device is somewhere within the Display Radius. Tr. 39; *see also* Tr. 581 (“68% is approximately the industry standard”). In other words,

⁴ Available at <https://support.google.com/maps/answer/2839911?co=GENIE.Platform%3DAndroid&hl=en>.

Google simply changes the size of the Display Radius, or shaded circle, in order to achieve 68% confidence. As Google explains, “The smaller the circle, the more certain the app is about your location.” Google, *Find and Improve your Location's Accuracy* at 1. By contrast, a large circle means that Google is less confident in a user’s location, indicating that they could be anywhere within a much larger area, the product of a larger Display Radius. *See* Tr. 213, 530-31. There is always a 32% chance a device is outside of the Display Radius altogether. *See* Tr. 213. Or in other words, the odds are better than 1-in-4 that the user’s actual location lies beyond the shaded circle.

III. Location History Advertising

Google appears well satisfied with the 68% accuracy industry standard. *See* Tr. 581. According to Google, “the resulting picture of the user’s location and movements is sufficiently precise and reliable for the purposes for which it was designed.” Def. Ex. 2 at 10 n.7. For Google, Location History has two purposes: (1) to support a “Timeline” map for users, *see* Tr. 195, and (2) to provide targeted advertising based on a user’s location, *see* Tr. 22-23, 196–98, 301. Neither function, however, relies on a high degree of accuracy for any data point. Rather, Google infers a user’s Timeline from a series of data points even when an “outlier” strays from the logical path. *See* Tr. 195–96. For advertising purposes, Google actively obscures individual device information, preventing businesses from being able to track particular users. *See* Tr. 197.

Google uses Location History for a specific advertising purpose—to calculate “store visit conversions.” A “store visit conversion” refers to a user who saw a Google-placed advertisement and then visited the relevant business in person. Tr. 196–97. Location History is not used for other types of location-based advertising, such as “radius targeting,” Tr. 197–98, which allows businesses to show an ad to all devices in a given area. As Google explains, “Location History does not power all ads. ... [A]ny geotargeting or other use of Location for ads is coming from the

location services at the device level.” Tr. 367–68. So, although businesses can use Google to target advertising based on a device’s location, they cannot do so using Location History. Tr. 198.

Regardless of the advertising type, however, Google “never share[s] anyone’s location history with a third party.” *See* Tr. 197. Google is “not giving user location data over to stores about who was around.” Tr. 197. Even when Google uses location data sources other than Location History, such as “Web & App Activity,” the smallest possible radius available to advertisers is a kilometer. Tr. 198. This is done for privacy purposes, so that those advertisers do not actually get to see which devices were in the area. Tr. 197, 199. Likewise, advertisers cannot go back to Google and ask for more information about where certain devices were before or after they saw an ad or visited a store. Tr. 199. Advertisers simply cannot get any identifiable information about individual Google users. Tr. 199; *see also* Tr. 23 (explaining that the data in warrant returns is “much different” than what is accessible to advertisers).

IV. Enabling Location History

Google asserts that Location History is an “opt-in” feature for Google users, Def. Ex. 1 at 12, which means that a user must actively enable it at some point in order for it to work. There are, however, many different ways for a user to enable Location History, either through the device settings or through certain Google applications. Def. Ex. 6 at 4; Tr. 74; *see* Tr. 285–86.

One possibility is to enable Location History during the initial setup of a new device. As demonstrated by defense expert Spencer McInville during the January 2020 discovery hearing, Google first prompts users to enable Location History during the initial phone setup process. *See* 1/21/20 Tr. at 51. If a user does not opt-in at that point, Google will prompt them to enable Location History through pop-up screens, known as a “consent flow,” when opening certain Google applications or using certain Google features.

Another way to enable Location History is to set up Google applications that rely on location information. These apps include the primary Google App (for search queries), as well as Google Maps, Google Photos, and Google Assistant. *See* Tr. 221, 285–86. If a user does not enable Location History while setting up the device, Google prompts them to do so before they can use any of these applications. *See* Tr. 350–52. For example, as the defense demonstrated through video evidence and detailed expert testimony, Google prompts users to enable Location History when first opening Google Maps following the setup of a new phone. 1/21/20 Tr. at 55–56. The whole process took under five minutes and did not mention Location History by name. *Id.* at 56–57.

In this case, a combination of Google data and an extensive forensic analysis of Mr. Chatrie’s phone revealed that Location History was likely enabled through the Google Assistant setup process, shortly after midnight on July 9, 2018. Def. Ex. 6 at 4–5; Tr. 76–77, 286–87. Two basic facts led to this conclusion. *See* Def. Ex. 6 at 4–5. First, Google reported that Location History was enabled on Mr. Chatrie’s account on July 9, 2018, at approximately 4:09 Universal Time Code (“UTC”), or 12:09 a.m. Eastern time. *See* Def. Ex. 6 at 2; Def. Ex. 23 at 2. Second, Mr. Chatrie’s phone shows that Google Assistant was installed two minutes earlier, at 4:06:51 UTC. A Google “Audit Log” shows three timestamps indicating changes to the Location History setting occurred just seconds later at 04:07:25 UTC, 4:09:08 UTC, and 04:09:08 UTC. *See* Def. Ex. 6 at 4. Therefore, Mr. McInville concluded that “it is likely Google Location History was enabled using the Google Assistant application.” Def. Ex. 6 at 5. Neither the government nor Google can challenge this conclusion. *See* Tr. 287.

When a user who does not have Location History enabled attempts to use Google Assistant for the first time, Google displays a pop-up box that is part of a “consent flow” that prompts the user to enable up to three Google features, including Location History. This pop-up box will also

appear if the user “long press[es] the home button” on an Android device that does not have Google Assistant set up. Tr. 79; Tr. 351. A “long press” means leaving one’s finger on the button for a moment, as opposed to tapping it quickly; the “home button” is the big button at the bottom of the screen. On Android devices like Mr. Chatrie’s, a long press of the home button will activate Google Assistant, as if a user had opened the application by tapping on an icon.

Neither Google nor any party has been able to definitively state how this “consent flow” would have appeared on Mr. Chatrie’s device on July 8, 2018. Tr. 81, 298. There are two possibilities, however. *See* Def. Ex. 7 at 1–3; Tr. 298. First, the screen could have read: “Creates a private map of where you go with your signed-in devices” with a blue “YES I’M IN” button, as shown below in Figure 3. *See* Def. Ex. 7 at 2. Alternatively, the screen could have read: “Saves where you go with your devices” with a blue “TURN ON” button, as shown below in Figure 4. *See* Def. Ex. 7 at 4; Def. Ex. 23 at 8; Tr. 102, 298. Google calls this line the “descriptive text.” Tr. 328. Above both versions of the descriptive text, at the top of the screen, was a sentence that read: “The Assistant depends on these settings in order to work correctly.” Def. Ex. 7 at 3. And at the bottom of the screen, separated by a line and in lighter and less-contrasting font, were two additional sentences indicating that this data “may be saved” and that “You can see your data, delete it and change your settings at account.google.com.” Def. Ex. 7 at 4; Def. Ex. 23 at 8.

Figure 3

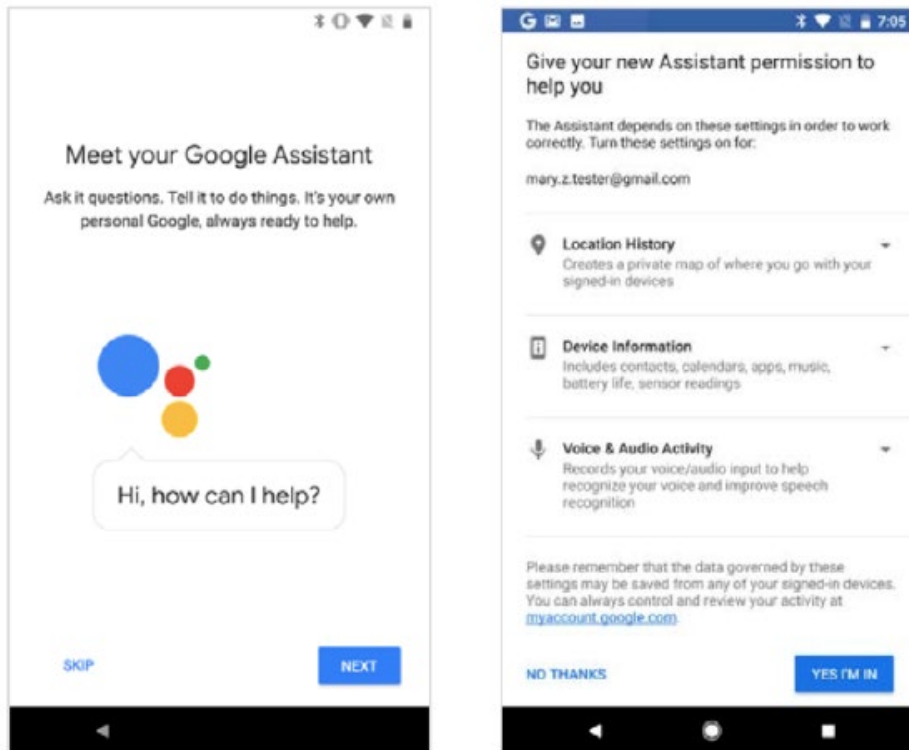


Figure 4

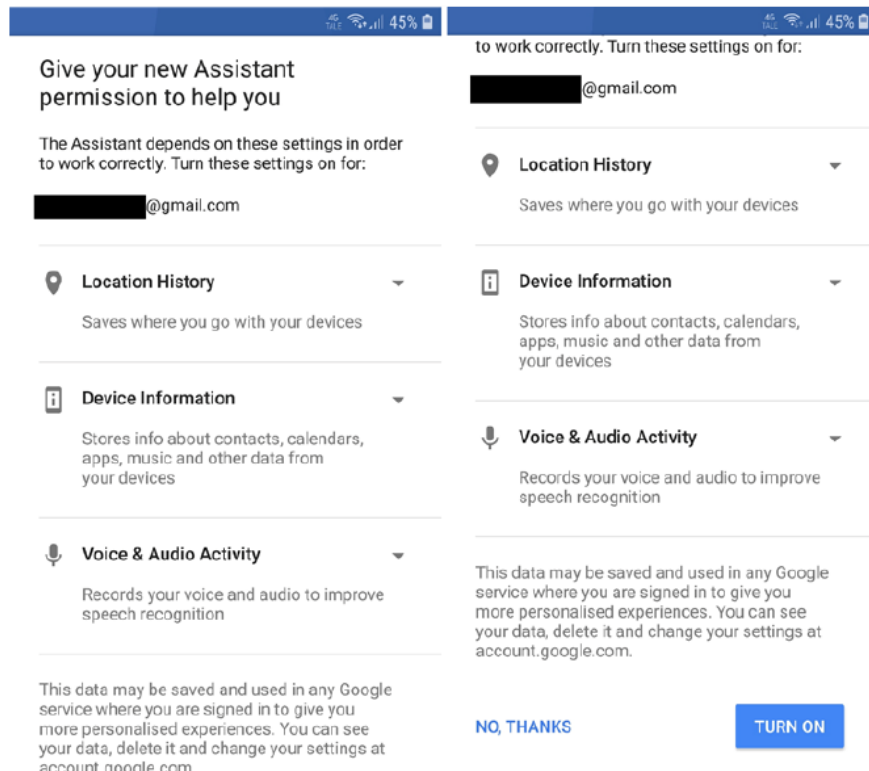
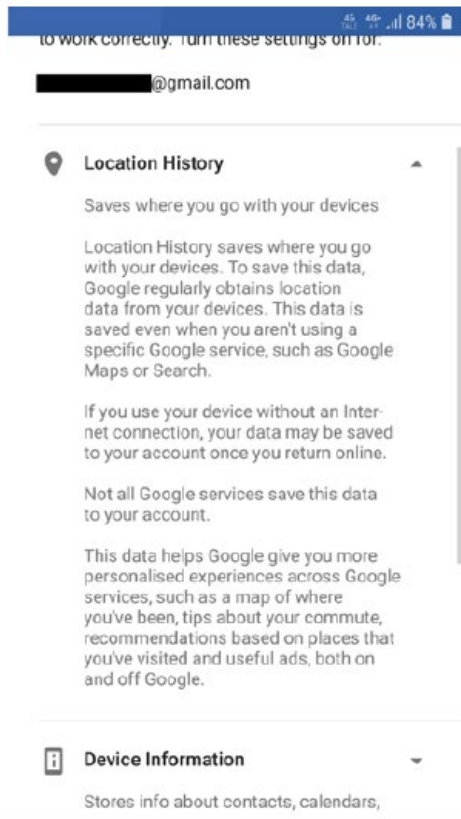


Figure 5



As shown here in Figures 3 and 4, this screen would have asked users to enable two other Google settings—“Device Information” and “Voice & Audio Activity”—if not already enabled. Def. Ex. 7 at 3; Tr. 109, 333. If presented with more than one permission, a user would have had to enable all of them together, or else quit the Google Assistant setup. Tr. 109, 334. In other words, users were not given the option to make an individual determination with respect to each of the three possible permissions. *Id.*

Additional information, which Google calls the “consent copy text,” is shown only if users tap on the “expansion arrow,” the small triangle on the other side of the page from “Location History.” *See* Tr. 106, 329. Figure 5 depicts this “copy text” for Location History, which would have been the same regardless of which “descriptive text” appeared. *See* Def. Ex. 7 at 3; Tr. 271. **Users are not required to view the “copy text.”** Tr. 330. Only users who tap the expansion arrow will see it. Def. Ex. 7 at 3; Tr. 110, 345. **And users can enable Location History without ever seeing this information.** *See* Tr. 110, 330, 335.

The Google Assistant setup screen did not contain or link to Google’s Privacy Policy. *See* Def. Ex. 7 at 1–4. Users who nonetheless viewed Google’s Privacy Policy during the relevant timeframe—from when Mr. Chatrue enabled Location History in July 2018 to his arrest in September 2019—would have seen two different versions of the policy depending on when they accessed it. In the first iteration, in effect from May 2018 to January 2019, the Privacy Policy

mentioned “Location History” twice. *See* Tr. 294. The first reference read: “You can also turn on Location History if you want to save and manage location information in your account.” Def. Ex. 43 at 7. The second reference stated: “Decide what types of activity you’d like saved in your account. For example, you can turn on Location History if you want traffic predictions for your daily commute, or you can save your YouTube Watch History to get better video suggestions.” *Id.* at 8. The next iteration of the Privacy Policy covered January 2019 to October 2019, and changed the first reference to read: “You can also turn on Location History if you want to create a private map of where you go with your signed-in devices.” Def. Ex. 44 at 7. The second reference remained the same. *See id.* at 8.

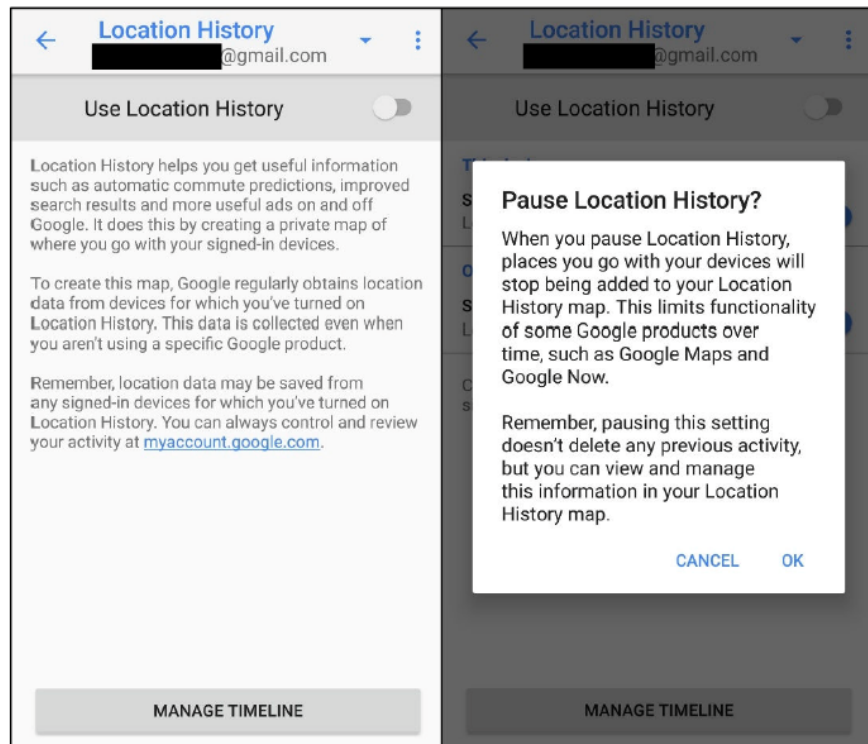
V. “Pausing” Location History

Once enabled, Location History cannot be turned “off,” only paused. Tr. 360–61. There are three ways to pause Location History: (1) in the settings for an application like Google Assistant, (2) in the settings panel for the device, or (3) by logging in to “myactivity.google.com” and changing the account’s settings. *See* Tr. 340–41. These are the only methods of pausing Location History. **If a user disables or stops using Google Assistant, for example, Location History is still enabled and running.** Tr. 123-24, 362. A user has to know to actively navigate one of these paths in order to locate and pause Location History. Tr. 341. Upon doing so, Google would display another pop-up screen containing text called the “pause copy,” as shown in Figure 6. Def. Ex. 27 at 23.

The text of the “pause copy” warns users that pausing Location History will “limit[] functionality of some Google products over time, such as Google Maps and Google Now.” It does not specifically mention Google Assistant or provide any details about how app functionality might be limited. In fact, Google Assistant will continue to function with Location History paused, but

Google does not inform users of this option, either when setting up the application or when displaying the “pause copy.” *See* Tr. 339, 343.

Figure 6



VI. Deleting Location History

Just as pausing Location History does not delete Location History data, disabling Google Assistant does not delete Location History data. That requires manual input. *See* Tr. 356, 361. Google now offers an “auto-delete” function that allows users to automatically delete Location History data older than three months, *see* Def. Ex. 46, but this function was unavailable for Mr. Chatrie. Tr. 356. To delete Location History data manually, a user must access the “Timeline UI,” or user interface, at which point records can be deleted by day or date range. Tr. 356. Deleting Location History records will not stop Location History from continuing to collect data. Tr. 188.

VII. The Geofence Warrant

The warrant in this case authorized the search of all Google Location History data, for all users, in order to identify devices of interest and obtain additional information about those accounts. The warrant outlines a dependent, three-step process, now familiar to this Court. *See* Def. Ex. 2 at 12–14; *see also* ECF No. 29 at 4–7; ECF No. 104 at 1–2.

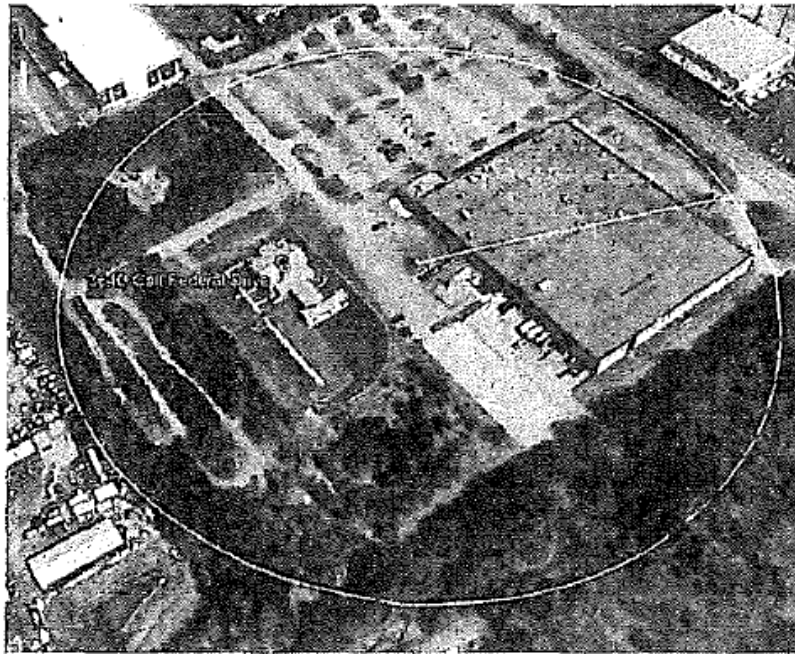
Step one required Google to search the Sensorvault to determine which devices were purportedly within 150 meters of the Call Federal Credit Union during the time of the robbery as well as 30 minutes before and after it occurred. Def. Ex. 1 at 4. To carry out this command, Google had to search the contents of every account with Location History enabled, *i.e.*, “numerous tens of millions” users, for records satisfying the government’s criteria. Tr. 29, 52–53, 204–05. It is impossible to search only users who were within 150 meters of the bank because there is “no way to know *ex ante* which users may have [Location History] data indicating their potential presence in particular areas at particular times.” Def. Ex. 2 at 12. Rather, “Google must 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.” Tr. 204 (quoting Def. Ex. 2 at 12).

Google ultimately identified 19 accounts with responsive data. The government seized those records in a database file containing 210 location points on June 28, 2019. Tr. 132, 642. Google states it provided this data in “anonymized” form, meaning that it did not include account names or usernames. Tr. 404. It did, however, contain a “Device ID” number, a unique number in Sensorvault linked to the user’s device that does not change over time. Tr. 451, 453–54.

Google identified this data by selecting any devices with an estimated latitude/longitude inside the 150-meter geofence from the warrant, shown in Figure 7. For some of these location

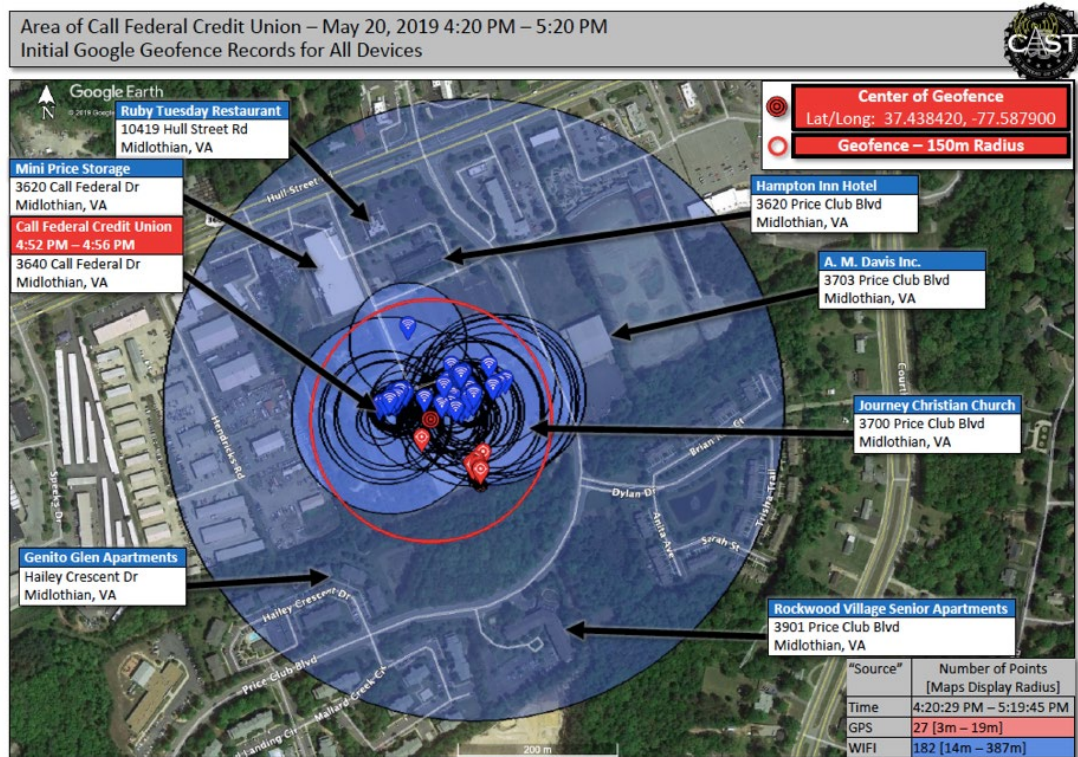
points, however, the Map Display Radius extended beyond the geofence, meaning that the device was just as likely to be outside the boundary. *See supra* at 7; Tr. 587–88. Both Google and the government acknowledge this possibility of “false positives.” *See* Tr. 586; Def. Ex. 2 at 9, 20 n.12.

Figure 7



The largest Display Radius is 387 meters from coordinates near the center of the 150-meter geofence. *See* Def. Ex. 3 at 6–12, 17–37. Consequently, the effective range of the search was more than twice as far as the geofence requested in the warrant. Tr. 41–42. Agent D’Errico notes that the actual location of that device remains unknown, meaning that it could have been inside or outside the geofence. *See* Tr. 587. All agree, however, that there is a 68% chance it was somewhere in the largest blue circle depicted in Figure 8 below. Tr. 39–40, 215, 587. That circle encompasses not just the bank and the Journey Christian Church, but also multiple streets plus all of the businesses and residences nearby—including Hull Street and Price Club Drive, Ruby Tuesday’s, the Hampton Inn, A.M. Davis, Inc., Mini Price Storage, the Genito Glen Apartments, and the Rockwood Village Senior Apartments. *See* Tr. 32–33, 49; 1/21/20 Tr. at 66–67.

Figure 8



Step two of the warrant process required the government to review the step one data and “attempt to narrow” the list of devices. Def. Ex. 1; Tr. 592. Google would then provide two hours of additional Location History data for a subset of those devices, called “contextual” data, for one hour before and after the robbery. *Id.*; Tr. 26, 30.

Initially, Det. Hylton sent two emails on July 1 and 2, 2019, each requesting contextual data for all 19 devices from step one. *See* Gov’t Ex. 4; Tr. 472, 622; ECF No. 96-2 at 5. Det. Hylton also requested the subscriber information for all 19, *i.e.*, “de-anonymized” records that the warrant reserved for step three. *Id.* Det. Hylton sent these emails after consulting with the United States Attorney’s Office. Tr. 622. When Det. Hylton did not receive a reply from Google, he left two voicemails on July 8, 2019. Tr. 621–22, 642. A Google specialist called back the same day and specifically advised Det. Hylton that the warrant required the government to narrow the number of devices for which they were seeking expanded data. Tr. 473–74. Google did not say by how

much the government had to narrow the list, but advised it was required. *Id.* at 474. The Google specialist also had to advise Det. Hylton about what types of information would be produced in the later stages of warrant. *Id.* The specialist reported to her supervisor, Ms. Rodriguez, that it did not appear Det. Hylton was familiar with the process outlined in the warrant. Def. Ex. 24 at 5-6.

Following the July 8 phone conversation with Google, Det. Hylton emailed Google once again, this time requesting stage two data (only) for nine of the 19 devices. Tr. 642. Accordingly, Google created another database file on July 9, 2019, containing the “contextual” data for those nine devices and sent it to the government. *See* Def. Ex. 8.

Step three of the warrant required the government to further cull the number of devices and identify an even narrower subset. Tr. 26, 543–44; Def. Ex. 1. Google would then produce de-anonymized account information, including the username and subscriber information, associated email addresses and telephone numbers. *Id.* The government twice requested this data for three devices on July 10 and 11, 2019. Tr. 643. On July 11, Google sent the government a third database file matching each “Device ID” with its “Gaia ID” as well as records reflecting the associated subscriber information. Tr. 544. One of those three subscribers was Mr. Chatrie.

ARGUMENT

The geofence warrant was an unconstitutional search that intruded upon Mr. Chatrie’s reasonable expectation of privacy in his Google data. For the reasons set forth below, Mr. Chatrie maintains that the warrant was invalid because it was a general warrant, fatally overbroad and devoid of particularity, and therefore impermissible under the Fourth Amendment. *See* ECF No. 29 at 7, 16–24; ECF No. 104 at 10. The *Leon* good faith doctrine does not apply because the warrant was so obviously deficient that it was *void ab initio*. As a result, this Court should suppress the results of the geofence warrant, including all of the fruits thereof.

I. Mr. Chatrie Had a Reasonable Expectation of Privacy in His Location History Data.

Mr. Chatrie enjoys a reasonable expectation of privacy in his Location History data following the Supreme Court’s landmark decisions in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), and *United States v. Jones*, 565 U.S. 400 (2012). Although the shortest search at issue in either case involved seven days of cell phone location information for a single individual, *see Carpenter*, 138 S. Ct. at 2217, the Court’s reasoning applies with at least equal force here. *See* ECF No. 104 at 10; ECF No. 29 at 9.

A. Location History Is At Least As Precise as CSLI

Location History data is at least as precise as the CSLI in *Carpenter*. *See* ECF No. 104 at 12–14. The government concedes this point. *See* ECF No. 41 at 8; ECF No. 109 at 9. In this case, all of the estimated Location History points derive from either Wi-Fi or GPS signals, which Google states are “capable of estimating a device’s location to a higher degree of accuracy and precision than is typical of CSLI.” Def. Ex. 21 at 4. Additionally, 12% of the data points in this case are from the same type of GPS signals at issue in *Jones*, which can be accurate to less than a meter. *See* Tr. 18–20; ECF No. 29 at 8; ECF No. 104 at 14.

But, Google did not design Location History to solve bank robberies. Google’s estimation of a device’s location may be “sufficiently precise and reliable for the purposes for which it was designed,” *i.e.*, creating a user Timeline and targeting advertisements within a kilometer. Def. Ex. 2 at 10 n.7.; *see also supra* at 8. But because Google did not design Location History to respond to 150-meter geofence warrants, its ability to accurately do so comes with caveats, such as the possibility of “false positives,” *see supra* at 8, 17, and “false negatives.” *See* Tr. 44–45, 47–48, 217, 585. Also, due to the Map Display Radius, the effective range of the search extended more than twice as far as the 150-meter circle described in the geofence warrant. *See supra* at 17.

B. A Search of Location History Data Is Highly Intrusive

A search of even small amounts Location History data is highly intrusive. As the government recognizes, *Carpenter* “explicitly declined to determine whether there is a ‘limited period’ for which the government can acquire cell phone location information without implicating the Fourth Amendment.” ECF No. 41 at 7. Short-term searches are capable of revealing the “privacies of life,” 138 S. Ct. 2214, which was the Court’s main concern in both *Carpenter* and *Jones*.

Although *Jones* and *Carpenter* involved so-called “long-term” searches,⁵ what motivated the Court in each instance was the risk of exposing information “the indisputably private nature of which takes little imagination to conjure: ‘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) (quoting *People v. Weaver*, 12 N.Y.3d 433, 441–42 (2009)); accord *Carpenter*, 138 S. Ct. at 2215. Thus, “[i]n cases involving even short-term monitoring, some unique attributes of GPS surveillance ... will require particular attention.” *Jones*, 565 U.S. at 415. The same is true for cell phone location information, given that “[a] cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor’s offices, political headquarters, and other potentially revealing locales.” *Carpenter*, 138 S. Ct. at 2218.

Even before *Jones* and *Carpenter*, the Supreme Court was concerned with short-term location tracking, especially when it reveals information about the interior of a constitutionally-protected space, such as a home. In *United States v. Karo*, the Court found that using an electronic beeper to track an object inside a private residence was a search. 468 U.S. 705, 716 (1984). A

⁵ In fact, the government’s demand for seven days of data in *Carpenter* netted only two days of data. See 138 S. Ct. at 2212.

search occurs at the moment the object “has been withdrawn from public view.” *Id.* at 717. Especially relevant here, the 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.” *Id.* at 716. So too in *Kyllo v. United States*, the Court found that using a thermal imaging device to peer through the walls of a private residence was a search. 533 U.S. 27, 37 (2001). It was a search despite the fact that the scan “took only a few minutes” and could not show people or activity inside. *Id.* at 30. As the Court explained, “[t]he Fourth Amendment’s protection of the home has never been tied to measurement of the quality or quantity of information obtained.” *Id.* at 37.

Here, the geofence search revealed Google users inside the bank as well as in nearby homes, apartment complexes, a hospital, and the Journey Christian Church. *See* 1/21/20 Tr. at 80–90 (describing the paths for “Mr. Green,” “Mr. Blue,” and “Ms. Yellow”). Although Google had “anonymized” this data, the defense was easily able to determine the likely identities of at least three individuals. *See* Tr. 62–70; ECF No. 104 at 12; 1/21/20 Tr. at 83, 87–88, 90–91. This is why Google treats Location History data not as a “business record” but as sensitive user “content” under the Stored Communications Act, 18 U.S.C. § 2703, likening it to a “digital journal” of users’ movements and travels and requiring a warrant to search it, even for two hours of data. *See* ECF No. 104 at 12; Def. Ex. 2 at 16. Furthermore, once the government seizes the “anonymized” Device IDs in steps one and two, it could simply obtain the subscriber information for any Device ID by issuing a subpoena to Google. In Illinois, Judge Fuentes recently denied a geofence warrant application in which the government promised to forego step three, 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.” *See Fuentes Opinion*, 481 F. Supp. 3d at 754.

Focusing only on the length of the search, however, is to ignore the unprecedented breadth of a geofence warrant, setting it apart from the individualized searches in *Jones* and *Carpenter* (and most every other case). This was not a search of one person’s data over the course of one or two hours; it was a search of “numerous tens of millions” of people, all at once.

The government argues that this defining feature of a geofence warrant is irrelevant to the Fourth Amendment analysis, *see* ECF No. 109 at 8. But as Justice Gorsuch remarked, “On what possible basis could such mass data collection survive the Court’s test while collecting a single person’s data does not?” *Id.* at 2267 (Gorsuch, J., dissenting). The fact that the government is searching millions multiplies the privacy intrusion.

C. Mr. Chatrie Did Not “Voluntarily” Share Location History Data With Google

The government contends that Mr. Chatrie has no expectation of privacy in his Location History records because Location History is an “opt-in” service and he “voluntarily” shared this data with Google. *See* ECF No. 109 at 5; ECF No. 41 at 10–12. But Mr. Chatrie maintains that, as in *Carpenter*, the question is not whether there was an agreement between an individual and a service provider. The question is whether, in a “meaningful sense,” users “voluntarily ‘assume[] the risk’ of turning over a comprehensive dossier of [their] physical movements” to the government. *Carpenter*, 138 S. Ct. at 2220 (quoting *Smith*, 442 U.S. at 745). But based on the facts in this case, it is clear that typical users like Mr. Chatrie would have no idea what Location History is, how it works, or whether they have it enabled on their phones.

An examination of the “opt-in” process reveals that the act of enabling Location History could not have been meaningful or informed, but was perfunctory at best and deceptive at worst.

This is evident on its face from the evidence presented to this Court about how the “consent flow” pop-up screen appears in Google Assistant. *See supra* at 11–13. It is also bolstered by the highly public and highly negative “feedback” that Google received regarding Location History and consent, reflected in changes that Google made to Location History after the facts of this case. And it is further demonstrated by the words of Google’s own engineers, who repeatedly emailed a massive, company-wide discussion group to express their frustration over Google’s lack of clarity with respect to location tracking permissions, and with Location History specifically.

First, consider the “opt-in” process. Google describes it as a complex seven-step process. Def. Ex. 2 at 7–8; Def. Ex. 21 at 2–3. But for Mr. Chatrue, it boiled down to a single pop-up screen in Google Assistant, at midnight, a week after he got the phone. *See supra* at 10.⁶ That screen had one phrase of “descriptive text” about Location History. It in no way indicated that location data would be saved by Google, as opposed to stored locally on the device. It did not begin to convey the fact that it would operate independently of Google Assistant or convey that Google would collect location data constantly, at an average of every two minutes. *See supra* at 5. While additional information was available, users would have had to actively seek it out. Even then, what little else Google said about Location History did not adequately convey how it functioned.

There is a vast chasm between the reality of Google’s Location History data collection and the advisements it actually requires users to read. To begin with, the “descriptive text” for Location History—the only text a user is actually required to read—is not only inadequate but outright confusing. One iteration tells users that it “Creates a private map of where you go with your signed in devices.” *See supra* at 11. A later version says that Location History “Saves where you go with

⁶ Previously, counsel for Mr. Chatrue suspected that the opt-in to Location History occurred either during the initial setup of the device, or upon opening an application like Google Maps. *See* ECF No. 104 at 15–18; Def. Ex. 21 at 2–3; Def. Ex. 2 at 12.

your devices.” *See id.* In either event, a user might reasonably infer that this “private map” or saved data would be saved only on their device, not with Google. Tr. 301, 346 (descriptive text does not make a “distinction” as to whether location information is saved on-device or on Google servers).⁷ In fact, that is how certain personalized features work on Apple Maps, available on Apple iPhones. *See Privacy*, Apple, <https://www.apple.com/privacy/features/> (last visited Apr. 23, 2021) (describing how certain personalized features on Apple Maps “are created using data on your device” to “help[] minimize the amount of data sent to Apple servers”). Unless a user actively clicked the small “expansion arrow” on the other side of the screen from “Location History,” there would be no indication that the data is saved in the cloud on Google’s servers. *See supra* at 13; Tr. 110, 330. Google does not maintain records on who or how many people click the expansion arrow, Tr. 365, and there is no indication that Mr. Chatric did here.

Additional language appeared at the bottom of the screen, away from the Location History “descriptive text,” and in lighter font. There are two potential versions of this language, *see supra* at 11-12, but both state that this “data may be saved” and that “You can see your data, delete it and change your settings at account.google.com.” *Id.* Neither version mentions Location History or location data, nor gives any indication of what it is, let alone that the phone will begin to transmit its location to Google every two minutes in perpetuity. It does not mention the Location History “Timeline,” the virtual “journal” that is supposedly the reason users enable Location History.

Google did not require users to view any other text before enabling Location History, Tr. 110, 330, and, the other optional information it provided did not put users on notice about the true nature of the Sensorvault database. The expanded “consent copy,” for instance—viewable only if a user clicked on the expansion arrow near “Location History”—explained that Google would

⁷ Mr. McGriff testified that Google does not ascribe any significant difference in meaning between these two variations, *see* Tr. 301, raising the question of why the change occurred at all. *See infra* at 35.

obtain location data from users' devices, but it contained no warning about the frequency or sheer quantity of data collected. Tr. 347–48; *see* Def. Ex. 7 at 3. In this case alone, the Location History records revealed that Google collected location information every six minutes, twenty-four hours a day, seven days a week. Tr. 122, 436. On average, Google collects Location History data as often as every two minutes. *See supra* at 5. Nothing in the “descriptive text” or the “consent copy” explains the volume of information that Google plans to collect.

Additionally, nothing explains that Location History will operate independently, regardless of whether the phone is in use. The government contends that Mr. Chatrie’s “voluntary disclosure of location information to Google is evident from the nature of the location-based services (like mapping) that Google provided him.” ECF No. 109 at 9–10. But this argument falls flat. Once enabled, Location History silently collects data in the background, regardless of what a user is or is not doing on the device. This is in stark contrast to the facts in *Smith v. Maryland*, where phone users often had to interact with telephone operators using switching equipment to complete calls. *See* 442 U.S. 735, 742 (1979). Here, Mr. Chatrie could have enabled Location History by accident, just after midnight, following a long-press of the home button, after a week of annoying prompts, on a pop-up screen for Google Assistant, and bundled with other choices. If he did this, there would still be no further indication that Location History was running. Even if Mr. Chatrie never again engaged with Google’s “location-based services,” or any other Google service, Location History would be enabled and tracking his location at all times, even while he slept. *See supra* at 5; Tr. 122 (“[T]here were no periods of data not being collected.”).

Google’s Privacy Policy has little if any bearing on an individual’s Fourth Amendment expectations of privacy. *See United States v. Irving*, 347 F. Supp. 3d 615, 621 (D. Kan. 2018) (rejecting government’s argument that defendant had no expectation of privacy in his Facebook

account information where he agreed to Facebook’s terms that “generally inform[ed] users that Facebook collects a user’s content and information.”); *see also Smith*, 442 U.S. at 745 (declining to “make a crazy quilt of the Fourth Amendment” based on phone company policies). It is of no assistance to the government here. First, there is no link in the “consent flow” at issue to Google’s Privacy Policy, *see* Def. Ex. 7 at 1–4, a factor that courts weigh heavily when evaluating reasonable notice. *See* ECF No. 104 at 18–20; *Melo v. Zumper*, No. 3:19-cv-621 (DJN), 2020 WL 465033, at *9 (E.D. Va. Jan. 28, 2020). Second, the text of the policy was not any more illuminating than the pop-up screen. *See supra* at 19. At the time Location History was enabled on Mr. Chatrie’s phone, the policy had just two lines that mention Location History. *See* Tr. 294. One line cast Location History only as a way to “save and manage location information in your account.” Def. Ex. 43 at 7. The other line, in passing, states that “you can turn on Location History if you want traffic predictions for your daily commute.” *Id.* at 8. These brief mentions sow only further confusion.

The government likes to point out that it was still possible to disable Location History and delete saved records. *See* Tr. 160, 416. But this assumes that Mr. Chatrie was both fully aware of the collection taking place as well as knowledgeable about how to control or stop it, and the government has offered no evidence to indicate that this was the case. On the contrary, while it is arguably too easy to enable Location History, it would have been counterintuitive and difficult for Mr. Chatrie to disable and delete, assuming he even knew about its existence.

Deleting the application from which Location History was enabled, for example, would not turn off Location History. Tr. 124; *see* Tr. 361–62. Likewise, deleting Location History data would not turn off Location History. Tr. 361. Indeed, it is telling that, once enabled, Location History can never be turned “off,” only “paused.” *See supra* at 14. And it is only possible to “pause” Location History by navigating through complicated settings menus and disregarding a

pop-up warning from Google that doing so will “limit[] functionality” on the device. *See id.* Similarly, while pressing “pause” means that no future data will be recorded, it does not delete any past data collected. *See supra* at 15. Even disabling Google Assistant, the app used to enable Location History here, would have no effect on either stored data or future collection. *See id.* In short, for a user to completely remove their data from the Sensorvault database, they would need to follow a specific settings permutation: a two-step process of both deleting all past Location History data and “pausing” Location History. Nowhere, not in either version of the “consent flow” or the Privacy Policy, did Google inform users of the need to take both steps or how to do them.⁸

This is not surprising, however, because Google has a clear financial incentive in increasing the number of users with Location History enabled. *See supra* at 8–9; Tr. 435–36. Google is not disinterested or neutral when presenting users with options. Rather, Google is invested in having users whose data can be used to sell lucrative advertisements that calculate rate of return by measuring “store visits.” *Id.*; Tr.196–97, 301. Indeed, advertising is the main “product” that drives Google’s revenue. *See* Tr. 560; *see also* Gov’t Ex. 1 at 40 (showing that advertising comprised 85% of Google’s revenue in 2018). In this light, the “consent flow” fits the pattern perfectly and bears a striking resemblance to lobster traps: easy to get in, hard to get out.

At the same time, Google has never been immune to public criticism, lawsuits, or regulatory action. On the contrary, Google has repeatedly received terrible headlines, civil complaints, and government inquiries over its location tracking practices, putting the company

⁸ Instead, media outlets have taken on this task, publishing “how-to” articles on disabling Location History and other forms of Google location tracking. *See, e.g.,* Dave Johnson, *How to Stop Google from Tracking Your Android’s Location*, Business Insider (Nov. 25, 2020, 9:16 AM), <https://www.businessinsider.com/how-to-stop-google-tracking-android>; Barbara Krasnoff, *Android 101: How to Stop Location Tracking*, Verge (Aug. 25, 2020, 3:04 PM), <https://www.theverge.com/21401280/android-101-location-tracking-history-stop-how-to>; Chandra Steele & Jason Cohen, *How to Get Google to Quit Tracking You*, PC Mag (Feb. 11, 2020), <https://www.pcmag.com/how-to/how-to-get-google-to-quit-tracking-you>; Todd Haselton, *Google Maps Tracks Everywhere You Go. Here’s How to Automatically Delete What It Stores*, CNBC (Dec. 7, 2019, 9:15 AM), <https://www.cnbc.com/2019/12/07/how-to-stop-google-maps-from-tracking-your-location.html>.

squarely on notice that its practices surrounding user consent were unacceptable and incompatible with user expectations of privacy. And in response, Google acted. *See* Def. Ex. 46; Def. Ex. 47; Tr. 260, 317, 383. Although, Google notes that it is “always looking for ways to further improve,” Tr. 300, the changes Google made to Location History in this context are telling.

Since at least 2017, Google has been on notice that people found it difficult to understand how Google collects location data and what their options are. Mr. McGriff, in charge of Location History for Google since 2016, *see* Tr. 192, was acutely aware of a 2017 article in the online magazine *Quartz* as well as a 2018 article by the *Associated Press* (“AP”), both involving Location History. Tr. 220, 223–24. Both articles described Location History with alarm and were highly negative. Tr. 221–23, 225–26. The AP article made such an impression that Google prepared a report tracking how much follow-up coverage mentioned the “lack of user consent/creepy factor.” Tr. 228. It also became the subject of a Monday-morning “Oh Shit” meeting for the Location History team. Tr. 248. In his defense, Mr. McGriff noted that the Google Location History team has such a meeting every Monday, which is understandable. *See id.*

It is understandable because those articles were just the beginning of the public “feedback” that Google received regarding Location History and Google’s location tracking practices. *See* Tr. 218–19. Google not only became aware of the *Quartz* article, for example, but also the subsequent letter that the United States Senate to the Federal Trade Commission, urging the agency to investigate “deceptive acts and practices” associated with Location History. *See* Tr. 236; Def. Ex. 53 at 4 (“Most consumers do not understand the level, granularity, and reach of Google's data collection, and there are serious questions about whether they have provided their informed consent and maintain a reasonable ability to avoid participating in this collection.”). And following the 2018 AP article, Google became aware of a class action lawsuit over its location tracking

practices. *See* Tr. 236–37. Google was also aware of a *New York Times* article revealing Google’s role in geofence warrants, which in turn prompted another letter critical from Congress (this time addressed to Google’s CEO). *See* Tr. 314.

Most recently, the Attorney General of Arizona filed lawsuit against Google, leading to the public release of hundreds of pages of internal emails concerning Location History. *See* Tr. 240. After publication of the AP and *Times* articles, Google employees took to company-wide email groups to express their confusion over Google’s location settings. *See, e.g.*, Tr. 241–43, 246, 252–53, 255–56; Def. Ex. 30; Def. Ex. 31 (“Add me to the list of Googlers who didn’t understand how this worked and was surprised when I read the article.”); Def. Ex. 36 (explaining that Google was “trying to rein in the overall mess that we have with regards to data collection, consent, and storage”); Tr. 310–12; Def. Ex. 37 (“I’d want to know which of these options (some? all? none?) enter me into the wrongful-arrest lottery. And I’d want that to be very clear to even the least technical people.”).

Regardless of the truth of these criticisms, there is no question that Google heard, discussed, internalized, and then acted on them. Public reaction was strong enough that Google made reforms to Location History, crediting this “feedback” for spurring the “auto-delete” option for Location History data. *See supra* at 15; Tr. 317; Def. Ex. 46. Google also began to send out monthly emails to users who had enabled Location History, after recognizing that users might not “understand the granularity of the data that’s being collected or simply just wouldn’t know . . . what exactly [Google was] collecting and how that information was being processed.” Tr. 359–60. Google has no record of sending such emails to Mr. Chatrie and concedes that it may not have

sent him those emails.⁹ Tr. 328; Def. Ex. 23 at 8–9. Nonetheless, these changes demonstrate that even Google knew that the “opt-in” for Location History was confusing and potentially deceptive.

D. The Third-Party Doctrine Should Not Apply Even If Mr. Chatrle Intentionally Enabled Location History.

Timothy Carpenter signed a contract with his cell phone service provider. *Carpenter*, 138 S. Ct. at 2225 (Kennedy, J., dissenting). He did not allege that he was tricked or coerced into it. And yet, the Supreme Court still found that he was not “voluntarily” conveying his location data to the service provider, even though everyone was aware that that is how cell phones work. *Id.* at 2220 (“Cell phone location information is not truly ‘shared’ as one normally understands the term.”). Rather than “mechanically” applying the third-party doctrine, the Court looked at the context—whether the “choice” to hand over the data truly outweighed the privacy intrusions given the realities of the digital age. *Id.* at 2219–20; *see also* ECF No. 29 at 9–11.

The Court’s contextual concern exists here in abundance. “[M]echanically” applying the third-party doctrine here would divest, at a minimum, tens of millions of people of their Fourth Amendment rights merely for participating in normal everyday life. *See* Tr. 205. Google Location History may not be a pillar of digital society, but there are still “numerous tens of millions” of people who use it, wittingly or not. The *Carpenter* Court remarked on the pervasiveness of cell phones in the United States. 138 S. Ct. at 2220 (citing *Riley v. California*, 134 S. Ct. 2473, 2484 (2013)). At issue here is one-third of all Google users. It would be nonsensical to deem this data unworthy of Fourth Amendment protection unless everyone is using it, yet that is the line the government seeks to draw. Moreover, there is nothing in the government’s reasoning that would limit the use of geofences to Location History data.

⁹ Google also describes a “warm welcome” notification appearing in the Google Maps application, Tr. 355, but there is no indication that there was such a notification in Google Assistant, or that Mr. Chatrle received one.

Under the government’s theory, people do not have an expectation of privacy in any data stored with a third-party or service provider, other than long-term CSLI. Thus, there would be nothing separating a search of Location History data from a search of Gmail users for messages mentioning a robbery of the Call Federal Credit Union. This is no mere hypothetical. Law enforcement has already forced Google to conduct reverse “keyword” searches, disclosing everyone who searched for a particular term or address.¹⁰

Lastly, Mr. Chatrie respectfully persists in his property-based arguments here. *See* ECF No. 29 at 14–16; ECF No. 48 at 8–10; ECF No. 109 at 20–21. Ownership is inherent in the language Google uses to describe Location History, whether telling users they are creating a “private map” of their whereabouts or calling it “your data” to delete or manage as users see fit. *See supra* at 11. Under either a property-based theory or the reasonable expectation of privacy framework set forth in *Katz*, obtaining Mr. Chatrie’s Google Location History records was a Fourth Amendment search.

II. The Geofence Warrant Was an Unconstitutional General Warrant

As Mr. Chatrie has argued from the beginning, geofence warrants are inherently unconstitutional. *See* ECF No. 29 at 19–21; ECF No. 104 at 21. They are digital versions of the “dragnet” searches that Fourth Amendment was intended to prohibit. *See* ECF No. 104 at 21–24; ECF No. 29 at 16–23. The Supreme Court has never sanctioned the search of “numerous tens of millions” of people, in any context. *See* Def. Ex. 21 at 4. Additional facts from the March hearing confirm that the warrant in this case was uniquely overbroad and so lacking in particularity that it is the digital equivalent of an impermissible general warrant.

¹⁰ Alfred Ng, *Google Is Giving Data to Police Based on Search Keywords, Court Docs Show*, CNET (Oct. 8, 2020 1:21 PM), <https://www.cnet.com/news/google-is-giving-data-to-police-based-on-search-keywords-court-docs-show/>.

E. Overbreadth

Overbreadth concerns probable cause, which is defined as “a fair probability” that contraband or evidence of a crime will be found in a particular place. *Illinois v. Gates*, 462 U.S. 213, 238 (1983). A warrant is overbroad if the government lacks probable cause for the things to be searched or seized. *United States v. Hurwitz*, 459 F.3d 463, 473 (4th Cir. 2006). Here, the government did not have probable cause to search “numerous tens of millions” of Google accounts. It did not have probable cause to search 19 users, either, and it did not have probable cause to search nine or three. The government did not have probable cause to search even one Google account, because investigators admittedly had no suspects. Tr. 487, 637. No matter how the government seeks to dress it up in steps or stages, the complete absence of probable cause means that the warrant is fatally overbroad from beginning to end.

Step one was a dragnet, conducted by Google at the government’s direction. The government made Google search through every user account with Location History enabled to identify any people within 150 meters of the Call Federal Credit Union during a 1-hour window. According to Google, this required searching “numerous tens of millions” of accounts—reviewing the contents of each one to determine if it met the government’s criteria. Tr. 29, 52–53, 205; *see* Tr. 575. In other words, the government compelled Google to access “numerous tens of millions” of accounts and apply a filter of the government’s peculiar design—a digital dragnet.

The warrant application provided no case-specific facts that the robber was a Google user or had Location history enabled at the time in question.¹¹ All the government offered was that an unknown bank robber had a cell phone and that Google tracks a lot of people’s cell phones. ECF

¹¹ Despite “tens of millions” being an exceedingly large number, it accounts for only one-third of Google’s active users. In other words, even if every cell phone user was signed into a Google account, there would only be a one in three chance of the suspect having LH enabled.

No. 109 at 14. The government contends that this is a “substantial basis” for probable cause, *id.*, but if that is true, then the government could get a geofence warrant in any investigation, simply by reciting the facts of the crime and some statistics about Google. As Mr. Chatrue has consistently argued, such broad conjecture about the popularity of Google or cell phones generally does not amount to probable cause. *See* ECF No. 29 at 23; ECF No. 48 at 19. Probable cause must be based on individualized facts, not group probabilities. *See Ybarra v. Illinois*, 444 U.S. 85, 91 (1979). In *Illinois*, Judge Fuentes denied the government’s application for a geofence warrant on these grounds, noting that it “resembles an argument that probable cause exists because those users were found in the place ... [where] the offense happened,” an argument the Supreme Court squarely rejected in *Ybarra*. *See* Fuentes Opinion, 481 F. Supp. 3d at 754.

Had the government provided a nexus between the robber and Location History, then there would have been no need to go fishing in Google’s ocean of data. The government could have simply requested the Location History data for the suspect account, as it typically does. But, the government did not seek to search a particular account; it sought to search *all* accounts. That is the definition of a general warrant. *See Warden v. Hayden*, 387 U.S. 294, 313 (1967) (describing the “practice of the Star Chamber empowering a person ‘to search in all places, where books were printing, in order to see if the printer had a licence; and if upon such search he found any books which he suspected to be libellous against the church or state, he was to seize them, and carry them before the proper magistrate.’”).

The fact that the government’s dragnet ensnared 19 people does not diminish the scope of the initial search conducted at their behest. The Fourth Amendment does not distinguish between Google and the government when it comes to conducting this initial search of millions. This case does not involve a “private search.” Google did not decide on its own to search for users near the

bank, and Google never provides such information to advertisers. *See supra* at 9; Tr. 432–33. Likewise, the data produced was not an existing “business record.” Google did not possess a list of people near the bank until the government required them to create one. Tr. 433. In short, Google had no independent motivation to conduct this geofence search, and Google would not have done so without a warrant. *Id.* The entire search, including the “numerous tens of millions” in step one, was conducted at the government’s direction.

The government contends that this was just like a “tower dump”—another type of exceedingly broad search, the constitutionality of which is in doubt following the Supreme Court’s decision in *Carpenter*. A tower dump requires cell phone service providers to produce the records of every device connected to a particular cell tower or towers during a particular time. *See* Tr. 49–50; Def. Ex. 2 at 14. Any similarity to geofence warrants, however, is merely superficial. Significantly, the number of people searched in a geofence warrant is far larger—by at least four orders of magnitude—than the number of people searched in a typical tower dump. *See* Tr. 53 (the number of people searched in a tower dump “wouldn’t be close to” the number of people searched here); *see also* ECF No. 104 at 22 (surveying reported tower dump cases and finding that they tend to impact hundreds or thousands of people at most). Even the government’s own hypothetical tower dump would have involved a search of roughly 3,000 people, Tr. 55, which is just a tiny fraction of the “numerous tens of millions” searched here. And more importantly, it is a long way off from a “normal Location History request for a specific account when they name the account because we know who we’re looking for.” Tr. at 53.

A tower dump is more limited than a geofence, relatively speaking, because cellular service providers organize, or “index” data based on location, *i.e.*, the cell towers in their networks. Unlike Google, they keep information about the use of each tower for internal business purposes, like

identifying towers that become overloaded and determining where to put up more. As a result, they are able to provide information about particular towers without searching the phone records of every customer. Google, on the other hand, indexes Sensorvault by Google account and has no way of searching by location. *See* Tr. 431–32, 572–73. The government responds that they cannot be responsible for the way Google chooses to structure its database and suggests that Google could “create an additional Location History database indexed by location” to make it easier to execute geofence warrants. ECF No. 109 at 17. But Google does not operate cell towers and has no business need to index user data in this way.

Furthermore, the warrant would still be overbroad even if it were somehow possible to restrict the initial search to devices within the geofence. The government argues that the warrant was “limited based on location, dates, and times,” but the location at issue is anything but narrowly tailored. It encompasses not only the bank and parking lot, but the entire church nearby, with an effective range that included major streets, a hotel, a restaurant, other businesses, and two apartment complexes. *See supra* at 17-18. Judge Weisman recently reached this conclusion as well in denying the government’s application for a geofence warrant in Illinois. *See* Weisman Opinion at *5 (“[T]he geographic scope of this request in a congested urban area encompassing individuals’ residences, businesses, and healthcare providers is not ‘narrowly tailored’ when the vast majority of cellular telephones likely to be identified in this geofence will have nothing whatsoever to do with the offenses under investigation.”). Furthermore, the government would not have had probable cause to search all 19 people who happened to be in the area. As Judge Fuentes reasoned, that data might “*include* evidence of the crime, but it will include other information as well: The location information of persons not involved in the crime.” Fuentes Opinion, 481 F. Supp. 3d at 751. To justify such an “all persons” warrant, the government would have needed probable cause

that all 19 people were involved in the bank robbery. *See Owens ex rel. Owens v. Lott*, 372 F.3d 267, 276 (4th Cir. 2004) (“[A]n ‘all persons’ warrant can pass constitutional muster if the affidavit and information provided to the magistrate [judge] supply enough detailed information to establish probable cause to believe that all persons on the premises at the time of the search are involved in the criminal activity.”). That would have been impossible to do, of course, because the government would have had no way of knowing, *ex ante*, that there would be 19 people in the geofence.

The fact of the matter remains, however, that the step one search did not just involve 19 people, but “numerous tens of millions,” none of which the government had probable cause to search. Probable cause was still absent in steps two and three, when the government seized even more Location History data from nine accounts as well as subscriber information for three of them. *See supra* at 18-19. While the government may have learned new information from the step one data it seized, the warrant application did not change and the government did not seek additional court authorization. The government lacked probable cause to search anyone’s Location History, whether three, nine, nineteen, or millions. The warrant was therefore overbroad from start to finish.

F. Particularity

Particularity concerns officer discretion. Warrants must particularity describe both the place to be searched and the items to be seized in order to limit officer discretion and prevent the “exploratory rummaging” that the Framers abhorred. *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971); *see also United States v. Williams*, 592 F.3d 511, 519 (4th Cir. 2010). The particularity requirement takes on special importance where, as here, a search implicates First Amendment concerns. *See* ECF No. 104 at 24; ECF No. 29 at 13, 22; ECF No. 48 at 3 n.3. In this case, the place to be searched is the millions of accounts stored on Google’s servers. The items to be seized are not specified, but instead described as the product of a three-step process that explicitly requires

the government to use its discretion. In reality, the warrant left the entire process up to Google and the government to work out internally.

The basic contours of the warrant were the product of repeated engagement between the FBI and Google. *See supra* at 4. Google decided to search Location History data, as opposed to Web & App Activity or Google Location Services data. *See id.*; Tr. 212; Def. Ex. 21 at 8. And Google picked a method of calculating which devices were inside the geofence that generated a high number of false positives—people swept up in the dragnet who were never there at all. *See supra* at 16-17. Google had to do all of this because the warrant did not specify one way or another. The issue is not whether Google should have searched other databases, or taken the Display Radius into account in its search, or whether these decisions were “correct.” *See* ECF No. 109 at 18. The issue is that Google is making these decisions instead of a judge. *See Groh v. Ramirez*, 540 U.S. 551, 561 (2004). And here, these decisions had measurable consequences: At least one and as many as five of the 19 users identified in step one were likely never within the geofence, with one device that could have been more than 200 meters outside of it. *See* Tr. 42, 64, 587; ECF No. 104 at 8.

Far more troubling is the amount of discretion that the warrant envisioned for the government at steps two and three. At each step, it was up to the government to “narrow” the list of devices and determine which users will be subject to further scrutiny. Def. Ex. 1 at 4–5. Thus, in step two, the government was to decide, in some unspecified manner, which devices they would receive “contextual” data for, *i.e.*, two hours of Location History data without geographic limitation. *Id.* at 4. And in step three, the warrant left it up to the government to pick the accounts for which Google would provide full subscriber information. *Id.* at 5. This is precisely the kind of officer discretion that the particularity requirement was designed to prevent. *See* Fuentes Opinion,

481 F. Supp. 3d at 754 (finding a geofence warrant lacked particularity because it “puts no limit on the government’s discretion to select the device IDs from which it may then derive identifying subscriber information”); Weisman Opinion, 2020 WL 5491763, at *6 (“[T]his multi-step process simply fails to curtail or define the agents’ discretion in any meaningful way”).

Even this process, however, involved additional uncertainty and negotiation over what data the government could seize. After step one, the government repeatedly emailed and called Google to demand step-two “contextual” data, as well as step-three subscriber information on all 19 devices identified in step one. *See supra* at 18-19. It was only because Google refused that the government was unsuccessful, acquiesced, and eventually requested additional data on only nine users. *Id.* The problem is that the Fourth Amendment requires courts, not detectives or companies, to decide what the government can search and seize. Here, the warrant allowed Google and Det. Hylton to decide which accounts to search and “de-anonymize,” and Det. Hylton demonstrated why the Fourth Amendment does not trust law enforcement to make that decision.

Step three similarly imbued the government with the sole discretion to decide which people would have their full subscriber information disclosed by Google. The warrant did not identify any of them, or provide any objective criteria by which to identify them. *See Weisman Opinion*, 2020 WL 5491763 at *6 (“For example, the warrant does not limit agents to only seeking identifying information as to the ‘five phones located closest to the center point of the geofence,’ or some similar objective measure of particularity.”). Once again, the decision belonged to the government, not a court. And once again, the government used this discretion to seek additional information about one person who was likely never inside the geofence at all, something that should have been apparent from the step-two data. *See Tr.* 65–66; ECF No. 104 at 27.

At each step, the warrant allowed Google and the government to be the arbiters of what was reasonable to search and seize. No objective observer could look at the warrant and ascertain which accounts the government had authority to “de-anonymize” or obtain “contextual” about. The warrant therefore lacked particularity and violated the Fourth Amendment.

III. The Good Faith Exception Does Not Apply

The Fourth Amendment’s most fundamental restraint is the warrant requirement. In *United States v. Leon*, 468 U.S. 897, 919 (1984), the Supreme Court qualified that restraint where a warrant is based on “objectively reasonable law enforcement activity.” But, *Leon* “good faith” offers no qualifications in four circumstances: (1) where a warrant is based on knowing or recklessly false statements, *id.* at 914 (citing *Franks v. Delaware*, 438 U.S. 154 (1978)); (2) where the judge acted merely as a rubber stamp for the police, *id.* (citing *Illinois v. Gates*, 462 U.S. 213 (1983)); (3) where a warrant affidavit lacks a substantial basis to determine probable cause, *id.* at 915 (citing *Gates*); and (4) where no officer could reasonably presume the warrant was valid, *id.* at 923.

The Supreme Court did not intend for the good faith exception to diminish the power and force of the Fourth Amendment. *Id.* at 924. Rather, the Supreme Court tethered the exclusionary rule to the primary tenets of the Fourth Amendment: particularity, probable cause, and a neutral magistrate who is “not [an] adjunct[] to the law enforcement team.” *Id.* at 917, 923. As Mr. Chatrue has argued, *see* ECF Nos. 48 at 17-20 and 104 at 28-30, the *Leon* good faith exception to the exclusionary rule does not apply to evidence obtained from a warrant that was *void ab initio*. As set forth above and in the earlier briefing, this geofence warrant is void from its inception and is no warrant at all. *See United States v. Krueger*, 809 F.3d 1109, 1123-24 (10th Cir. 2015) (Gorsuch, J., concurring); *see also Groh v. Ramirez*, 540 U.S. 551, 558 (2004) (“[T]he warrant was so

obviously deficient that we must regard the search as ‘warrantless’ within the meaning of our case law.”). But, even if the Court determines that *Leon* applies here, three of the firm boundaries to the good faith rule that *Leon* recognized clearly apply.

First, the magistrate issuing the geofence warrant “abandoned his judicial role” and acted as a rubber stamp here. On June 14, 2019, the police presented the geofence warrant to a magistrate who had served for less than a year, had finished his probationary period a handful of months before, and had only a bachelor’s degree from an unlicensed school. *See* ECF Nos. 135-2 at 22 and 156. There is no evidence in this case that the magistrate had any training on geofence warrants or had even seen a geofence warrant before June 14, 2019. On that date, Det. Hylton walked into the magistrate’s office where other magistrates were present. Tr. 638. He handed the warrant application to Magistrate Bishop. *Id.* The magistrate looked over the application privately for maybe fifteen or thirty minutes and signed the warrant without asking a single question or making a single change to the warrant. *Id.* at 638-39. While perhaps that type of review may suffice for a more ordinary warrant, a warrant that necessarily requires governmental invasion into the intimate details of many innocent persons’ private lives should generate more distress.

The magistrate’s utter lack of concern regarding the obvious flaws in the warrant constituted a complete abandonment of his role as the neutral arbiter between individual privacy and government overreach. The magistrate apparently had no qualms with signing a warrant that—contrary to the Fourth Amendment’s patent particularity requirement—allowed the police to search a haystack composed of numerous tens of millions of people’s intimate, private data to see if a needle might turn up. The magistrate was further unconcerned that the warrant granted immense discretion to the executing officers and Google to decide what Google data to search. The affidavit in this case did not describe objectively reasonable law enforcement activity. Rather,

it described a general warrant that the framers created the Fourth Amendment to preclude. The particularity requirement “makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.” *Stanford v. Texas*, 379 U.S. 476, 512 (1965); *see also United States v. Wilhelm*, 80 F.3d 116, 121-23 (4th Cir. 1996) (finding that magistrate acted as rubber stamp by abandoning scrutiny of basic tenet of Fourth Amendment); *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); *United States v. Winn*, 79 F. Supp. 3d 904, 924 (S. D. Ill. 2015) (finding 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”).

Second, the good faith exception should not apply because the geofence warrant was “so lacking in indicia of probable cause” to search for Mr. Chatrie’s location data that it was entirely unreasonable for any objective officer—i.e., one who had even a rudimentary understanding of the Fourth Amendment’s particularity and breadth requirements—to rely on. *See Leon*, 468 U.S. at 923. Here, police knew a robbery suspect was carrying what appeared to be a cell phone. Tr. 608. They had no idea what company made the cell phone, what carrier provided service for the phone, what operating system the phone used, or what applications and permissions were installed and actively gathering data on the phone. Rather than trying to do some detective work like track down the owner of the car the suspect was seen in and compare that information to cell phone numbers that had connected with a nearby cell phone tower, Tr. 578-79, the police decided to get permission to rummage through numerous tens of millions of people’s location data simply because the robbery suspect had what appeared to be a cell phone in his hand.

Police must demonstrate a fair probability that the evidence the police seek will be where they are searching. *See United States v. Doyle*, 650 F.3d 460, 472 (2011) (rejecting good-faith exception where warrant application contained “remarkably scant evidence . . . to support a belief that [the defendant] *in fact* possessed child pornography”); *see also United States v. Church*, 2016 WL 6123235, at *6-7 (E.D. Va. Oct. 18, 2016) (observing that good-faith exception inappropriate where no evidence to connect suspect’s house to the crime under investigation); *United States v. Shanklin*, 2013 WL 6019216, at *9 (E.D. Va. Nov. 13, 2013) (“A reasonable police officer would be unable to infer through normal inferences that electronic devices owned by child abusers in general or the Defendant specifically contain evidence related to the criminal activity being investigated”). That did not happen here. Rather, what happened here was the police obtained a warrant based on conjecture that Google had location data for the cell phone the robbery suspect appeared to be carrying. Obtaining warrants based on conjecture is certainly not “objectively reasonable law enforcement activity.” *See Leon*, 468 U.S. at 919.

Third, the good faith exception should not apply because the geofence warrant was “facially deficient” and no objective officer could reasonably presume it was valid. *See Leon*, 468 U.S. at 923. As an initial matter and as set forth above, “it is obvious that a general warrant authorizing the seizure of ‘evidence’ without [complying with the particularity requirement] is void under the Fourth Amendment” and “is so unconstitutionally broad that no reasonably well-trained police officer could believe otherwise.” *United States v. George*, 975 F.2d 72, 77 (2d Cir. 1992); *see also United States v. Leary*, 846 F.2d 592, 607-09 (10th Cir. 1988) (“reasonably well-trained officer should know that a warrant must provide guidelines for determining what evidence may be seized,” and collecting like cases from the First, Eighth, and Ninth Circuits).

Additionally, the extraordinary discretion this warrant purported to authorize renders the warrant facially deficient. Law enforcement agencies and Google worked hand-in-hand in to develop the three-step process outlined above for requesting and responding to geofence warrants. Tr. 455-57, 476. Google, sometimes with police help, gets to decide how big of a geographical area is too big. Tr. 455-58, 461. Google, sometimes with police help, gets to decide if a range of time is too long. Tr. 458-59, 462-64. Google also gets to decide if it does not want to comply with a geofence warrant because it is too sensitive, say for political reasons. Tr. 459-60. Google gets to decide any time limits it wants to apply in between the various steps in the three-step process. Tr. 464-66, 469-70. Google gets to decide if the police have attempted to narrow the information to be seized between the various stages. Tr. 467-69, 471-72. In sum, the three-step process that law enforcement agencies and Google created for Google to respond to geofence warrants entrusts essentially unfettered discretion with the police and Google to execute the warrant.

While Det. Hylton had no training in understanding or applying for geofence warrants, Tr. 627-28, no objective officer could have reasonably believed that a warrant that gave Google and the police unprecedented discretion in executing the warrant was valid. *See George*, 975 F.2d at 76 (“Absent some limitation curtailing the officers’ discretion when executing the warrant, the safeguard of having a magistrate determine the scope of the search is lost.”); *Leary*, 846 F.2d at 609 (“A warrant that directs an officer to seize records ‘relating to’ violations of the federal export laws offers no such guidelines. The officers were left to their own discretion.”); *see also Winn*, 79 F. Supp. 3d at 924 (“it was not objectively reasonable for the[police] to think that a warrant was valid when it gave them unbridled discretion to search for and seize whatever they wished”). Obtaining warrants authorizing nearly unfettered discretion is certainly not “objectively reasonable law enforcement activity.” *See Leon*, 468 U.S. at 919.

For any of these reasons, the Court cannot find that the good-faith exception applies to evidence that the government obtained from the geofence warrant and the fruits flowing therefrom. While Mr. Chatrie has not and is not raising a *Franks* claim, the misleading information in the warrant application and material information the police omitted from the warrant certainly reinforces the conclusion that the Court should not apply the good-faith exception in this case. *See Leary*, 846 F.2d at 609-10 (finding that conduct and circumstances of the search reinforced conclusion that “suppression of the evidence is appropriate to deter government misconduct”). In this case, the government falsely told the magistrate that the Google data in the first two stages was anonymous. We know now that a person can reasonably be identified through a handful of location points. Tr. 62-70; ECF 104 at 12; 1/21/20 Tr. at 83, 87-88, 90-91. The Device ID Google uses to identify a device and account remains the same from warrant to warrant. Tr. 451-54. The police did not inform the magistrate that Google would have to search numerous tens of millions of people’s private location diaries in stage one. The police also did not inform the magistrate that the geofence would almost certainly capture devices outside of the geofence or that the approximate device locations were only 68% accurate. This level of misinformation and omitted information only underscores that the geofence warrant in this case was not “objectively reasonable law enforcement activity.” *See Leon*, 468 U.S. at 919.

CONCLUSION

If ever there were a case to find that the government used a general warrant, then this is it: a dragnet of “numerous tens of millions” paired with unchecked discretion. The warrant was so profoundly overbroad and lacking in particularity that the good faith doctrine should not apply. Mr. Chatrie therefore asks this Court to suppress all evidence obtained from geofence warrant and all of its poisonous fruits.

Respectfully submitted,
OKELLO T. CHATRIE

By: /s/
Michael W. Price
NY Bar No. 4771697 (*pro hac vice*)
Counsel for Defendant
National Association of Criminal Defense Lawyers
Fourth Amendment Center
1660 L St. NW, 12th Floor
Washington, D.C. 20036
Ph. (202) 465-7615
Fax (202) 872-8690
mprice@nacdl.org

/s/
Laura Koenig
Va. Bar No. 86840
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0881
Fax (804) 648-5033
laura_koenig@fd.org

/s/
Paul G. Gill
Va. Bar No. 31461
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0870
Fax (804) 648-5033
Paul_gill@fd.org

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Richmond Division

UNITED STATES OF AMERICA)	
)	
v.)	CRIMINAL NO. 3:19-CR-130-MHL
)	
OKELLO T. CHATRIE,)	
)	
Defendant.)	

**GOVERNMENT’S RESPONSE IN OPPOSITION TO
DEFENDANT’S MOTION FOR SUPPRESSION**

When someone robbed the Call Federal Credit Union in Chesterfield, Virginia, Google was a witness. Defendant Okello T. Chatrie had chosen to have Google keep a record of where he went with his cell phone in order for Google to provide him with location-based services. As a result, evidence of the defendant’s presence at the bank robbery was stored in a database that Google accesses freely to provide services to its users and advertisers. A Virginia magistrate determined that there was probable cause to believe that Google possessed evidence of the robbery, and he issued a geofence search warrant.

The warrant authorized disclosure from Google of two hours of location information associated with electronic devices that were, over a one-hour interval, within 150 meters of the site of the bank robbery. Pursuant to the warrant, Google produced location information over a two-hour interval of three subsequently identified and six unidentified individuals, and limited location information over a one-hour interval of ten other unidentified individuals. From this information, investigators identified the defendant and solved the robbery.

In his post-hearing brief, the defendant continues to argue that this evidence should be

suppressed, but this Court should deny the defendant's motion to suppress for three separate and independent reasons. *See* Def.'s Post-Hearing Mot. To Suppress, ECF No. 203, (hereinafter, "Def. Post-Hr'g Suppl. Br."). First, the government did not conduct a search under the Fourth Amendment when it obtained this location information from Google. Second, the geofence warrant complied with the Fourth Amendment, as it was based on probable cause and specified its object with particularity. Third, suppression is inappropriate because investigators relied on the warrant in good faith.

I. STATEMENT OF FACTS

A. The Robbery and the Geofence Warrant

At approximately 4:50 pm on May 20, 2019, a then-unknown male entered the Call Federal Credit Union in Midlothian, Virginia. *See* Geofence Search Warrant, Gov't Ex. 2, at 6 (hereinafter, "Gov't Ex. 2")¹; Motion to Suppress Hearing Transcript, ECF Nos. 101, 102, at 608 (hereinafter, "Suppression Hr'g Tr."). With his right hand, the robber held a cell phone to his face and appeared to be speaking to someone. Gov't Ex. 2 at 6; Suppression Hr'g Tr. 608. He approached a teller and presented a note that read, in part, "I got your family as hostage and I know where you live, If you or your coworker alert the cops or anyone your family and you are going to be hurt. . . . I need at least 100k." Gov't Ex. 2 at 6; Suppression Hr'g Tr. 608-09. After the teller replied that she did not have access to that amount of money, the robber pulled out a silver and black firearm. Gov't Ex. 2 at 6; Suppression Hr'g Tr. 609. After first forcing everyone to the ground at gunpoint, the robber escorted the manager and others to the back of the business where the vault was located. Gov't Ex. 2 at 6; Suppression Hr'g Tr. 608-09. The robber forced the manager to open the safe

¹ Page numbers for Government Exhibit 2 refers to the numbering in red at the bottom of each page. Such numbering is consistent where an exhibit of the United States has red numbering at the bottom.

and place \$195,000 into a bag. Gov't Ex. 2 at 6. The robber then fled towards a church west of the bank. Gov't Ex. 2 at 6; Suppression Hr'g Tr. 609-10.

Federal Bureau of Investigation Task Force Officer ("FBI TFO") Josh Hylton responded to the scene to investigate. Suppression Hr'g Tr. 607. From the fact that the robber had carried a phone, FBI TFO Hylton knew that there was a possibility that the robber might have had a lookout or a driver nearby. Suppression Hr'g Tr. 610.

FBI TFO Hylton also knew that Google could have data that would show the robber was in the area at the time of the robbery. Suppression Hr'g Tr. 610. On three prior occasions, FBI TFO Hylton had obtained geofence warrants directed to Google. Suppression Hr'g Tr. 603. Moreover, he had consulted with prosecutors prior to obtaining the geofence warrants. Suppression Hr'g Tr. 604. One was issued by a United States Magistrate Judge, and two were issued by Virginia state judges. Suppression Hr'g Tr. 603-04. In seeking these warrants, he had never been told that geofence warrants were not legal. Suppression Hr'g Tr. 604-05.

On June 14, 2019, FBI TFO Hylton sought and obtained a geofence warrant from the Chesterfield Circuit Court of Virginia. *See* Gov't Ex. 2. His statement of probable cause began by describing the facts of the robbery, including that prior to the robbery, the robber held a cell phone to his ear and appeared to be speaking with someone. Gov't Ex. 2 at 6. The statement then explained why there was reason to believe that Google would have evidence pertaining to the robbery. Gov't Ex. 2 at 7. Among other facts, the statement disclosed: (1) that as of 2013, 56% of cell phones were smartphones; (2) that "[n]early every" Android phone "has an associated Google account"; (3) that Google "collects and retains location data" from such devices when the account owner enables Google location services; and (4) that Google collects location information from non-Android smartphones if the devices are "registered to a Google account and the user has

location services enabled.” Gov’t Ex. 2 at 7. Magistrate David Bishop issued the geofence warrant upon a finding of probable cause. *See* Gov’t Ex. 2 at 8.

The geofence warrant specified a target geographical area, identified as a circle of radius 150 meters around a specific latitude and longitude point west of the bank, such that the circle covered both the bank and the place where the robber parked. Gov’t Ex. 2 at 5; Suppression Hr’g Tr. 523. It authorized disclosure of location information over a two-hour interval (from 3:50 pm to 5:50 pm) from accounts associated with devices within this target area at some point during a one-hour interval that included the robbery (from 4:20 pm to 5:20 pm). Gov’t Ex. 2 at 4-5. The warrant also authorized disclosure of specified customer identity information associated with these accounts, including user name and email address. Gov’t Ex. 2 at 4-5.

The warrant authorized this disclosure through a three-step process that enabled law enforcement to “narrow down” the information disclosed by Google and thus obtain less than the maximum amount of information covered by the warrant. Gov’t Ex. 2 at 4-5. The warrant directed that in the first step, Google was to disclose anonymized location for devices present in the target area during the hour of the robbery, but not the identity information associated with the devices. Gov’t Ex. 2 at 4. In particular, the warrant directed that Google disclose “a numerical identifier for the account, the type of account, time stamped location coordinates and that data source that this information came from if available.” Gov’t Ex. 2 at 4.

In the second step, law enforcement was to review the anonymized location information produced by Google and identify the accounts of interest, and Google was then to disclose location information for those accounts over the full two-hour interval, both within and outside of the target area, but again without disclosing user identity information. Gov’t Ex. 2 at 4-5. In the third step, law enforcement was to identify accounts that remained of interest, and Google was to disclose

user name and other specified subscriber identity information for those accounts. Gov't Ex. 2 at 5.

Investigators followed this three-step process in executing the warrant. Suppression Hr'g Tr. 533-50. In the first phase, Google provided 209 data points concerning 19 accounts (including 38 points from the defendant's account), all within the 150 meter circle and during the hour of the bank robbery. *See* FBI Cellular Analysis Survey Team, Gov't Ex. 1, at 20, 22 (hereinafter, "FBI CAST Report"); Suppression Hr'g Tr. 534-35; *see also* Sealed PDF of Raw Data, Def. Ex. 3. For each data point, Google produced an account ID, date and time, latitude and longitude coordinate, source of information (wi-fi or GPS), and "map display radius." *See* FBI CAST Report at 17-22. "Map display radius" is a measure of Google's confidence in the accuracy of its location information; Google's aim is to capture roughly 68% of users within the circle defined by its location estimate and the map display radius. Suppression Hr'g Tr. 213-14; *see also* McGriff Decl. dated Mar. 11, 2020 at ¶¶ 24-25 (ECF No. 96-1), Gov't Ex. 3, (hereinafter, "Gov't Ex. 3").

By reviewing the phase 1 data in conjunction with witness interviews and video surveillance tapes, investigators concluded that the defendant's device likely belonged to the robber. Suppression Hr'g Tr. 549-50.

In the second phase, FBI TFO Hylton initially asked Google for data regarding all 19 accounts, but Google was nonresponsive. Suppression Hr'g Tr. 622; Email Correspondence between FBI TFO Hylton and Google, Gov't Ex. 4 at 4. Concerned about the dangerousness of the situation, FBI TFO Hylton called Google, and he ultimately narrowed the second-stage production to nine accounts. Suppression Hr'g Tr. 622, 642; Gov't Ex. 4 at 9. Google produced two hours of location data for each of these accounts—a total of 680 data points, including 94 data points for the defendant's account with a device ID ending in 5659. FBI CAST Report at 26.

In the third phase, FBI TFO Hylton directed Google to disclose subscriber information for three accounts, including the account of the defendant. Suppression Hr’g Tr. 543. This information included the defendant’s email address. Suppression Hr’g Tr. 544.

Location History information is the only information stored by Google that can be responsive to a geofence warrant because it is the only information stored by Google that is associated with specific users and sufficiently granular to be responsive. *See* Gov’t Ex. 3 at ¶ 20; Suppression Hr’g Tr. 378-79. To identify responsive information, Google runs a computation against all stored Location History coordinates to determine which ones match the geofence parameters. *See* Gov’t Ex. 3 at ¶ 20. It would be technically possible for Google to index its Location History database by user location rather than user accounts. Suppression Hr’g Tr. 402-03.

B. The Defendant’s Google Account

On August 20, 2017, the defendant created the email account Okellochatric55@gmail.com. McGriff Decl. dated Aug. 7, 2020 at ¶ 2 (ECF No. 171-1) & Gov’t Ex. 3c at Exhibit A (hereinafter, Gov’t Ex. 3c). At that time, he agreed to Google’s terms of service. Suppression Hr’g Tr. 382. Those terms specified that “[b]y using our Services, you agree that Google can use such data in accordance with our privacy policies.” *See* Google Terms of Service last modified October 25, 2017 at 3, Gov’t Ex. 5a, (hereinafter, “Gov’t Ex. 5a”).²

On July 9, 2018, the defendant opted in to Google’s storage of his Location History. Gov’t Ex. 3c at ¶ 5 & Exhibit B. Google Location History allows users “to keep track of locations they

² The terms of service available at that time are also available at <https://policies.google.com/terms/archive/20140414>. The best evidence of Google’s privacy policy and terms of service is online. Suppression Hr’g Tr. 386.

have visited while in possession of their compatible mobile devices.” Gov’t Ex. 3 at ¶ 4. Google uses Location History to provide location-based services to users: for example, users can obtain “recommendations based on places they have visited, get help finding their phones, and receive real-time traffic updates about their commutes.” Gov’t Ex. 3 at ¶ 6; Suppression Hr’g Tr. 292, 347.

Google also uses Location History for advertising purposes. Gov’t Ex. 3 at ¶¶ 5, 14; Suppression Hr’g Tr. 196-98, 561. It infers users’ interests from where they visit, and it uses that “semantic location information” to target advertising to users. Gov’t Ex. 3 at ¶¶ 5, 14. Google also targets ads to users based on their proximity to a particular business. Suppression Hr’g Tr. 198. In addition, Google uses location information to measure “store visit conversions”—how many customers who saw a particular ad went on to visit a relevant store. Gov’t Ex. 3 at ¶ 14; Suppression Hr’g Tr. 196-97. Although Google does not share a user’s Location History directly with advertisers, it does share with advertisers store visit conversion information that it derives from Location History. Suppression Hr’g Tr. 196-97, 561.

The majority of Google users decline to opt in to Location History. Suppression Hr’g Tr. 351. In 2019, approximately one-third of active Google users had Location History enabled. Gov’t Ex. 3 at ¶ 13; Suppression Hr’g Tr. 387.

A Google user may review, edit, or delete Location History information. Gov’t Ex. 3 at ¶ 15; Suppression Hr’g Tr. 321, 388, 416. Deletion takes place nearly immediately. Suppression Hr’g Tr. 416. Deleted Location History information is not retained at all, even in anonymized form. Suppression Hr’g Tr. 321. A Google user may also stop collection of Location History information. Suppression Hr’g Tr. 416. Stopping collection can be accomplished through any of three paths: settings on any App that uses Location History, device-level settings, or through the

myactivity.google.com website. Suppression Hr’g Tr. 340-41.

Opting in to storage of Location History is not the only step a user must take in order for Google to store the user’s Location History. Gov’t Ex. 3 at ¶¶ 7-11. As Location History Product Manager Marlo McGriff explained, Location History “functions and saves a record of the user’s travels only when the user opts into [Location History] as a setting on her Google account, enables the ‘Location Reporting’ feature for at least one mobile device, enables the device-location setting on that mobile device (and for iOS devices provides the required device-level application location permission), powers on and signs into her Google account on that device, and then travels with it.” Gov’t Ex. 3 at at ¶ 10.³

When the defendant opted in to Location History on July 9, 2018, a user could not opt in to storage of Location History without following Google’s “supported consent flow,” which is “the steps and consent text necessary to opt in” to its service. Gov’t Ex. 3c at ¶ 6. If a user attempted to opt in using an unsupported consent flow, the process would not be successful. Suppression Hr’g Tr. 297. Under the supported consent flow for Location History on July 9, 2018, Google presented the user with the following text:

Location History

Saves where you go with your devices

This data may be saved and used in any Google service where you were signed in to give you more personalized experiences. You can see your data, delete it and change your settings at account.google.com.

NO THANKS

TURN ON

Gov’t Ex. 3c at ¶ 7.

³ In his testimony at the suppression hearing, McGriff affirmed that he stood by his affidavits. Suppression Hr’g Tr. 376.

Along with this text, Google presented an expansion arrow to the user that the user could tap to obtain additional information about Location History. Gov't Ex. 3c at ¶ 8. This expanded Location History text stated:

Location History

Saves where you go with your devices

Location History saves where you go with your devices. To save this data, Google regularly obtains location data from your devices. This data is saved even when you aren't using a specific Google service, like Google Maps or Search.

If you use your device without an internet connection, your data may be saved to your account once you return online.

Not all Google services save this data to your account.

This data helps Google give you more personalized experiences across Google services, like a map of where you've been, tips about your commute, recommendations based on places you've visited, and useful ads, both on and off Google.

This data may be saved and used in any Google service where you were signed in to give you more personalized experiences. You can see your data, delete it and change your settings at account.google.com.

NO THANKS

TURN ON

Gov't Ex. 3c at ¶ 8.

Regardless of the Application or service a user was using, a user could not opt in to Location History on July 9, 2018, without encountering this consent flow text and tapping "TURN ON." Gov't Ex. 3c at ¶¶ 10-11.

Defense expert Spencer McInville determined that he could not "replicate the opt-in process [for Location History] Mr. Chatrue would have seen." McInville Suppl. Report, Def. Ex. 7, at 1 (hereinafter, "Def. Ex. 7"); Suppression Hr'g Tr. 152. From his analysis of the defendant phone, McInville believed that the defendant installed Google Assistant shortly before he opted

in to Location History. Suppression Hr’g Tr. 76. McInville opined that the defendant had used Google Assistant to activate Location History. Suppression Hr’g Tr. 79.

McInville then looked for publicly available information regarding past use of Google Assistant to opt in to Location History. Def. Ex. 7 at 1; Suppression Hr’g Tr. 82. He found three examples, but only his third came from the time frame when the defendant opted in to Location History. Def. Ex. 7 at 1-4. His first example is an article that appeared at qz.com on January 24, 2018, nearly six months before the defendant opted in to Location History. Def. Ex. 7 at 1; Suppression Hr’g Tr. 220. That article includes a screenshot showing some opt-in language for Location History, but the language shown does not follow the supported consent flow required by Google to opt-in on July 9, 2018. Def. Ex. 7 at 1. For example, rather than saying “Saves where you go with your devices”, it says “Creates a private map of where you go with your signed-in devices.” Def. Ex. 7 at 1.

Second, McInville found an Oracle report dated September 2018. Def. Ex. 7 at 2; Oracle Report dated September 2018, Def. Ex. 11 at 4 (hereinafter, “Def. Ex. 11”). The Oracle report also includes screenshots capturing some opt-in language for Location History, but it does not identify when its screenshot were taken, and the language from the screenshots again does not follow the supported consent flow required by Google to opt in on July 9, 2018. Def. Ex. 7 at 2; Def. Ex. 11 at 4. For example, like the qz.com article, the screenshot states: “Creates a private map of where you go with your signed-in devices.” Def. Ex. 7 at 2; Def. Ex. 11 at 4.

Third, McInville found a report from the Norwegian Consumer Council with screenshots taken approximately contemporaneously with when the defendant opted in to Location History. Def. Ex. 7 at 3-4. In particular, the Norwegian reports includes screenshots taken on July 2 and August 9, 2018. *Id.* The screenshots in the Norwegian report are consistent with the supported

consent flow set forth by McGriff: every word of the supported consent flow set forth by McGriff is visible in the Norwegian screenshots. Gov’t Ex. 3c at ¶¶ 7, 8; Def. Ex. 7 at 3-4. McInville believed that the Norwegian report captures “the true depiction of the opt-in process.” Suppression Hr’g Tr. 100.

The Google Assistant process varied based on a user’s previous use of Google’s products and services. Suppression Hr’g Tr. 415. The screenshots from the Norwegian report showed opt-in text for Location History bundled with opt-in language for Device Information and Voice and Audio Activity. Def. Ex. 7 at 3-4. However, a user who had previously consented to Device Information and Video and Audio Activity would see only Location History. Suppression Hr’g Tr. 335. The record does not indicate whether the defendant opted in to any other Google services at the time he opted in to Location History.

Google’s Privacy Policy provided further information to Google users regarding Google’s storage and use of location information. Google Privacy Policy effective January 22, 2019, Gov’t Ex. 5 (hereinafter, “Gov’t Ex. 5”). The Privacy Policy in effect on the date of the robbery—May 20, 2019—included the following:

We collect information about your location when you use our services, which helps us offer features like driving directions for your weekend getaway or showtimes for movies playing near you. . . .

The types of location data we collect depend in part on your device and account settings. For example, you can turn your Android device’s location on or off using the device’s settings app. You can also turn on Location History if you want to create a private map of where you go with your signed-in devices. . . .

We use the information we collect in existing services to help us develop new ones. . . .

For example, you can turn on Location History if you want traffic predictions for your daily commute.

Gov't Ex. 5 at 4-6, 9. The Privacy Policy also explained to users multiple mechanisms for deleting their data, including deleting specific data and deleting data from specific services. Gov't Ex. 5 at 11-12.

II. ARGUMENT

A. *The Defendant Had No Reasonable Expectation of Privacy in Two Hours of the Location Information He Disclosed to Google.*

The defendant had no reasonable expectation of privacy in any of the information disclosed by Google pursuant to the geofence warrant. This result is hardly surprising: to obtain location-based services, a user must disclose his location to the service provider. Thus, the government's acquisition of two hours of the defendant's location information is governed by the long-standing principle that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities." *United States v. Miller*, 425 U.S. 435, 443 (1976). In addition, the defendant has no reasonable expectation of privacy in his location information under *Carpenter v. United States*, both because *Carpenter* retained the third-party doctrine and because *Carpenter* held only that the government infringes a cell phone owner's reasonable expectation of privacy when it accesses seven days or more of cell phone location information. *See Carpenter v. United States*, 138 S. Ct. 2206, 2217 n.3, 2220 (2018).

1. The Fourth Amendment does not protect information disclosed to a third party and then conveyed by the third party to the government.

In cases ranging from private conversations to business records, the Supreme Court has repeatedly held that the Fourth Amendment does not protect information revealed to a third party and then conveyed by the third party to the government. This principle applies to statements made in the presence of an informant. *See Hoffa v. United States*, 385 U.S. 293, 302 (1966). It applies to information disclosed to an accountant. *See Couch v. United States*, 409 U.S. 322, 335-36

(1973). It applies to bank records. *See United States v. Miller*, 425 U.S. 435, 443 (1976). It applies to dialed telephone number information. *See Smith v. Maryland*, 442 U.S. 735, 742-44 (1979). It applies to financial records. *See SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984). And in this case, this principle applies to two hours of location information disclosed to Google to obtain location-based services.

In addition to its broad scope, the principle that the government may obtain information revealed to a third party has deep roots. The Supreme Court has recognized that “as early as 1612, . . . Lord Bacon is reported to have declared that ‘all subjects, without distinction of degrees, owe to the King tribute and service, not only of their deed and hand, but of their knowledge and discovery.’” *Blair v. United States*, 250 U.S. 273, 279-280 (1919) (quoting *Countess of Shrewsbury Case*, 2 How. St. Tr. 769, 778 (1612)). Similarly, the Court has recognized that it is an “ancient proposition of law” that the public “has a right to every man’s evidence.” *United States v. Nixon*, 418 U.S. 683, 709 (1974). In this case, Google was a witness to the robbery: it had information regarding the bank robbery in a database which it accessed and used to provide services to its users and advertisers. The public had a right to Google’s evidence, and the Fourth Amendment did not bar the United States from obtaining that evidence from Google.

2. The defendant voluntarily conveyed his location information to Google.

A closer look at Google’s location-based services, its opt-in process, and its agreements with the defendant all confirm what Google told this Court: that Google users “voluntarily choose to save and share [Location History] information with Google.” ECF No. 59 at 22.

a. *Google’s location-based services*

As an initial matter, the fact that the defendant voluntarily disclosed his location to Google is evident from the nature of the relationship between Google and its users: users provide their

location to Google in order to receive location-based services. Courts often infer that an individual voluntarily disclosed information to a third party based on the nature of the relationship between the individual and the third party. For example, in *Miller*, the Supreme Court did not need to consider Miller's explicit agreements with his bank in order to conclude that he had voluntarily disclosed his financial information. Instead, the Court's conclusion was based on "examin[ing] the nature of the particular documents sought" and concluding that they were "not confidential communications but negotiable instruments to be used in commercial transactions." *Miller*, 425 U.S. at 442.

Google customers disclose their location to Google to obtain services that depend on Google knowing their specific location, such as mapping, traffic updates, help finding their phones, and help with their commutes. Gov't Ex. 3 at ¶ 6; Suppression Hr'g Tr. 347; Gov't Ex. 3c at ¶ 8. Google also uses location information to target advertisements to users, both through users' current location and based on inferences Google draws from Location History. Gov't Ex. 3 at ¶ 5, 14; Suppression Hr'g Tr. 198. In addition, Google uses location information to measure "store visit conversions," which it shares with advertisers. Suppression Hr'g Tr. 196-97.

All of these services demonstrate that Google does more than provide a mere storage service for location information. Based on a user's location, Google provides services that are helpful to the user, like mapping or finding a phone. It uses location information to provide services that are helpful to both the user and other users in the area, like traffic updates. And Google's advertising services employ user location information to benefit the user, the advertiser, and Google itself. In sum, a user of Google's location services does not keep his location private; a user shares location information with Google to obtain location-based services. Because "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and

conveyed by him to Government authorities,” *Miller*, 425 U.S. at 443, the government did not infringe the defendant’s Fourth Amendment interests when it obtained location information he disclosed to Google.

Furthermore, the fact that Google does not normally share a user’s specific location directly with additional parties does not affect this analysis. As the Supreme Court stated in *Miller*, the third-party doctrine applies to information disclosed to a third party even “if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.” *Miller*, 425 U.S. at 443. Here, the United States did not infringe the defendant’s Fourth Amendment interests because he disclosed his location to Google; the extent to which Google shares that information with others does not change this result.

b. Google’s opt-in process

The opt-in process necessary for Google to store the defendant’s Location History further demonstrates that the defendant voluntarily disclosed his location to Google. Unlike a phone company’s collection of cell-site information, Google would not have obtained the defendant’s location information during the bank robbery unless the defendant had taken the multiple steps necessary to enable him to share his location with Google. Google saves Location History “only when the user opts into [Location History] as a setting on her Google account, enables the ‘Location Reporting’ feature for at least one mobile device, enables the device-location setting on that mobile device (and for iOS devices provides the required device-level application location permission), powers on and signs into her Google account on that device, and then travels with it.”

Gov't Ex. 3 at at ¶ 10.⁴

McGriff also specified the supported consent flow necessary for the defendant to store his Location History. Gov't Ex. 3c at ¶¶ 7, 8. The text of this consent flow establishes that the defendant voluntarily disclosed his location information to Google.

As an initial matter, the record makes clear that the consent flow language that the defendant agreed to is the consent flow language set forth in the McGriff affidavit. Gov't Ex. 3c at ¶ 7-8. McGriff swore that this language was used “across all applications and services, and across all Android devices and operating systems” on July 9, 2018, when the defendant opted in to Location History. Gov't Ex. 3c at ¶ 7. Moreover, every word of this language appears in the contemporaneous Norwegian report cited by the defendant, which states that its screen shots were taken in July and August of 2018. Gov't Ex. 3c at ¶ 7, 8; Def. Ex. 7 at 3-4. In contrast, the qz.com article comes from January 2018, and the Oracle report does not document when its screenshots were taken, but it has language similar to the qz.com article. Def. Ex. 7 at 1-2; Def. Ex. 11 at 4.

Thus, when the defendant argues based on language from the qz.com article, such as his repeated references to Google referring to Location History as creating a “private map,” he is arguing based on opt-in language that Google did not present to the defendant during the opt-in process. Def. Post-Hr'g Suppl. Br. at 24, 32. Had defendant not encountered the supported consent

⁴ The defendant claims that this process “boiled down to a single pop-up screen in Google Assistant,” but his claim is not supported by the record. Def. Post-Hr'g Suppl. Br. at 24. The defendant's own expert conceded that he could not replicate the defendant's opt-in process. Suppression Hr'g Tr. 152. Only McGriff provided sworn testimony regarding all the steps of the opt-in process. Gov't Ex. 3 at at ¶ 10. Moreover, it is clear that the “single pop-up screen in Google Assistant” could not have done everything necessary for Google to store the defendant's Location History. For example, prior to that screen, the defendant would have had to sign into his Gmail account Okellochatrie55@gmail.com using his phone. The defendant may have used Google Assistant, but he still needed to complete all the steps described by McGriff in order for Google to store his Location History.

flow language, his attempt to opt in to Location History would have failed. Gov’t Ex. 3c at ¶ 6. This Court should disregard arguments based on language from outside the supported consent flow presented to users on July 9, 2018.

The language from the supported consent flow of July 9, 2018, confirms that the defendant voluntarily disclosed his location to Google. Google informed the defendant that Location History “[s]aves where you go with your devices” and that “[t]his data may be saved and used in any Google service where you were signed in to give you more personalized experiences. You can see your data, delete it and change your settings at account.google.com.” Gov’t Ex. 3c at ¶ 7. This language was concise, accurate, and easy to understand, and it set forth the core components of Google’s Location History service: that Google would store the defendant’s location information and that Google would use that information to provide services to the defendant. It also informed the defendant that he could see and delete his information through the Google website. *See id.* In addition, Google provided the defendant with the opportunity to obtain more detailed information concerning Location History by clicking an expansion arrow. Gov’t Ex. 3c at ¶ 8. After Google presented this text to the defendant, he tapped “TURN ON.” Gov’t Ex. 3c at ¶ 10. This opt-in process establishes that the defendant voluntarily disclosed his location to Google.

The defendant makes numerous objections to this opt-in language, but his objections cannot obscure the fundamental fact that he agreed that Google would save his Location History and use it to provide him services. His objections therefore do not withstand scrutiny.

First, the defendant objects that “a user might reasonably infer that this ‘private map’ or saved data would be saved only on their device, not with Google.” Def. Post-Hr’g Suppl. Br. at 25. Not only did Google not refer to a “private map,” and not only is the storage location of data disclosed to Google to obtain Google services of no significance, but also Google’s concise

consent-flow language made clear that the defendant's location data would be stored remotely: Google informed the defendant that he could review or delete his data "at account.google.com." Gov't Ex. 3c at ¶ 7. Google's use of this URL confirms that the data is stored remotely by Google, not on the user's device. In addition, via the expansion arrow, Google further informed potential Location History customers that "[t]o save this data, Google regularly **obtains location data from your devices.**" Gov't Ex. 3c at ¶ 8 (emphasis added). Google informed the defendant that his data would be stored remotely.

Second, the defendant objects that Google did not inform users "about the frequency or sheer quantity of data collected." Def. Post-Hr'g Suppl. Br. at 26. The Supreme Court, however, has made clear that this objection lacks constitutional significance. In *Smith v. Maryland*, 442 U.S. at 745, the Court held that a phone company's choices regarding storage of dialed telephone number information did not "make any constitutional difference" because the defendant "voluntarily conveyed to it information that it had facilities for recording and that it was free to record." Here, the defendant similarly conveyed his location information to Google, and Google's decisions regarding how often to store that information lack constitutional significance. Moreover, Google did not mislead the defendant in any way. Google did exactly what the defendant agreed it should do: store where he went with his device. Because people often move fast and do not stay in one place for long, relatively frequent storage of location information by Google is necessary for it to provide quality service. Furthermore, Google informed the defendant that he could review his stored data at account.google.com. Thus, if he wanted to know more about how frequently Google stored his location, that information was available to him there.

Third, the defendant objects that "nothing explains that Location History will operate independently, regardless of whether the phone is in use." Def. Post-Hr'g Suppl. Br. at 26. Again,

this objection is based on a misinterpretation of Google’s consent flow language. Google’s concise explanation of its service stated that Location History “[s]aves where you go with your devices.” Gov’t Ex. 3c at ¶ 7. This categorical language includes no limitations or exceptions, thereby making clear that the Location History service did not depend on use of specific Apps. The defendant is essentially suggesting that Google should have added redundancy to Google’s concise consent flow language, but redundancy was not required for the defendant to voluntarily disclose his location to Google. In addition, Google’s expanded consent flow language stated that “[t]his data is saved even when you aren’t using a specific Google service.” Gov’t Ex. 3c at ¶ 8.

Fourth, the defendant objects that “it would have been counterintuitive and difficult for Mr. Chatrie to disable and delete [his Location History], assuming he even knew about its existence.” Def. Post-Hr’g Suppl. Br. at 27. But Google did not keep secret the data or the defendant’s ability to delete it. It informed him: “You can see your data, delete it and change your settings at account.google.com.” That language was more than sufficient to inform the defendant of his ability to delete information and where to find the details on how to do so. The defendant also seems to suggest that the distinction between deleting data and halting its future collection is hopelessly complicated, but nothing in that distinction is particularly confusing. On the contrary, given the defendant’s ability to review his data at account.google.com, it would have been easy for him to confirm that he had, in fact, deleted his data.

In sum, the defendant’s objections to Google’s consent-flow language are premised on the notion that Google should have presented the defendant with a longer description of its service, rather than including the longer description through an optional expansion arrow. But Google’s actual approach—concise text informing the defendant that it would save his location information and use it to provide him services, along with an expansion arrow linking to more detailed

information—is sufficient to establish that the defendant voluntarily disclosed his location information to Google. At the evidentiary hearing, McGriff explained the practical result of the defendant’s approach: a “wall of text” that users would not be inclined to read. Suppression Hr’g Tr. 441.⁵

c. Google’s Privacy Policy

Finally, Google’s Privacy Policy further supports the fact that the defendant voluntarily disclosed his location information to Google. Courts rely on terms of service and privacy policies in evaluating whether a service provider’s disclosure of information to the government violates the Fourth Amendment. *See, e.g., United States v. Adkinson*, 916 F.3d 605, 610 (7th Cir. 2019) (holding that that T-Mobile’s disclosure of cell-site information to the government did not violate Adkinson’s Fourth Amendment rights because Adkinson “agreed to T-Mobile’s policy that T-Mobile could disclose information when reasonably necessary to protect its rights, interests,

⁵ The defendant points to criticism of Google’s Location History service from other parties, *see* Def. Post-Hr’g Suppl. Br. at 29-30, but this Court should give such criticism no weight. First, this Court did not admit that criticism for the truth of the matter asserted. Second, the record in this case sets forth the actual consent flow language Google presented to the defendant. Thus, there is no need for this Court to defer to the views of various third parties about Google’s opt-in procedures—views potentially based on different language than that actually presented to the defendant. In addition, those critics are not attempting to address the question before this Court: whether, for Fourth Amendment purposes, the defendant voluntarily conveyed his location information to Google.

property, or safety”).⁶ Here, through Google’s Terms of Service, the defendant agreed that Google could use his information in accordance with its Privacy Policy. Suppression Hr’g Tr. 382; Gov’t Ex. 5a at 3. And that Privacy Policy stated: “We collect information about your location when you use our services, which helps us offer features like driving directions for your weekend getaway or showtimes for movies playing near you.” Gov’t Ex. 5 at 4. In addition, the Privacy Policy contained specific examples pertaining to Location History, including: “you can turn on Location History if you want traffic predictions for your daily commute.” *Id.* at 9. This language confirms that the defendant agreed to share his location with Google in order for Google to provide him with location-based services. Furthermore, the Privacy Policy provided an additional explanation to the defendant of his ability to delete his information. *Id.* at 11-12.

3. The defendant has no reasonable expectation of privacy in two hours of Google location information under the reasoning of *Carpenter*.

In *United States v. Carpenter*, 138 S. Ct. 2206, 2217 & n.3 (2018), the Supreme Court determined that individuals have a “reasonable expectation of privacy in the whole of their physical movements,” and it held “that accessing seven days of [cell-site location information] constitutes a Fourth Amendment search.” The Court emphasized that its decision was “a narrow one,” and it explicitly declined to determine whether there is a “limited period” for which the government can

⁶ The defendant fundamentally misreads *Smith v. Maryland* when he claims that it supports his argument that courts should not consider a company’s Privacy Policy in evaluating whether a customer has a reasonable expectation of privacy. See Def. Post-Hr’g Suppl. Br. at 27. In fact, *Smith*’s determination that users have no reasonable expectation of privacy in dialed phone numbers was based in part on Privacy Policy-like statements included in phonebooks. See *Smith*, 442 U.S. at 742-43 (“Most phone books tell subscribers, on a page entitled ‘Consumer Information,’ that the company ‘can frequently help in identifying to the authorities the origin of unwelcome and troublesome calls.’”). In contrast, *Smith* found no Fourth Amendment significance in the phone company’s internal data storage practices and definition of local-dialing zones, which do not at all resemble privacy policies. See *id.* at 745.

acquire cell phone location information without implicating the Fourth Amendment, or whether a cell tower dump constituted a search. *Id.* at 2217 n.3, 2220.

Although *Carpenter* declined to resolve whether obtaining two hours of cell phone location information constitutes a search, *Carpenter*'s reasoning suggests it does not, because *Carpenter* is focused on protecting a privacy interest in long-term, comprehensive location information. The Court began its opinion by framing the question before it as "whether the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements." *Carpenter*, 138 S. Ct. at 2212. The Court emphasized that long-term cell-site information created a "comprehensive record of the person's movements" that was "detailed" and "encyclopedic." *Id.* at 2216–17. It explained that "this case is not about 'using a phone' or a person's movement at a particular time." Rather, the Court explained, the case concerned "a detailed chronicle of a person's physical presence compiled every day, every moment, over several years." *Id.* at 2220. By this standard, the government did not conduct a search when it obtained the two hours of the defendant's location information pursuant to the geofence warrant. Rather than providing an encyclopedic chronicle of the defendant's life, the information disclosed by Google provided a summary of his location for less than half an afternoon. This information is not quantitatively or qualitatively different from information that could be obtained from other sources, such as surveillance video or live witnesses.

In addition, in numerous cases involving other sophisticated new technologies, lower courts held that *Carpenter* protects only comprehensive, long-term location information. For example, the Seventh Circuit recently held that real-time tracking of a specified cell phone over a period of approximately six hours was not a search. *See United States v. Hammond*, — F.3d —, 2021 WL 1608789, at *7-*11 (7th Cir. Apr. 26, 2021). The Seventh Circuit previously determined

that a cell tower dump was not a search, and two other district courts reached the same result. *See United States v. Adkinson*, 916 F.3d 605, 611 (7th Cir. 2019) (stating that *Carpenter* “did not invalidate warrantless tower dumps (which identified phones near *one location* (the victim stores) at *one time* (during the robberies))” (emphasis in original)); *United States v. Walker*, 2020 WL 4065980, at *8 (W.D.N.C. July 20, 2020) (concluding that the “privacy concerns underpinning the court's holding in *Carpenter* do not come into play” for a cell tower dump, which is limited to “particular *place at a limited time*”) (emphasis in original)); *United State v. Rhodes*, 2021 WL 1541050, at *2 (N.D. Ga. Apr. 20, 2021) (stating that *Carpenter* “centrally relied on the strong Fourth Amendment privacy interests implicated when law enforcement monitors or obtain voluminous, detailed cell phone information of a person's physical presence compiled over a lengthy period that effectively delineates the contours of the individual's life and communications”).⁷ These cases all support the conclusion that the United States did not infringe the defendant’s Fourth Amendment interests when it obtained two hours of his location information from Google.

Significantly, *Carpenter* did not reject the third-party doctrine or “disturb the application

⁷ Similarly, courts have rejected a broad interpretation of *Carpenter* in cases involving automatic license plate reader databases, which record the time and place a license plate is observed. Obtaining a large amount of location information about an individual from such a database could potentially implicate *Carpenter*’s concerns regarding comprehensive location information. But investigators do not conduct a search when they obtain only a small quantity of location information from such a database. *See Commonwealth v. McCarthy*, 484 Mass. 493, 494 (2020) (“[W]hile the defendant has a constitutionally protected expectation of privacy in the whole of his public movements, an interest which potentially could be implicated by the widespread use of [automatic license plate readers], that interest is not invaded by the limited extent and use of ALPR data in this case.”); *United States v. Yang*, 958 F.3d 851, 862 (9th Cir. 2020) (Bea, J., concurring) (stating that a query of a large automatic license plate recognition database that revealed only a single location point for Yang was not a search under *Carpenter* because “the information in the database did not reveal ‘the whole of [Yang’s] physical movements.’”).

of *Smith* and *Miller*.” *Carpenter*, 138 S. Ct. at 2220. Instead, *Carpenter* held that cell phone users do not voluntarily disclose their cell-site records to the phone company because cell-site information is collected “without any affirmative act on the part of the user beyond powering up,” because “there is no way to avoid leaving behind a trail of location data,” and because carrying a cell phone “is indispensable to participation in modern society.” *Carpenter*, 138 S. Ct. at 2220. These factors are not present here. Google could not obtain and store the defendant’s location without his undertaking multiple affirmative acts, including signing in to Google on his phone, enabling the phone’s device location setting, enabling location reporting, and opting in to Location History. Gov’t Ex. 3 at ¶ 10. The defendant also had discretion to delete any or all of his Location History. Gov’t Ex. 3 at ¶ 15; Suppression Hr’g Tr. 321, 388, 416. And none of the services associated with Google’s storage of Location History are indispensable to participation in modern society. In fact, approximately two-thirds of Google’s users reject those services. Gov’t Ex. 3 at ¶ 13; Suppression Hr’g Tr. 387.

Citing *Carpenter*, the defendant asserts that this Court should disregard the third-party doctrine, “Even If Mr. Chatrie Intentionally Enabled Location History.” Def. Post-Hr’g Suppl. Br at 31. To do so, however, would disregard controlling precedent. *Carpenter* held based on facts specific to the cell phone provider context that *Carpenter* had not voluntarily disclosed his cell phone location information to the phone company, but it did not otherwise reverse or limit the third party doctrine. *See Carpenter*, 138 S. Ct. at 2220. Thus, if this Court determines that the defendant intentionally disclosed his location to Google, this Court must conclude that the defendant had no reasonable expectation of privacy in the location information the United States obtained from Google, as “a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.” *Smith v. Maryland*, 442 U.S. at 743-44.

4. The defendant's remaining arguments are without merit.

None of the defendant's remaining arguments establish that the United States infringed the defendant's Fourth Amendment interest when it obtain location information from Google.

First, he argues that "Location History Is At Least As Precise as CSLI," but he fails to explain why that fact creates a reasonable expectation of privacy. Def. Post-Hr'g Suppl. Br. at 20. The third-party doctrine applies to information voluntarily disclosed to a third party; it includes no exception for accurate location information. And the Supreme Court in *Carpenter* assumed that cell-site information "is rapidly approaching GPS-level precision," *Carpenter*, 138 S. Ct. at 2219, but *Carpenter* still only protected disclosure of long-term, comprehensive location information.

Second, the defendant claims that "A Search of Location History Data Is Highly Intrusive," but this argument is neither supported by facts in the record nor sufficient to establish that he had a reasonable expectation of privacy in his location information. Def. Post-Hr'g Suppl. Br. at 21-23. As an initial matter, the principle that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties" is not limited to information which is not particularly revealing about an individual. Conversations with others, dialed telephone numbers, and bank records can all contain sensitive information that an individual would like to keep private, but they are all subject to the third-party doctrine. Furthermore, the information the United States obtained from Google in this case was not particularly sensitive. Indeed, the defendant makes no claim that it revealed anything sensitive about him at all. Neither presence at a bank nor movements along public roads are particularly sensitive information. *See, e.g., United States v. Knotts*, 460 U.S. 276, 285 (1983) (holding that monitoring movements along public roads using a

transponder installed in a container of chemicals was not a search).⁸

Third, the defendant cites the fact the United States obtained information about other Google users, but he provides no explanation of how this fact supports his claim that he had a reasonable expectation of privacy in the location information disclosed by Google. Def. Post-Hr’g Suppl. Br. at 22. In addition, his attempt to rely on the Fourth Amendment interests of others is foreclosed by Supreme Court precedent. The Supreme Court has squarely held that Fourth Amendment rights “may not be vicariously asserted.” *Rakas v. Illinois*, 439 U.S. 128, 133-34 (1978) (quoting *Alderman v. United States*, 394 U.S. 165, 174 (1969)). Defendants lack standing to challenge the government obtaining others’ cell phone location information. *See, e.g., United States v. Patrick*, 842 F.3d 540, 545 (7th Cir. 2016).

Fourth, the defendant cites the fact that Google filtered through its entire Location History database to find information responsive to the warrant, Def. Post-Hr’g Suppl. Br. at 22, but he fails to explain how this filtering would give him an expectation of privacy. In determining whether a defendant has a reasonable expectation of privacy, courts consider the totality of the circumstances regarding the relationship between the defendant and the object of the search, *see United States v. Castellanos*, 716 F.3d 828, 846 (4th Cir. 2013), but they do not consider the particular legal process used by the government to obtain that object. The defendant would have had no reasonable expectation of privacy in two hours of his Google Location History regardless of whether the United States obtained it using a geofence warrant or a warrant explicitly identifying his account.

⁸ The defendant’s claim that “the defense was easily able to determine the likely identities of at least three individuals” from the geofence location information is not supported by the record. *See* Def. Post-Hr’g Suppl. Br. at 22. The defense’s expert witness stated that he had not “figured out who anyone is.” Suppression Hr’g Tr. 151. Moreover, neither identifying someone present at a bank nor identifying the neighborhood that someone visits (or even their home) is particularly invasive.

Fifth, the defendant is mistaken when he argues that “[u]nder the government’s theory, people do not have an expectation of privacy in any data stored with a third-party or service provider, other than long-term CSLI.” Def. Post-Hr’g Suppl. Br. at 31. Here, the defendant has no reasonable expectation of privacy in his location information because he disclosed it to Google in order for Google to provide him with location-based services. This principle does not apply in many common circumstances involving online service providers. For example, when an email service provider transmits and stores email on behalf of a customer, the email service does not typically depend on the substantive contents of the email, so the user may retain a reasonable expectation of privacy in email content information.

Finally, the defendant adopts by reference his “property-based arguments,” Def. Post-Hr’g Suppl. Br. at 32, but his argument remains contrary to the fundamental principle that “the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities.” *Miller*, 425 U.S. at 443. The defendant cites no case—and the United States is aware of no case—in which a court has relied on a “property-based theory” to discard the third-party doctrine of *Smith* and *Miller* or prevent witnesses from providing evidence to the government. Justice Gorsuch’s solo dissent in *Carpenter* did contemplate abandoning the third-party doctrine based on some sort of property rights theory of the Fourth Amendment, *see Carpenter*, 138 S. Ct. at 2262-72 (Gorsuch, J., dissenting), but a solo dissent is not the law, and the third-party doctrine of *Smith* and *Miller* remains binding law.

B. The Geofence Warrant Satisfied the Fourth Amendment

The geofence warrant did not remotely resemble a general warrant. As set forth below, the warrant satisfied the Fourth Amendment because it was supported by probable cause and specified its object with particularity.

More generally, the facts of this case illustrate why use of a geofence warrant involves no unreasonable search or seizure. When law enforcement officers sought the warrant, they were investigating a serious violent crime, and they had reason to believe that the perpetrator posed a danger to the public if not identified and apprehended. Suppression Hr’g Tr. 622. The geofence warrant enabled them to solve the crime and protect the public by allowing them to obtain a limited and focused set of records from Google: location information over a two-hour interval of three identified and six unidentified individuals, and limited location information over a one-hour interval of ten other unidentified individuals.

The defendant argues that investigators should have taken a different path: “track down the owner of the car the suspect was seen in and compare that information to cell phone numbers that had connected with a nearby cell phone tower.” Def. Post-Hr’g Suppl. Br. at 42. This approach would have required investigators to obtain a cell tower dump covering a much broader area, which likely would have revealed location information about thousands of people. Suppression Hr’g Tr. 55. It would have required them to obtain a list of everyone who had a blue Buick. Suppression Hr’g Tr. 578. And then it would have required them to further investigate everyone who fell within the overlap of these sets.

Although the defendant’s approach would also have complied with the Fourth Amendment, it would have been substantially more intrusive than the geofence warrant, as well as being less likely to succeed and more expensive. It would be a very strange result if the Fourth Amendment were to bar use of a precise, focused investigative technique like a geofence warrant, and if it instead forced investigators to cast much broader nets. Fortunately, the defendant is mistaken, and the geofence warrant complied with the Fourth Amendment.

1. The Geofence Affidavit Established Probable Cause

Probable cause requires only “a fair probability, and not a prima facie showing, that contraband or evidence of a crime will be found in a particular place.” *United States v. Bosyk*, 933 F.3d 319, 325 (4th Cir. 2019) (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983) (internal quotation marks omitted)). It is “not a high bar.” *Id.* (quoting *District of Columbia v. Wesby*, 138 S. Ct. 577, 586 (2018)). In addition, this Court does not conduct *de novo* review concerning the existence of probable cause: “the duty of a reviewing court is simply to ensure that the magistrate had a substantial basis for concluding that probable cause existed.” *United States v. Hodge*, 354 F.3d 305, 309 (4th Cir. 2004) (quoting *Gates*, 462 U.S. at 238–39).

Here, the affidavit in support of the geofence warrant established an ample basis for the issuing magistrate’s finding of probable cause. In particular, the affidavit established: (1) that an unknown subject committed an armed bank robbery at a particular place and time; (2) that prior to the robbery, the robber held a cell phone to his ear and appeared to be speaking with someone; (3) that the majority of cell phones were smartphones; (4) that “[n]early every” Android phone “has an associated Google account,” and that Google “collects and retains location data” from such devices when the account owner enables Google location services; and (5) that Google can collect location information from non-Android smartphones if the devices are “registered to a Google account and the user has location services enabled.” Gov’t Ex. 2 at 6-7. From this information, there was a substantial basis for the magistrate to conclude that there was a fair probability that Google possessed evidence related to the robbery.

One United States Magistrate Judge recently explained his basis for issuing a geofence warrant in an arson investigation, including his determination that the warrant was supported by probable cause. *See In re Search Warrant Application*, 497 F. Supp. 3d 345 (N.D. Ill. 2020)

(hereinafter, “Harjani Opinion”). In that investigation, there was “no evidence in the affidavit that any of the suspects possessed cell phones.” *Id.* at 355. Nevertheless, the magistrate judge noted that judges “may draw reasonable inferences about where evidence is likely to be found based on the nature of the evidence and the offense,” and he determined that it was reasonable to infer that suspects and passerby witnesses would have cell phones, and that Google would have information about their location and identity. *See id.* at 355-56. He concluded that “the affidavit, when considering the totality of the circumstances and the agent's training and experience, allows the Court to conclude there is a fair probability that location data at Google will contain evidence of the arson crime, namely the identities of perpetrators and witnesses to the crime.” *Id.* Here, where the robber used his phone just before the robbery, the basis for the magistrate’s finding of probable cause was stronger than in the investigation addressed in the Harjani Opinion.

The probable cause determination for a geofence warrant is similar to that for a tower dump warrant, and in *United States v. James*, No. 18-cr-216, 2019 WL 325231 (D. Minn. Jan. 25, 2019), the district court held that a series of tower dump warrants satisfied the Fourth Amendment. In *James*, the government used tower dump warrants to solve a series of robberies. The defendant there argued that there was no probable cause for the warrants because it was “unknown whether a phone was used by the suspect before or after the robbery.” *Id.* at *3. Nevertheless, the district court found that probable cause existed based on the affiant’s representations about the “ubiquitous nature” of cell phones, the likelihood of criminals using cell phones, and the storage by cell phone companies of location information. *Id.* This reasoning similarly supports the magistrate’s finding of probable cause for the geofence warrant in this case.

Two other magistrate judges from the Northern District of Illinois have written opinions denying applications for geofence warrants. The first magistrate judge found that the bounds of

the geofence sought by the government were too broad, but he stated that the government “could easily have sought a constitutionally valid search warrant” if it had “constrained the geographic size of the geofence and limited the cellular telephone numbers for which agents could seek additional information to those numbers that appear in all three defined geofences.” *See In re Search of Information Stored at Premises Controlled by Google*, 2020 WL 5491763, at *7 (N.D. Ill. July 8, 2020). Whether the bounds of a particular geofence are too broad will always be based on the facts and circumstances of the investigation. In this investigation, the bounds of the geofence were appropriately drawn for the magistrate to conclude that there was a fair probability that Google possessed the specified evidence of crime. *See* Suppression Hr’g Tr. 523 (discussing the bounds of the geofence).

The second magistrate judge held that probable cause for a geofence warrant was lacking because there was not “probable cause to believe *every* person who entered the location engaged in the criminal activity.” *In re Search of Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 752 (N.D. Ill. 2020) (emphasis in original). As the Harajani Opinion recognized, however, “it is nearly impossible to pinpoint a search where only the perpetrator’s privacy interests are impacted.” Harjani Opinion, 497 F. Supp. 3d at 361-62. For example, the Fourth Amendment does not bar a search warrant to search a residence that a suspect shares with others. Both the defendant here and the second magistrate judge base their arguments on *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979), in which the Supreme Court held that the probable cause that supported a warrant to search a tavern and its bartender for drugs did not extend to a search of tavern patrons. But *Ybarra* is not a general limitation on search warrants that might reveal information concerning non-suspects; it merely held that the probable cause to search a commercial premises for drugs did not extend to a search of the business’s patrons. The Harjani

Opinion explains why *Ybarra* does not limit a geofence warrant like the one here: “the government has established a fair probability that location data obtained will retrieve location data of perpetrators, co-conspirators and witnesses within the geofence, and the request is sufficiently particular to avoid any concerns resulting from *Ybarra*.” Harjani Opinion, 497 F. Supp. 3d at 362 n.6.

The defendant makes several arguments that attempt to narrow or redefine the meaning of “probable cause.” These arguments lack merit, and this Court should reject them.

First, the defendant argues that the geofence warrant lacked probable cause “because investigators admittedly had no suspects.” Def. Post-Hr’g Suppl. Br. at 33. However, a search warrant need not identify specific suspects—all it must do is establish a fair probability that specified evidence will be found in the place to be searched. For example, in *Zurcher v. Stanford Daily*, 436 U.S. 547, 551 (1978), the Supreme Court approved a search warrant that authorized seizure from a newspaper of photographs of unidentified individuals who had assaulted police officers. The defendant cites no case suggesting that a warrant cannot be used to solve crime.

Second, the defendant asserts that “[p]robable cause must be based on individualized facts, not group probabilities,” and he claims it was improper to infer that “the robber was a Google user or had Location History enabled.” Def. Post-Hr’g Suppl. Br. at 33-34. This is error: a magistrate may “draw such reasonable inferences as he will from the material supplied to him by applicants for a warrant.” *Illinois v. Gates*, 462 U.S. 213, 240 (1983). Here, the magistrate’s finding of probable cause was based on a combination of specific facts (that the bank had been robbed and that the robber carried a cell phone) and reasonable inferences (that there was a fair probability that Google stored location evidence pertaining to this crime). Warrants commonly rely on a combination of specific facts and reasonable inferences, and the defendant cites no contrary case

law. For example, in *United States v. Jones*, 942 F.3d 634, 639-40 (4th Cir. 2019), the Fourth Circuit held that a magistrate had made a reasonable inference that evidence of a defendant's threats would be found at his home. Here, the magistrate similarly made a reasonable inference that Google stored evidence of the robbery.

Third, the defendant's argument is based on an improperly constricted view of what would constitute evidence of the robbery. He focuses on whether "the robber was a Google user," Def. Post-Hr'g Suppl. Br. at 33, but the issuing magistrate here had additional reasons to believe that location information held by Google would be evidence. Investigators could use the location information directly to reconstruct what took place at the crime scene at the time of the crime. They could use it to identify any accomplices. They could use it to identify potential witnesses and obtain further evidence. They could use it to corroborate and explain other evidence, including surveillance video. They could use it to rebut potential defenses raised by the robber, including an attempt by the robber to blame someone else for his crime. Thus, although the affidavit did in fact establish a fair probability that Google would have evidence concerning the robber, the probable cause established by the warrant extended well beyond that, and it was reasonable for the magistrate to conclude that all of the information that fell within the scope of the warrant constituted evidence of crime.⁹

⁹ *Messerschmidt v. Millender*, 565 U.S. 535 (2012), supports this understanding of what may constitute evidence for purposes of a search warrant. In *Messerschmidt*, police obtained a warrant for "all guns and gang-related material" in connection with a known gang member shooting at his ex-girlfriend. *Id.* at 539. In a civil suit under 42 U.S.C. § 1983, Millender challenged the warrant as overbroad, but the Supreme Court rejected the suit based on qualified immunity. *See id.* The Court provided multiple reasons why it was not unreasonable for a warrant to seek "all gang-related materials" in connection with someone shooting at his ex-girlfriend. These reasons included that it could "help to establish motive," that it could be "helpful in impeaching [the shooter]," that it could be helpful in "rebutting various defenses," and that it could "demonstrat[e] [the shooter's] connection to other evidence." *Id.* at 551-52.

2. The Geofence Warrant Was Not Overbroad and Specified its Objects with Particularity

Under the Fourth Amendment, “a valid warrant must particularly describe the place to be searched, and the persons or things to be seized.” *United States v. Kimble*, 855 F.3d 604, 610 (4th Cir. 2017) (internal quotation marks omitted). In addition, the items specified to be seized pursuant to a warrant must be “no broader than the probable cause on which it is based.” *United States v. Hurwitz*, 459 F.3d 463, 473 (4th Cir. 2006). The test “is a pragmatic one” that “may necessarily vary according to the circumstances and type of items involved.” *United States v. Torch*, 609 F.2d 1088, 1090 (4th Cir. 1979) (quoting *United States v. Davis*, 542 F.2d 743, 745 (8th Cir. 1976)). Here, the geofence warrant satisfied these requirements.

a. *Overbreadth*

The geofence warrant was not overbroad because it was narrowly constrained based on location, dates, and times. The warrant sought only location and identity information from Google regarding a two-hour interval for individuals present at the site of a robbery during a one-hour window. Based on the facts and circumstances investigators knew about the robbery, it was appropriately tailored toward its investigatory purpose, which was to obtain evidence to help identify and convict the armed bank robber. The geofence was based on specific features of the site of the robbery. For example, it went up to but did not cover Price Club Boulevard to the east, and it covered the area where the robber had parked. Suppression Hr’g Tr. 523. Like the geofence warrant approved in the Harjani Opinion, the government “established a fair probability that location data obtained will retrieve location data of perpetrators, co-conspirators and witnesses within the geofence.” Harjani Opinion, 497 F. Supp. 3d at 362 n.6. Because the evidence the

government was authorized to obtain was “no broader than the probable cause on which it is based,” the warrant was not overbroad.

The cell tower dump opinion *James* provides additional authority that the warrant here was not overbroad. In *James*, the defendant challenged the tower dump warrants used to identify him as a robber because they “allowed law enforcement to identify the location of hundreds if not thousands of cell phone users on specific days during specific time frames.” *James*, 2019 WL 325231 at *3. The district court, however, found that the warrants satisfied the Fourth Amendment because they sought information that was “constrained—both geographically and temporally—to the robberies under investigation.” *Id.* This reasoning is fully applicable here: the geofence warrant was appropriately constrained in space and time to obtain evidence of the robbery. Indeed, the location information obtained from Google was more narrowly constrained than the location information in *James*. The 150-meter radius of the geofence warrant is smaller than most cellular sites, and the government only obtained location information regarding 19 individuals, most of them never identified, rather than hundreds or thousands.¹⁰

The defendant argues that the geofence warrant was overbroad because Google filtered its Location History database to comply with it, but this argument is without merit. Def. Post-Hr’g Suppl. Br. at 33. He cites no case law holding that a service provider may not review a large data set in order to produce a narrowly defined set of information. Such process is not new: for example, in response to a subpoena, a phone company may review every call made by all its customers in order to find calls made to a specified phone number. *See Ameritech Corp. v.*

¹⁰ The defendant argues that cell tower dumps are more limited than geofence warrants because cell phone companies “‘index’ data based on location.” Def. Post-Hr’g Suppl. Br. at 35. But as discussed further below, a company’s internal data structures have no Fourth Amendment significance. *See infra* pp. 36-37.

McCann, 403 F.3d 908, 910 (7th Cir. 2005).

Here, Google stores its users' location information in a single database, Sensorvault. Gov't Ex. 3 at ¶ 11. Google accesses its users' location information freely to provide them and others with location-based services. For example, Google offers its advertisers a service called "radius targeting," which requires Google to determine whether a customer is within a specified distance of a specified point. Suppression Hr'g Tr. 198. And then Google further accesses users' location information to measure store visit conversions, which it shares with the advertisers. Gov't Ex. 3 at ¶ 14; Suppression Hr'g Tr. 196-97. Here, the warrant mandated an equivalent to radius targeting, but for the purpose of solving a bank robbery, rather than selling a product. The Fourth Amendment does not prohibit Google, in response to warrant, filtering data that it accesses and uses for its own business purposes.

Moreover, Google's review of a large set of data to comply with the geofence warrant is a result of Google's internal data storage practices, not an overbroad warrant. It would be possible for Google to create an additional Location History database indexed by location. Suppression Hr'g Tr. 402-03. This database would enable Google to comply with a geofence warrant—and produce the exact same data as Google currently produces—without filtering the data of all customers. The constitutionality of a search warrant does not depend on a service provider's internal data storage practices invisible to customers and the government alike. For example, in *Smith v. Maryland*, the Supreme Court held that a phone company's internal practices regarding storage of dialed number information did not "make any constitutional difference." *Smith*, 442 U.S. at 745. This reasoning is fully applicable here to Google's choice of internal data structures. The appropriate measure for the breadth of the geofence warrant here is the data sought by the warrant, which resulted in the government obtaining location information for only 19 individuals,

all of whom were near the bank at the time of the robbery.

b. Particularity

The geofence warrant specified the items to be seized with unusual precision. The warrant authorized disclosure from Google of two hours of location information associated with electronic devices that were, within a 30 minutes on either side of a bank robbery, within 150 meters of a specified point, as well as specified subscriber information associated with those devices. Gov't Ex. 2 at 4-5. Most warrants require a human to make judgments regarding whether particular items fall within the scope of the items to be seized, but here, Google could use a computer algorithm to find the responsive information. The defendant's assertion that "[t]he items to be seized are not specified" by the geofence warrant is therefore wrong. Def. Post-Hr'g Suppl. Br. at 37.

The defendant asserts that the warrant left too much discretion to Google, but the warrant left Google no discretion at all. *See* Def. Post-Hr'g Suppl. Br. at 38. First, the defendant complains that "Google decided to search Location History data, as opposed to Web & App Activity or Google Location Services data," *see id.*, but only the Location History database held information responsive to the warrant. Gov't Ex. 3 at ¶ 20; Suppression Hr'g Tr. 211. Second, the defendant complains that Google "picked a method of calculating which devices were inside the geofence that generated a high number of false positives," Def. Post-Hr'g Suppl. Br. at 38, but the warrant itself directed Google to disclose information for devices "inside the described geographical area" during the time of the robbery. Gov't Ex. 2 at 4. Google correctly interpreted this language to mean that Google should disclose information concerning devices whose latitude and longitude coordinates fell within the circle specified by the warrant. Although there always remains a possibility of imprecision in Google's location information, and a defendant may certainly challenge at trial the weight given to this information, that possibility does not make a warrant

insufficiently particular.¹¹

Nor was there anything improper about FBI TFO Hylton's correspondence with Google, in which he ultimately requested that Google produce step 2 location information about nine individuals. Suppression Hr'g Tr. 622, 642; Gov't Ex. 4 at 9. Google remains an independent actor, and courts have held that a provider like Google has a due process right to object to an order directing it to comply with a search warrant. *See, e.g., In re Application*, 610 F.2d 1148, 1157 (3d Cir. 1979). Where a service provider produces a portion of the information specified by legal process, the United States does not violate the Fourth Amendment when it chooses not to litigate over the rest. A contrary rule would waste judicial resources and harm privacy. Nothing in the execution of the geofence warrant supports the defendant's argument that the warrant was insufficiently particular.

The defendant also challenges the warrant because it included the second and third steps of its three-step process, thereby allowing investigators to obtain less than the maximum quantity of location and identity information that the warrant authorized. *See* Def. Post-Hr'g Suppl. Br. at 38-39. The warrant, however, established probable cause for all the evidence that law enforcement could have obtained: identity information and two hours of location data for all individuals present

¹¹ The defendant exaggerates the magnitude of uncertainty associated with Google's location information. He emphasizes individual location measurements that had a large display radius. These measurements, however, were in general accompanied by other measurements for the same device with smaller display radius. For example, the defendant points to one measurement in the initial production from Google with a display radius of 387 meters. *See* Def. Post-Hr'g Suppl. Br. at 17. However, a separate measurement point for that same device taken only 23 seconds before had a display radius of only 84 meters. *See* FBI CAST Report at 22 (noting initial GeoFence returns, including for Device ID 702354289); Def. Ex. 3 (cell entries 208 and 209 for Device ID 702354289). As Special Agent D'Errico explained, Google location data of this nature (two records close in time with the same center point, but a larger second display radius) indicates that the device is traveling. Suppression Hr'g Tr. 532. The uncertainty associated with the second point does not affect the accuracy of the first.

at the site of the robbery during the hour of the robbery. The information specified by a warrant must be “no broader than the probable cause on which it is based,” *Hurwitz*, 459 F.3d at 473, but officers do not violate the Fourth Amendment if they ultimately seize less evidence than the maximum a warrant authorizes. The Harjani Opinion approved a multiple-step geofence warrant for precisely this reason: “[T]he government has established probable cause to seize all location and subscriber data within the geofence locations identified. Whether it chooses to obtain all that information, or partial information, is of no matter to the Court's consideration of the constitutionality of the warrant under the Fourth Amendment.” Harjani Opinion, 497 F. Supp. 3d at 362.

The most heavily-litigated search warrant in history—the search warrant in the investigation of the Playpen child pornography website—included a similar component that allowed investigators to prioritize the evidence they seized, and courts have agreed that that component did not violate the Fourth Amendment.¹² Playpen was a dark web child pornography site with over 158,000 members. *See United States v. McLamb*, 880 F.3d 685, 688 (4th Cir. 2018). FBI investigators obtained a warrant authorizing a search of the computers of everyone who logged into Playpen for 30 days. *See id.* at 689. The attached affidavit, however, allowed the FBI to choose to obtain less than the maximum amount of information the warrant authorized. It explained that that “in executing the requested warrant, the FBI may deploy the NIT more

¹² Eleven Courts of Appeals have considered various challenges to the Playpen warrant, and all have ultimately rejected suppression. *See United States v. Taylor*, 935 F.3d 1279, 1281 (11th Cir. 2019) (“[W]e become today the eleventh (!) court of appeals to assess the constitutionality of the so-called ‘NIT warrant.’ Although the ten others haven't all employed the same analysis, they've all reached the same conclusion—namely, that evidence discovered under the NIT warrant need not be suppressed.”). Approximately 100 district court cases have resolved suppression motions challenging the Playpen warrant. As discussed in Section C below, the Fourth Circuit rejected a challenge to the particularity of the Playpen warrant based on the good-faith exception. *See United States v. McLamb*, 880 F.3d 685, 689-91 (4th Cir. 2018).

discretely against particular users.” *United States v. Anzalone*, 208 F. Supp. 3d 358, 363 (D. Mass. 2016).

Some defendants argued that the discretion given the FBI in executing the Playpen warrant violated the Fourth Amendment’s particularity requirement, but courts uniformly rejected this argument. For example, in *United States v. Matish*, 193 F. Supp. 3d 585, 609 (E.D. Va. 2016), the court concluded that “the fact that the FBI could have and did narrow its search in this case is immaterial, since the warrant was based on probable cause to search any computer logging into the site.” *See also Anzalone*, 208 F. Supp. 3d at 368 (“Every court to consider this question has found the NIT search warrant sufficiently particular.”). Similarly, the fact that investigators here could have and did narrow the information obtained from Google is immaterial, as the geofence warrant was based on probable cause and appropriately authorized seizure of location and identity information of anyone at the site of the robbery. Rather than violating the Fourth Amendment, the three-step process allowed investigators to further protect privacy.

Finally, even if there were a particularity problem in the three-step process for the geofence warrant, the appropriate remedy would at most be to sever the second step of the warrant and to suppress second-step information. “[E]very federal court to consider the issue has adopted the doctrine of severance, whereby valid portions of a warrant are severed from the invalid portions and only materials seized under the authority of the valid portions, or lawfully seized while executing the valid portions, are admissible.” *United States v. Sells*, 463 F.3d 1148, 1154–55 (10th Cir. 2006); *see also United States v. Jones*, 2018 WL 935396, at *16–*18 (E.D. Va. Feb. 16, 2018) (discussing and applying doctrine of severance).

Here, the first step of the geofence warrant targeted narrow and clearly-defined information: anonymized location information for devices within 150 meters of the bank during

the hour of the robbery. Even if this Court were to find the second step to be constitutionally inadequate, the appropriate remedy would thus be to sever the second step and retain the first. In addition, first-step information alone was sufficient for investigators to recognize that the defendant's account likely belonged to the robber. Suppression Hr'g Tr. 549-50. Thus, even if this Court were to sever the warrant and suppress second-step information from Google, the subsequent investigation of the defendant would not be the fruit of the poisonous tree.¹³

C. Evidence from the Geofence Warrant Should Not Be Suppressed Because Investigators Relied on it in Good Faith

Even assuming the geofence warrant was lacking in probable cause or particularity, suppression would not be an appropriate remedy. Suppression is a remedy of "last resort," to be used for the "sole purpose" of deterring future Fourth Amendment violations, and only when the deterrence benefits of suppression "outweigh its heavy costs." *Davis v. United States*, 564 U.S. 229, 236-37 (2011). "The fact that a Fourth Amendment violation occurred—*i.e.*, that a search or arrest was unreasonable—does not necessarily mean that the exclusionary rule applies." *Herring v. United States*, 555 U.S. 135, 140 (2009). "To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Id.* at 144.

Search warrants for Google information about the location of its users are a new investigative technique, and there were no judicial opinions analyzing them under the Fourth Amendment when FBI TFO Hylton sought his warrant. In *United States v. McLamb*, 880 F.3d

¹³ Under *Bynum*, 604 F.3d at 164, the defendant lacks a reasonable expectation of privacy in subscriber information obtained under step three of the geofence warrant, and he therefore lacks standing to challenge that portion of the warrant.

685 (4th Cir. 2018), the Fourth Circuit rejected suppression in this circumstance. The court held that when considering a motion to suppress the fruits of a novel investigative technique, suppression was inappropriate where the investigating officer consulted with counsel and then sought a warrant:

But in light of rapidly developing technology, there will not always be definitive precedent upon which law enforcement can rely when utilizing cutting edge investigative techniques. In such cases, consultation with government attorneys is precisely what Leon's 'good faith' expects of law enforcement. 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.

McLamb, 880 F.3d at 691. Here, Detective Hylton followed the approach endorsed by *McLamb*. He had consulted with prosecutors before seeking both state and federal geofence warrants. Suppression Hr'g Tr. 603-04. He had previously obtained geofence warrants from both state judges and a United States Magistrate Judge. Suppression Hr'g Tr. 603-04. No prosecutor or judge had ever found a problem with these warrants. Suppression Hr'g Tr. 604-05. In this investigation, he then sought and obtained a search warrant from a state magistrate. Detective Hylton thus did what *McLamb* calls for, and the good-faith exception precludes suppression here.

The defendant also insinuates that investigators did something wrong by using a go-by from the Computer Crime and Intellectual Property Section at the Department of Justice. Def. Post-Hr'g Suppl. Br. at 3-4. But *McLamb* affirmatively encourages such consultation: it applied the good faith exception where investigators had consulted with experts from another Department of Justice section, the Child Exploitation and Obscenity Section. *See McLamb*, 880 F.3d at 691.

The defendant notes that FBI TFO Hylton had received no training on geofence warrants, Def. Post-Hr'g Suppl. Br. at 44, but there is no indication in *McLamb* that the agents there had received training on darknet child pornography warrants. Indeed, such trainings may not exist

when a new investigative technique first arises. *McLamb* calls for direct consultation with prosecutors and then seeking a warrant, not meeting a bureaucratic training requirement. Consulting directly with experts is an effective form of training, even if it is not officially categorized as such.

Alternatively, suppression is inappropriate under the traditional good-faith analysis of *United States v. Leon*, 468 U.S. 897 (1984). When police act in “objectively reasonable reliance on a subsequently invalidated search warrant” obtained from a neutral magistrate, “the marginal or nonexistent benefits produced by suppressing evidence ... cannot justify the substantial costs of exclusion.” *Id.* at 922. *Leon* identified four circumstances in which an officer’s reliance on a warrant would not be objectively reasonable:

(1) when the issuing judge “was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth”; (2) when “the issuing magistrate wholly abandoned his judicial role ...”; (3) when “an affidavit [is] so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable”; or (4) when “a warrant [is] so facially deficient—*i.e.*, in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid.”

United States v. Perez, 393 F.3d 457, 461 (4th Cir. 2004) (quoting *Leon*, 468 U.S. at 923). None of these circumstances are present in this case.

The defendant argues that the good faith exception does not apply here because the affidavit was so lacking in indicia of probable cause that reliance on it was unreasonable, *see* Def. Post-Hr’g Suppl. Br. at 42-43, but he is mistaken. As an initial matter, “the threshold for establishing this exception is a high one” because “[o]fficers executing warrants are not often expected to question the conclusions of an issuing authority.” *United States v. Seerden*, 916 F.3d 360, 367 (4th Cir. 2019) (quoting *Messerschmidt v. Millender*, 565 U.S. 535, 547 (2012)). The defendant claims that the warrant was based on “conjecture,” Def. Post-Hr’g Suppl. Br. at 42-43, but in fact

it was based on facts and reasonable inferences from those facts. The affidavit established that the bank robber had a cell phone, that most cell phones are smartphones, and that nearly every Android phone user and some non-Android phone users use Google, and that Google may store user location information. Based on these facts, the executing officers' belief that the warrant to Google was issued based on probable cause was not entirely unreasonable, and the good-faith exception thus precludes suppression.

The defendant also argues that the good faith exception does not apply because the warrant was so facially deficient in failing to specify the things to be seized that officers could not reasonably rely on it. *See* Def. Post-Hr'g Suppl. Br. at 43. But as discussed previously, the warrant was unusually specific: Google determined the responsive information using a computer algorithm. As discussed above at pages 37-38, the warrant was limited to location information over a two-hour interval, as well as accompanying identity information, for individuals present at the site of the robbery during a one-hour interval.

The defendant further argues that the warrant left too much discretion to Google, Def. Post-Hr'g Suppl. Br. at 44, but the warrant left no discretion to Google at all. The warrant, not Google, specified the physical and temporal bounds of the geofence. The warrant authorized law enforcement, not Google, to narrow down the information to be disclosed at the warrant's second and third phase. Gov't Ex. 2 at 4. It is true that when a provider is directed to comply with a warrant, it has a due process right to challenge the warrant. *See, e.g., In re Application*, 610 F.2d 1148, 1156-57 (3d Cir. 1979). But that possibility provides no evidence that the warrant was insufficiently particular.

In addition, the Fourth Circuit's decision in *McLamb* forecloses the defendant's argument that the warrant was facially deficient because its three-step process left too much discretion to

investigators. *See* Def. Post-Hr’g Suppl. Br. at 44. The defendant in *McLamb* argued to the Fourth Circuit that the Playpen warrant was insufficiently particular, in part because it allowed the FBI to “deploy the [search technique] more discretely against particular users.” *See* Brief of Appellant at 46-47, *United States v. McLamb*, No. 17-4299 (available at 2017 WL 2832704). The Fourth Circuit relied on *Leon*’s good-faith exception to reject suppression, concluding that the Playpen warrant was not “so ‘facially deficient ... that the executing officers [could not] reasonably presume it to be valid.’” *McLamb*, 880 F.3d at 691. Under *McLamb*, the warrant here was not facially deficient, even though it authorized investigators to obtain less evidence than they established probable cause for.

The defendant also claims that the issuing magistrate “abandoned his judicial role,” but no evidence supports his claim. Def. Post-Hr’g Suppl. Br. at 41-42. The defendant begins by pointing out that the magistrate was relatively new to his job, but the defendant cites no law suggesting that *Leon* is somehow less applicable to a warrant issued by a new judge or magistrate. The defendant also notes that the magistrate spent 15 to 30 minutes reviewing the warrant application, but that was a sufficient length of time to read the relatively short affidavit and make a commonsense determination that there was a fair probability that Google possessed evidence of the bank robbery. The defendant further faults the magistrate for signing a warrant that the defendant claims lacked particularity, but as the United States has explained, the warrant specified its object with exacting particularity. *See supra* pages 37-40.

The Defendant concedes that he is “not making a *Franks* claim,” but he then goes on to allege that the warrant application contained misleading information and material omissions. Def. Post-Hr’g Suppl. Br. at 45. Because he is not making a *Franks* claim, these allegations do not support an argument that the good-faith exception should not apply here. The United States notes,

however, that the defendant's allegations are incorrect. First, he claims that the information produced by Google in the first two steps was not anonymous, but in fact Google did not identify any individual until step 3, and additional research or information would have been required to identify an account owner. In the context of the language of the search warrant, that is what "anonymized information" means—the warrant stated that "anonymized information" was "a numerical identifier for the account, the type of account, time stamped location coordinates and the data source." Gov't Ex. 2 at 4. Second, the defendant faults TFO Hylton for not informing the magistrate about Google's automated data filtering processes, but TFO Hylton lacked knowledge about Google's internal data structures. Suppression Hr'g Tr. 606-67. Third, the defendant faults FBI TFO Hylton for not addressing potential inaccuracies in Google's location information. But the fact that there is some imprecision in cell phone location measurements is common knowledge; there is no reason FBI TFO Hylton would not have expected the issuing magistrate to be aware of that fact. In sum, the affidavit contained no misleading information, and any omissions were neither material to the issuance of the warrant, nor deliberate or reckless.

Finally, there is another more general reason why the investigators' reliance on the geofence warrant was reasonable: across the country, a broad array of neutral magistrates had approved geofence warrants, thus indicating their determinations that the warrants satisfy the Fourth Amendment. Magistrate Bishop's decision to sign the warrant was no outlier: Google received approximately 9000 geofence requests in 2019. Suppression Hr'g Tr. 489. FBI TFO Hylton himself had had geofence warrants approved by two state judges and a United States Magistrate Judge. Suppression Hr'g Tr. 603-04. And no judge had written an opinion rejecting an application for a geofence warrant. Given this context, and given FBI TFO Hylton's knowledge of other judges signing geofence warrants, FBI TFO Hylton's reliance on the geofence warrant in

this investigation was reasonable.

III. CONCLUSION

For the reasons set forth in this brief, this Court should deny the defendant's motion to suppress the fruits of the GeoFence warrant.

Respectfully submitted,

RAJ PAREKH
Acting United States Attorney

By: _____/s/
Nathan Judish
Senior Counsel, Computer Crime and
Intellectual Property Section
Criminal Division
United States Department of Justice

Kenneth R. Simon, Jr.
Peter S. Duffey
Assistant United States Attorneys
Eastern District of Virginia
919 E. Main Street, Suite 1900
Richmond, VA 23219
(804) 819-5400
Fax: (804) 771-2316
Email: Kenneth.Simon2@usdoj.gov

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division**

UNITED STATES OF AMERICA)	
)	
)	Case No. 3:19cr130
)	
OKELLO T. CHATRIE,)	
Defendant)	

**REPLY TO GOVERNMENT’S RESPONSE IN OPPOSITION
TO MR. CHATRIE’S MOTION FOR SUPPRESSION**

Okello Chatrie, through counsel, replies as follows to the government’s response to his motion to suppress evidence obtained from a “geofence” general warrant. *See* ECF No. 207-2.

I. Introduction

The Government primarily argues that nobody has an expectation of privacy in their Location History information. They do so because they cannot—and do not—contest the fact that the warrant here commanded a search of “numerous tens of millions” of people, none of whom the government had probable cause to search individually. It was astoundingly overbroad and lacking particularity.

The government tries to separate its actions from Google’s by seeking refuge in a three-step process that required Google to conduct a dragnet search of Location History users. But the government developed this three-step process in partnership with Google. The government wants to reap the results of the geofence search but take no responsibility for its creation and execution. The fact is the government was responsible for every step of the search. Google never conducts searches like this for business purposes and any attempt to equate geofence warrants with Google advertising is unsupported by the facts. Google searched the accounts of tens of millions of people only because they received a warrant commanding it.

It is immaterial that Google could have structured user data to make it easier for the government to search, as the government suggests. This argument also ignores that there is at least one good reason why Google chose to organize the Sensorvault database by user account: because the data belongs to the users who created it. *See* ECF No. 59-1 at 8. Any Location History data that exists, exists only in individual accounts—it is generated by individuals; it belongs to those individuals; it is intended to be private; and so, it makes sense to store it in individual user accounts. As a result, any attempt to identify individuals in any area will necessarily entail the search of tens of millions of individual accounts.

Second, the government minimizes *United States v. Carpenter* and seeks to narrow its holding into insignificance. Instead, it relies on *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979), two relics of a bygone era that the Court declined to extend in *Carpenter*. The so-called “third-party” doctrine is simply not on solid footing when it comes to digital searches and seizures, and the government’s attempts to liken a geofence warrant to an “invited informant” are similarly out of touch and unpersuasive. The existence of a service agreement does not end the Fourth Amendment inquiry. On the contrary, Timothy Carpenter had an agreement with his cell phone service provider, yet the Supreme Court looked beyond that, considering context, common sense, and the sensitivity of the data, to hold that the sharing of cell phone location data was not truly “voluntary.” Here, as Mr. Chatrue has demonstrated, the process of enabling Location History was also not “voluntary” in any meaningful sense.

Location History data is also far more precise than the cell tower data at issue in *Carpenter*. This precision matters because it means that Location History data is more *potent* than CSLI. A little goes a long way; it can reveal the same kind of private information with much fewer data points. A single data point from CSLI may only be capable of revealing which neighborhood or

zip code a device is in. By contrast, a single Location History data point may have GPS-level accuracy, pinpointing a device's location inside of a house or church. That is why defense expert Spencer McInville was able to determine the likely identities of at least three other individuals based on the supposedly "anonymized" data provided by Google during steps one and two. That is also why the government now proposes to sever the warrant; they know that even a little bit of "anonymized" data can reveal a wealth of personal information.

A geofence warrant is a digital dragnet. No matter how the government tries to dress it up or break it down, its defining features are overbreadth and lack of particularity. That is precisely why the government sought one here – they had no suspects, and they hoped a geofence search might generate one. Yet the government asks this Court to ignore the dragnet and instead rule that no one, including Mr. Chatrie, has an expectation of privacy in their Location History data. Under the government's logic, there would be no privacy right in virtually any data that involves a third-party. These arguments must be rejected. Mr. Chatrie urges this Court to find that he had an expectation of privacy in his Location History data and suppress the fruits of this modern-day general warrant.

II. Mr. Chatrie Had a Reasonable Expectation of Privacy in His Location History Data

A. The Third-Party Doctrine Does Not Apply

The government contends that the "third-party doctrine" forecloses any expectation of privacy in Location History data, *see* ECF No. 207-2 at 12, but the Supreme Court has never sanctioned a warrantless search of an individual's cell phone location data, let alone the search of millions at once. *See* 138 S. Ct. at 2219 (Court has "shown special solicitude for location information in the third-party context"). Indeed, the Court in *Carpenter* declined to extend the third-party doctrine to similar data and instructed lower courts not to "mechanically" apply old

rules to new technologies. *Id.* Yet that is precisely what the government asks this Court to do: mechanically apply precedent from the 1960s and 70s to the technology of 2021.

The government therefore invites error by likening Location History to an “invited informant,” *see* ECF No. 207-2 at 12 (citing *Hoffa v. United States*, 385 U.S. 293, 302 (1966)), as if Google were no different from the guy who Jimmy Hoffa conspired with in his hotel room. The Court found it dispositive that the informant was not only in the suite by invitation, but that “every conversation which he heard was either directed to him or knowingly carried on in his presence.” *Hoffa*, 385 U.S. at 302. Location History, by contrast, runs imperceptibly in the background, constantly recording, even if a user is doing nothing on the device. *See* ECF No. 205 at 26.

The government also heavily relies on *Smith v. Maryland*, 442 U.S. 735 (1979). There, the Court found no expectation of privacy in the digits dialed from a landline telephone. 442 U.S. at 742. The Court found it highly significant that callers were actively aware that they were interacting with the phone company when they placed a call, sometimes speaking with an operator, and receiving monthly bills with printouts showing the information collected. *Id.* at 742-45. In this case, by contrast, a user may enable Location History once—perhaps without even realizing it—and have no awareness that it remains on, silently recording, indefinitely. *See* ECF No. 205 at 26. Thus, if a user enabled Location History through the Google Assistant setup process, and then never used Google Assistant once, Location History would still be on and logging data every two or six minutes. *Id.* at 14, 26. Such a user would not know Location History is enabled, let alone how much data is being collected or how to manage it. Appearing to recognize that this was a problematic practice, Google eventually began sending out monthly emails to users who had enabled Location History, but Google has no record of sending such reminders to Mr. Chatrue and concedes that it may not have done so here. *See* ECF No. 205 at 30-31. Moreover, Google does

not bill users for Location History and Google does not compile Location History information for business purposes, unlike the digits dialed in *Smith*. See ECF No. 59-1 at 22. Consequently, Location History is not a “business record;” it is user data—content—that belongs to the individuals who created it. See *id.* at 8.

The government’s reliance on *Miller* is likewise misplaced. In *Miller*, the Court found no expectation of privacy in checks, deposit slips, and statements because they were “*negotiable instruments*” intended for use in commercial transactions. 425 U.S. at 438 (emphasis added). The Court distinguished them from otherwise “confidential communications.” *Id.* Location History data, by contrast, is considered “content” under the Stored Communications Act, see 18 U.S.C. § 2703(a) & (b), and Google treats it accordingly. See ECF No. 59-1 at 4. And in any event, Location History data is not a “negotiable instrument.” No one gets paid in Location History. Rather, Location History is private data belonging to individual users that Google does not provide to advertisers. See ECF No. 205 at 9, 35; Tr. at 197 (regardless of the type of advertising, Google “never share[s] anyone’s location history with a third party.”); see also *Carpenter*, 138 S. Ct. at 2212 (wireless carriers “often sell aggregated location records to data brokers, without individual identifying information”).

In sum, Location History is not an “invited informant.” It is not a “business record.” And it is not a “negotiable instrument.” It is, however, significantly more revealing than the bank records in *Miller* or the telephone numbers in *Smith*. See *Carpenter*, 138 S. Ct. at 2217 (“After all, when *Smith* was decided in 1979, few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person’s movements.”). And it is almost certainly different than whatever Lord Bacon had in mind when declaring that “all subjects ... owe to the King tribute and service.” ECF No. 207-2 at 13. Rather, Location History data is most like the cell site location information (“CSLI”) at issue in *Carpenter*, in which the Supreme Court found the third-party doctrine inapplicable.

B. Mr. Chatrpie Did Not “Voluntarily” Convey His Location Information to Google

One reason the *Carpenter* Court did not extend the third-party doctrine to CSLI was that people do not “voluntarily” convey sensitive data to the cell phone service provider in any “meaningful sense.” 138 S. Ct. at 2220. Of course, cell phone users sign contracts with cell phone services providers, but the Supreme Court has never allowed such agreements to determine the contours of 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 never mentioned the contract or terms of service.¹ Instead, the Court looked to the realities of the relationship between cell phone users and cell phone companies.

Here, the government invites this Court to simply “infer” that Google users intend to enable Location History and disclose dossiers of their every move because “Google provides services that are helpful to the user, like mapping or finding a phone,” as opposed to “mere storage.” ECF No. 207-2 at 14. Yet the cell phone company in *Carpenter* provided a helpful service as well. It transmitted phone calls and text messages directly to a user’s mobile device, which of course required keeping track of where it was at all times. People were aware of this fact, the Court presumed. *See* 138 S. Ct. at 2211-12. Moreover, the records were “generated for commercial purposes,” *id.* at 2217, and often sold in aggregate to data brokers for advertising purposes. *Id.* at 2212. Nonetheless, the Court looked to the realities of the digital age and saw that the “voluntary exposure” rationale underlying the third-party doctrine did not “hold up when it comes to CSLI” for two reasons. *Id.* at 2220.

¹ Nevertheless, it is worth reiterating that the Privacy Policies then in effect provided scant information about Location History, mentioning it just twice in two sentences. One described it only as a way to “save and manage location information in your account,” while the other said “you can turn on Location History if you want traffic predictions for your daily commute.” ECF No. 205 at 26-27 (quoting Def. Ex. 43 at 7-8).

First, “cell phones **and the services they provide** are ‘such a pervasive and insistent part of daily life’ that carrying one is indispensable to participation in modern society.” *Id.* at 2220 (quoting *Riley*, 573 U.S. at 385) (emphasis added). There can be no serious dispute that this remains true today, although the government appears to maintain otherwise. *See* ECF No. 207-2 at 24. Their argument seems to be that some features, like Location History and “mapping,” are not so indispensable. But *Carpenter* did not intend to limit Fourth Amendment protections to devices that are only capable of making calls and text messages. Instead, *Carpenter* rested on *Riley*, where the Court based its decision on the fact that modern smartphones serve many critical functions beyond making calls. *See Riley*, 573 U.S. at 393. They “are in fact minicomputers that also have the capacity to be used as a telephone.” *Id.* And importantly, they “could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, **maps**, or newspapers.” *Id.* (emphasis added). For most users, these functions are likely to be just as essential as owning a phone in the first place. Indeed, it is difficult to imagine a consumer who would purchase a device now that was incapable of mapping or location services.

Second, the *Carpenter* Court found it significant that cell phones generate CSLI “by dint of its operation, without any affirmative act on the part of the user beyond powering up.” *Id.* at 2220. Location History operates the same way once enabled, requiring no further action or interaction with the service as it quietly and constantly logs the phone’s location data. As with CSLI, “[v]irtually any activity on the phone”—or no activity at all—generates Location History data, even if the user is asleep. *See* ECF No. 205 at 26; Tr. at 122 (“[T]here were no periods of data not being collected.”).

The wrinkle in this case is that Location History is not absolutely required to use features like Google Maps or Google Assistant, for example. And it is technically possible to disable

Location History without disconnecting the device from the cellular network. *Cf. Carpenter*, 138 S. Ct. at 2220. At the same time, however, Google failed to inform users of these options, did not describe the full functioning of Location History, and employed a maze of location settings that made it difficult for ordinary people to understand, let alone control, the location information transmitted to Google. *See* ECF No. 205 at 23-29.

Google used an “opt-in” process that was uninformative at best, and deceptive at worst, nudging users at every turn to enable it without fully realizing what was happening. *See* ECF No. 205 at 29-31. This much is apparent from the high-profile “feedback” Google received and acknowledged from the likes of the United States Senate, the *New York Times*, and the *Associated Press*, not to mention a civil lawsuit led by the Attorney General of Arizona. *See* ECF No. 205 at 29-30. It is also apparent from Google’s reforms in response to these criticisms, all of which either came too late to help Mr. Chatrie, or else didn’t come at all. *See id.* at 30-31. Furthermore, it is far from clear, based on either of the two possible “consent flows” presented to Mr. Chatrie,² that a reasonable user would understand what Location History is, based on the partial sentence provided in the so-called “descriptive text.” *See id.* at 11-12. Rather, it would be reasonable to believe that such data would be saved locally on the device itself and not with Google. *See id.* at 24. Users are neither required nor prompted to view additional “copy text” hidden behind an “expansion arrow,” and they can enable Location History without ever seeing this information, which is also unilluminating. *See id.* at 13, 25.

As for disabling Location History, there is no way to turn it “off”—only to “pause” it. And even attempting to “pause” it results in an immediate, ominous pop-up warning advising users that

² The government maintains that there is only one possible “consent flow” in this case, *see* ECF 207-2 at 16-17, but Google testified that it could not be sure which language Mr. Chatrie would have seen (i.e., the “saves where you go” or “creates a private map” language) because it did not record the “UI” (user interface) on Mr. Chatrie’s phone. *See* Tr. at 298; *see also* Def. Ex. 7 at 1-3; ECF No. 205 at 11.

doing so will result in unspecified “limited functionality” on the device. *See* ECF No. 205 at 27-28. Likewise, deleting all Location History records does not stop future collection, *see id.* at 15, and deleting the app used to enable Location History continues to allow collection. *Id.* at 14, 27. Even Google engineers found Google’s location controls confusing, *see id.* at 29-30, with one employee emailing a company-wide listserv to ask: “which one of these options (some? all? none?) enter me into the wrongful-arrest lottery;” another wrote, “Add me to the list of Googlers who didn’t understand how this worked.” *Id.* at 30. Most recently, newly disclosed Google emails demonstrated that Google executives viewed it as a “problem” when users took advantage of easy-to-find privacy settings and then sought to obscure them in the settings menu.³ This may well explain why Location History has been enabled by “numerous tens of millions” of Google users. It also accounts for any technical differences between Location History and CSLI when assessing whether the data is truly “shared” in a “meaningful sense.” *See Carpenter*, 138 S. Ct. at 2220.

At the same time, there may be some users who affirmatively wish to keep a timeline of where they have been. And in such cases, individuals would still enjoy an expectation of privacy in their Location History data because it is their private property—data they create and save about their travels. *See* ECF No. 205 at 31-32. And because Location History tracks users all the time, it necessarily records when they are inside homes, churches, and similarly private locations, *i.e.*, constitutionally-protected spaces. Consequently, any trespass on the privacy of this digital property, especially when it reveals who or what is in a protected space, would trigger Fourth Amendment protections as well. *See* ECF No. 205 at 31-32.

³ *See* Tyler Sonnemaker, ‘Apple is eating our lunch’: Google employees admit in lawsuit that the company made it nearly impossible for users to keep their location private, *Business Insider* (May 28, 2021), available at <https://www.businessinsider.com/unredacted-google-lawsuit-docs-detail-efforts-to-collect-user-location-2021-5>.

The government dismisses this property-based argument as an invention of Justice Gorsuch's dissent in *Carpenter*. See ECF No. 207-2 at 27; ECF No. 41 at 12. But, as Mr. Chatrie has previously explained, see ECF No. 48 at 8-10, this understanding of the Fourth Amendment predates *United States v. Katz*, 389 U.S. 347 (1967), and has been repeatedly identified by the Supreme Court as an equally valid and independent test. See, e.g., *United States v. Jones*, 565 U.S. 400, 409 (2012) (“[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.”). Justice Gorsuch was merely recognizing that such an approach would have been an appropriate way to resolve *Carpenter*, had the defendant raised the argument. Mr. Carpenter did not, but Mr. Chatrie has done so consistently and adopts those arguments again. See ECF No. 29 at 14–16; ECF No. 48 at 8–10; ECF No. 109 at 20–21; ECF No. 205 at 32.

C. Location History Data Is Highly Sensitive and Can Be as Precise as GPS

In holding that the third-party doctrine does not apply to CSLI, the *Carpenter* Court considered not just whether people “voluntarily” share their CSLI with service providers, but also whether CSLI was different from the bank records and phone numbers in *Smith* and *Miller*. As the Court explained: “*Smith* and *Miller*, after all, did not rely solely on the act of sharing. Instead, they considered ‘the nature of the particular documents sought’ to determine whether ‘there is a legitimate ‘expectation of privacy’ concerning their contents.’” *Carpenter*, 138 S. Ct. at 2219. And in *Carpenter*, the Court recognized that there “is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today.” *Id.* Unlike typical business records, CSLI “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.’” *Id.* at 2217. Consequently, the Court determined that cell phone location records “hold for many Americans the ‘privacies of life.’” *Id.* at 2217.

Location History data, no less than CSLI, provides a window into the same “‘privacies of life.’” *See* ECF No. 205 at 21-23. The government claims, however, that the data in this case was “not particularity sensitive” because “[n]either presence at a bank nor movements along public roads are particularly sensitive information.” ECF No. 207-2 at 25. The government is wrong on three counts. First, the 150-meter geofence fully encompassed the Journey Christian Church, which is where Google placed Mr. Chatrie’s phone most of the time. Only two of the data points from step one indicate that Mr. Chatrie was inside the bank. All the other points show him either inside the church or parked just outside of it. *See* Gov. Ex. 1 at 24. Second, because the effective range of the geofence was 387 meters, not 150 meters, the initial search encompassed not just the bank and the church, but all the private residences and businesses nearby, including a hotel. *See* ECF No. 205 at 17-18; Gov. Ex. 1 at 20. Many of these are constitutionally-protected spaces where Fourth Amendment protections are at their greatest. *See, e.g., United States v. Karo*, 468 U.S. 705, 714-15 (1984) (“Searches and seizures inside a home without a warrant are presumptively unreasonable.”); *Stoner v. California*, 376 U.S. 483, 486 (1964) (requiring a warrant to search a hotel room). Additionally, the step-two data was not limited by any geofence and did in fact show people in their homes and apartments, in addition to tracking one person to a hospital. *See* ECF No. 205 at 22. Thus, as with CSLI, this kind of information “provides an intimate window into a person’s life,” revealing not only one’s movements, but the “‘privacies of life’” that the Court has sought to secure against “arbitrary power.” *Carpenter*, 138 S. Ct. at 2214, 2217.

Third, it does not matter what data the government seized. It had no way of knowing, *ex ante*, what the geofence search would show. They cannot now justify that search based on the data they ultimately seized. But more importantly, it is a fiction that the search has a geographic limit to begin with. As Mr. Chatrue is now aware, a geofence search does not just entail searching the records of a few people in one place; it entails searching *all* Location History users in *any* place, regardless of how investigators draw the circle. *See* ECF No. 205 at 16, 33. Thus, any suggestion that a geofence search does not involve sensitive information misapprehends how it works. The government would have this Court believe that a geofence search is a garden-variety request for a few simple business records. But as in *Carpenter*, this “fails to contend with the seismic shifts in digital technology” that made the search possible in the first place. 138 S. Ct. at 2219. Consequently, the government “is not asking for a straightforward application of the third-party doctrine, but instead a significant extension of it to a distinct category of information.” *Id.*

The government’s remaining objection is that this case involves two hours of Location History instead of seven days of CSLI. *See* ECF No. 207-2 at 22. But two hours of Location History reveals the “privacies of life,” especially when accounting for its greater precision and frequency of collection. Location History is at least as precise as CSLI, but it can also be as accurate as GPS. *See* ECF No. 205 at 20. That is because Google uses multiple data sources to estimate a user’s location, including CSLI and GPS, as well as Wi-Fi and Bluetooth. *Id.* at 5. Thus, the precision varies from point to point, depending on the available inputs. *Id.* At the same time, it can do things that even GPS cannot do, like determine a user’s elevation and identify the specific floor of the building they are on. *Tr.* at 372-73. Google also logs Location History data every two to six minutes, regardless of whether the phone is in use. *See* ECF No. 205 at 26.

By contrast, the precision of CSLI “depends on the geographic area covered by the cell site.” *Carpenter*, 138 S. Ct. at 2211. This may be sufficient to place a person “within a wedge-shaped sector ranging from one-eighth to four square miles,” for example. *Id.* at 2218. Or as the government demonstrated in this case, the coverage area for the three cell sites closest to the bank measures approximately 7 or 8 kilometers by 10 kilometers. Tr. at 528-29. As a result, a single CSLI data point could be used to determine which neighborhood or zip code someone was in, but it would not be accurate enough to identify the block and building. Moreover, even though cell phones ‘ping’ nearby cell sites several times a minute, service providers only log when the phone makes a connection, by placing a phone call or receiving a text message, for example. *See Carpenter*, 138 S. Ct. at 2211.

These differences between Location History and CSLI are significant because they affect how much data is needed to infer where someone was and what they were doing. While *Carpenter* anticipated that the precision of CSLI would improve, the Court was also faced with the fact that it was necessary to stitch together some minimum amount of CSLI to reveal the “privacies of life.” The Court settled on seven days, but this was not a magic number; it was simply the number of days in the record for the shortest court order at issue. *See* 138 S. Ct. at 2266-67 (Gorsuch, J., dissenting). And in reality, that order only produced two days of CSLI. *Id.* at 2212. Moreover, *Carpenter* explicitly declined to say “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.

Location History’s greater precision and frequency of collection means that less time is needed to reveal the “privacies of life.” It might take days of CSLI to piece together a mosaic with enough detail to be so revealing, but it takes just a little Location History to achieve the same

result. In this case, two hours was more than sufficient to identify users in sensitive and constitutionally-protected areas, including Mr. Chatrie in the church. And as Mr. Chatrie explains, the Supreme Court has repeatedly found such short-term searches to run afoul of the Fourth Amendment. *See* ECF No. 104 at 11; ECF No. 205 at 21-22 (citing *Karo*, 468 U.S. at 716, and *Kyllo*, 533 U.S. at 37). In short, *Carpenter* supports finding that Mr. Chatrie had a reasonable expectation of privacy in his Location History data.

III. The Warrant Was Overbroad

The government argues that the geofence warrant was supported by probable cause because “there was a fair probability that Google possessed evidence related to the robbery.” ECF No. 207-2 at 29. And the government repeatedly refers to Google as a “witness” to the robbery. *Id.* at 1, 13. But Google neither witnessed the robbery nor independently possessed any evidence of it. Rather, people witnessed the robbery and some of those people possessed relevant Location History data in their Google accounts. The government, however, did not establish probable cause to search a single person’s Google account. And they certainly did not establish probable cause to search “numerous tens of millions” of accounts.

Instead, the government engages in a Fourth Amendment slight of hand, substituting Google for the individual users they seek to search. With this trick complete, it might appear sufficient to simply recite the facts of the case, note the ubiquity of cell phones, and cite Google’s popularity to establish probable cause. *See* ECF No. 207-2 at 32. But once again, Google is no “witness.” Google does not own or control Location History data; users do. Google does not generate or keep Location History data; users do. It belongs to individuals, “numerous tens of millions” of them, and a geofence warrant searches every one of their accounts.⁴

⁴ The government maintains that it “need not identify specific suspects,” only establish that “evidence will be found in the place to be searched,” ECF No. 207-2 at 32, citing *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978). But the

Because the government did not establish probable cause to search any of these accounts, they now seek to wash their hands of the massive dragnet they cast. The government does not once mention the “numerous tens of millions” of users it searched. Instead, they describe step one as “filtering” data and attribute the action to Google as if such novel searches were a routine business practice. ECF No. 207-2 at 26, 36, 46. Contrary to the government’s claims, however, Google does *not* use Location History for purposes of “radius targeting.” *See* ECF No. 205 at 8-9. And regardless of the advertising type, Google “never share[s] anyone’s location history with a third party.” *See* Tr. 197; ECF. No. 205 at 9.

The government also lays any fault for the scope of the search at Google’s feet, calling it “a result of Google’s internal data storage practices.” *Id.* at 37. But this was no garden-variety warrant. Instead of requesting data from specific users or accounts, which Google can identify and retrieve using unique account identifiers, the government required Google to search every Location History account for relevant data. Or in other words, the government reversed the normal warrant process, searching millions before identifying any suspects or specific accounts. Once again, this is not “equivalent to radius targeting” and is not something Google ever does for purposes of “selling a product,” ECF No. 207-2 at 36. It was, plain and simple, an epic dragnet compelled by the government. Location History was not designed for such purposes, *see* ECF 205 at 20, and it does not make a difference that it could have been. The government is responsible for the warrants they execute. They cannot force Google to conduct a dragnet and then disavow the consequences. The fact remains that the government did not establish probable cause to search any of the millions of accounts they Google-searched, rendering the warrant profoundly overbroad.

search at issue in *Zurcher* involved photographs of a demonstration taken by a newspaper employee. The newspaper owned those photographs, the photographer was a true witness to the events, and the newspaper office did not also house the private photographs taken by millions of other people. *See Zurcher*, 436 U.S. at 551.

IV. The Warrant Lacked Particularity

The government points to the geofence process as a means of redeeming an otherwise overbroad and unparticularized warrant. It says that the three-step process saves the warrant from unconstitutionality because the object of the search was clear and it was Google who “filtered” (searched) through records belonging to tens of millions of people. Yet the data to be searched and seized was the subject of significant back-and-forth between Google and the government, none of which involved a judge.

First, the search procedure was the product of repeated “engagement” between Google and the Justice Department. Tr. at 476. Google’s counsel engaged with the Computer Crimes and Intellectual Property Section to discuss “certain procedures that may be relevant for the way that ... Google will need to handle these types of requests, especially with reverse Location History being a relatively new type of request.” Tr. at 456-57; *see also* ECF 205 at 3-4. It rings hollow, therefore, to suggest that the government was unaware of how Google would interpret the warrant, how many people would be searched in step one, or that the method used would produce a high number of false positives. The affidavit contained none of this information, however, leaving it to the government and Google to follow the procedure they created behind closed doors. Such an understanding is also evident from the plug-and-play nature of the “go by” warrant that originated with CCIPS. *See* ECF No. 205 at 4.

Second, the warrant explicitly empowered the government to determine which users to search further in steps two and three. But the particularity requirement was designed to prevent that kind of officer discretion, as two federal courts in Illinois recently determined. *See* ECF No. 205 at 38-39. In fact, there were multiple emails and phone calls between the government and Google during step two because Google did not believe it was reasonable, as the government

requested, to provide additional Location History data for all 19 users identified in step one. *See id.* at 18-19, 39. The government responds, incredibly, that they had probable cause to seize stage two *and* stage three data for all 19 of these users, meaning two hours of Location History as well as full subscriber information for each account. *See* ECF No. 207-2 at 38-39. But their reliance on the “Playpen” cases is misplaced, *see* ECF 48 at 13-14, and Mr. Chatrie maintains that the government had no probable cause for any account. Furthermore, to read the warrant in this manner would make the entire three-step process superfluous, including the requirement that the initial two rounds of data be produced in “anonymized” form. It also guts the government’s argument that this process has any constitutional significance. The warrant therefore lacked particularity at each step of the way in violation of the Fourth Amendment.

V. The Good Faith Exception Does Not Apply

The government’s construction of *United States v. McLamb*, 880 F.3d 685 (4th Cir. 2018) is unsupportable. There, the government received a tip about the location of computer servers hosting a message board called Playpen that allowed visitors to upload and download child pornography. *Id.* at 688. The front page of the message board displayed “two partially clothed, prepubescent girls with their legs spread apart” and was “suggestive enough that Playpen’s content would be apparent to any visitor of the welcome page.” *Id.* Visitors then had to enter a username and passcode to access the message board. *Id.* Playpen had about 158,000 members. *Id.* Following the tip, the government seized the Playpen servers.

Once the government seized the servers, it tried to obtain identifying information for Playpen’s members, but could not because the members accessed the Playpen servers through a browser called Tor designed to conceal a user’s location and activity. *Id.* To get around Tor’s protections, the FBI used a digital tool that infected the Playpen servers. *Id.* Once an individual

accessed the infected Playpen server, the infected server sent instructions to the Playpen user's computer that allowed the FBI to remotely access information about the user's location and other identifying information. *Id.* at 688-89. The FBI sought a warrant allowing the FBI to install the digital tool on the Playpen servers for thirty days to identify Playpen members who entered a username and passcode within that thirty days. *Id.* at 689. The warrant accurately described the digital tool used and the scope of the intended search. *Id.* at 690.

At the time of the Playpen investigation, magistrate courts differed as to whether Federal Rule of Criminal Procedure 41 allowed a magistrate to issue a search warrant for searches that happened outside of the magistrate's district. *Id.* at 689. Concerned that its use of digital investigative tools exceeded the scope of the jurisdiction of the magistrate who authorized the Playpen search warrant, the FBI officers seeking the warrant discussed concerns about the legality of the Playpen warrant with attorneys within the Department of Justice and the FBI. *Id.* A federal magistrate in this district ultimately authorized the Playpen warrant, which allowed the FBI to use the digital tool to infect the Playpen servers and access identifying information about Playpen's members for thirty days. *Id.* Mr. McLamb was a Playpen member who accessed the Playpen servers within those thirty days. *Id.*

Mr. McLamb challenged the validity of the warrant and argued that *Leon's* good faith exception to the Fourth Amendment did not apply. The Fourth Circuit, however, applied the good faith exception using the traditional *Leon* analysis. The court observed that there was "no indication" that the magistrate acted as a rubber stamp or that the affidavit in support of the warrant lacked a substantial basis to determine probable cause. *McLamb*, 880 F.3d at 690. It is critical to view those findings in the context of the facts of *McLamb*. First, the warrant confined the search only to members of the Playpen message board who accessed the message board within a thirty-

day timeframe. The welcome page to the message board plainly indicated to all members that entering the site provided access to child pornography, meaning that all members who accessed the site were inherently suspected of engaging in criminal activity. And second, the warrant did not give the FBI liberal discretion in executing the warrant. Those facts clearly separate the Playpen warrant from the geofence warrant in this case.

As to the first point, the warrant in this case authorized a search that is unparalleled in its overbreadth, requiring Google to search the content of accounts belonging to numerous tens of millions of people. All but a few of those individuals inherently are unconnected to the investigation in this case. All but one⁵ of those individuals inherently are not suspects in this case. No search—digital or otherwise—can comply with the Fourth Amendment when it authorizes a global hunt through numerous tens of millions of innocent individuals’ sensitive data.

As to the second point, the warrant in this case left immense discretion to Google and the government to execute the search. *See supra* at 16-17. This discretion was baked into the warrant, something that has troubled other courts evaluating similar geofence applications. *See, e.g., Matter of Search of Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 746 (N.D. Ill. 2020) (denying geofence warrant application, even after amendment, and observing that, unlike geofence warrant, “there was probable cause to believe [in *McLamb*] that anyone reaching the dark website was involved in possessing or trading child pornography, so that agents’ discretion was in fact limited to seizing information about individuals as to whom probable cause was established”). The evidence before this Court paints the clearest picture yet as to just how much discretion the

⁵ The government’s assertions that a co-defendant could have been involved in the case potentially could have been a valid concern in the immediate aftermath of the robbery. But, once the police interviewed witnesses and watched the camera footage from the bank and the church—which the police did long before seeking the geofence warrant in this case, *see* Tr. at 623-25, there was no evidence to support a theory that the bank robber had co-defendants present within the geofence.

warrant left to Google and the government, which alone should preclude finding good faith.

The government very much wants to interpret *McLamb* as creating a new rule that cloaks police officers with good faith if they simply consult with an attorney before submitting a warrant. See ECF No. 207-2 at 41-43. *McLamb* adhered to the “traditional” *Leon* good-faith analysis. In discussing the question of the magistrate’s jurisdiction to issue a warrant for a search that would inevitably search computers outside of the magistrate’s district, the Fourth Circuit observed that one would expect an officer to have consulted with attorneys before seeking a search warrant that used “cutting edge investigative techniques.” *McLamb*, 880 F.3d at 690-91. But *McLamb* in no way gave a “good faith” pass to police officers who consult with attorneys before submitting a warrant. Such a rule would render the qualifications in *Leon* inapplicable in every federal case, as federal prosecutors routinely review and edit federal search warrant applications. And such a rule would also do nothing to check the government overreach apparent in this case. The law enforcement community worked hand in hand with Google to develop the discretionary process set forth in the geofence warrant in this case, see Tr. at 455-57, 476, and further has no qualms about the unprecedented scope of the search in this case. Thus, it is up to the courts to properly apply the Fourth Amendment in this case and sanction the government overreach in this case through suppression.

VI. Conclusion

The geofence warrant in this case was devoid of probable cause and particularity, casting a digital dragnet that searched tens of millions of people. In effect, it was a general warrant, so obviously deficient that this Court should find it void and suppress all the fruits thereof.

Respectfully submitted,
OKELLO T. CHATRIE

By: _____/s/_____

Michael W. Price
NY Bar No. 4771697 (*pro hac vice*)
Counsel for Defendant
National Association of Criminal Defense Lawyers
Fourth Amendment Center
1660 L St. NW, 12th Floor
Washington, D.C. 20036
Ph. (202) 465-7615
Fax (202) 872-8690
mprice@nacdl.org

_____/s/_____
Laura Koenig
Va. Bar No. 86840
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0881
Fax (804) 648-5033
laura_koenig@fd.org

_____/s/_____.
Paul G. Gill
Va. Bar No. 31461
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0870
Fax (804) 648-5033
Paul_gill@fd.org

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
RICHMOND DIVISION

UNITED STATES OF AMERICA)
v.) Criminal No.
OKELLO T. CHATRIE) 3:19CR130
-----) June 24, 2021
-----)

COMPLETE TRANSCRIPT OF ARGUMENT
ON MOTION TO SUPPRESS
BEFORE THE HONORABLE M. HANNAH LAUCK
UNITED STATES DISTRICT JUDGE

APPEARANCES:

Kenneth R. Simon, Jr., Assistant U.S. Attorney
Peter S. Duffey, Assistant U.S. Attorney
U.S. Attorney's Office
SunTrust Building
919 East Main Street, Suite 1900
Richmond, Virginia 23219

Nathan P. Judish, Assistant U.S. Attorney
U.S. Department of Justice
950 Pennsylvania Ave., NW
Washington, Virginia 20530

Counsel for the United States

Laura J. Koenig, Assistant Federal Public Defender
Paul G. Gill, Assistant Federal Public Defender
Office of the Federal Public Defender
701 E. Broad Street, Suite 3600
Richmond, Virginia 23219

Counsel for the Defendant

DIANE J. DAFFRON, RPR
OFFICIAL COURT REPORTER
UNITED STATES DISTRICT COURT

1 (The proceedings in this matter commenced at
2 10:10 a.m.)

3 THE CLERK: Case No. 3:19CR130, United States
4 of America versus Okello Chatrie.

5 Mr. Kenneth R. Simon, Jr., Mr. Peter S.
6 Duffey, and Mr. Nathan P. Judish represent the United
7 States.

8 Mr. Paul G. Gill, Ms. Laura G. Koenig, and
9 Mr. Michael W. Price represent the defendant.

10 Are counsel ready to proceed?

11 MR. SIMON: The United States is ready, Your
12 Honor.

13 MR. GILL: The defendant is ready, Judge.

14 THE COURT: Well, thank you all. Obviously,
15 we're here for argument. I want to be sure that you
16 all know that you should proceed as you are
17 comfortable with respect to COVID protocols. We have
18 lifted largely most of what we're doing.

19 If you approach the lectern, please, I still
20 think you should use our disinfectant in between
21 speakers just out of safety.

22 All right. I'm ready to hear argument.
23 Obviously, you have presented me with a good deal of
24 information. So I'll hear what you have to say.

25 MR. PRICE: Good morning, Your Honor.

1 THE COURT: Good morning.

2 MR. PRICE: At issue in this case is a
3 geofence warrant authorizing the search of numerous
4 tens of millions of people without probable cause for
5 a single one of them. It was a dragnet of epic
6 proportions. A general warrant. The very thing the
7 Fourth Amendment was designed to prevent.

8 It's obvious, or at least it should have
9 been, that valid warrants don't look like this.
10 There's a lot that's new about this case, but it's not
11 new that a warrant must be supported by probable
12 cause. It is not new that a warrant must be
13 particularized.

14 So it's striking that this warrant leaves
15 basic questions about what can be searched and seized
16 up to Google and the government to work out, to play
17 judge.

18 Good faith should therefore not apply. Valid
19 warrants do not look like this. It was so profoundly
20 overbroad, so lacking --

21 THE COURT: Sorry. I think you may have to
22 be a little closer to the microphone. I'm sorry. Or
23 pull it up. Yes, that's better.

24 MR. PRICE: I'm saying good faith should not
25 apply. That this warrant was so overbroad, so

1 profoundly lacking in particularity that no reasonable
2 officer could have relied on it.

3 As a result, Mr. Chatrie seeks this court to
4 hold the warrant unconstitutional, to suppress the
5 evidence obtained from it and all the fruits thereof.

6 I'd like to talk this morning first about
7 overbreadth, then particularity, and good faith.
8 First, I think it's very important to understand what
9 happened here at the beginning when the initial search
10 took place. When the government got a warrant
11 compelling Google to search the account records of
12 tens of millions of people. This was not something
13 that Google normally does. It's not something that
14 Google would have done absent the warrant. They were
15 acting in this case as a government agent compelled by
16 the warrant.

17 The search that Google did, the initial
18 search of numerous tens of millions of people, is
19 state action, no less than the seizure of the 19
20 accounts that followed or any of the steps, the
21 warrant after that.

22 Google ads do not work this way. Google does
23 not advertise and provide location information about
24 its customers to advertisers. Google's advertising
25 system doesn't sort through accounts in this manner.

1 The Sensorvault is, of course, not indexed
2 according to location. It is indexed according to
3 user account. And that is intentional. It's not that
4 Google flipped a coin and decided to do it this way.
5 It is irrelevant that they could have done it some
6 other way. Here it is organized by user account
7 because it is user data. It is not Google's business
8 records.

9 It is not enough to simply cite statistics
10 about Google's popularity or how many people have cell
11 phones to establish probable cause for the kind of
12 search that took place in this case.

13 There was not probable cause to search ten
14 million user accounts. There wasn't probable cause to
15 search 19 or 9 or even 1. There certainly wasn't
16 probable cause to seize the account records of 19
17 people who happened to be nearby.

18 The Supreme Court has already weighed in on
19 this, at least in the physical world. The idea that
20 you can search people just because they are nearby to
21 a crime was foreclosed by the Supreme Court in *Ybarro*,
22 *Ybarro v. Illinois*. It said, "Mere propinquity is not
23 enough. You must have probable cause with respect to
24 each person searched and seized."

25 Here the government did not have probable

1 cause to seize all 19 accounts after the initial
2 search.

3 THE COURT: Well, before you get there, I
4 want you to explain to me how the fact that the tens
5 of millions that were being searched were anonymized,
6 they are not identified users, how that does or does
7 not affect whether it's a search.

8 MR. PRICE: So, if you're talking about the
9 numbers that were attached to each individual's
10 account, those are unique identifiers that Google
11 provided. So they're not anonymized for this time
12 only. They are static identifiers associated with
13 people's location history Sensorvault accounts.

14 So aside from the fact that it is possible to
15 identify people based off of even a small segment of
16 data, it would be trivial for the government in this
17 case to obtain a subpoena, to go back to Google and to
18 say, Okay, now please tell us the subscriber
19 information for that anonymized number. They would
20 not need to go back to a court to seek a warrant for
21 that information once the Stage 1 data is turned over.

22 Those anonymized numbers associated with
23 individual accounts, frankly, are not truly anonymous.
24 It is very easy for the government to go back and get
25 that information without a warrant just using a

1 subpoena for subscriber records.

2 THE COURT: Okay.

3 MR. PRICE: We would argue, Your Honor, that
4 there was not -- we do argue that there was not
5 probable cause to search or seize even one person's
6 location history data in this case. There is no nexus
7 between the robber and location history. There is
8 some indication that the suspect had a cell phone, but
9 there is no indication, certainly not in the warrant,
10 that location history was enabled, something that only
11 about a third of Google users have.

12 There was a -- if you take Google's view of
13 it, there was a complex seven-step process that was
14 required to enable it. We would say it was probably
15 not that voluntary and knowing, but nonetheless, only
16 a third of Google users have this enabled. So it is
17 not enough to just say that the suspect had a cell
18 phone. It's not clear if that suspect, that cell
19 phone, was connected to Google. And it's not clear
20 that that cell phone, if it was connected to Google,
21 had location history enabled.

22 And, furthermore, given the uncertainty in
23 Google's method of estimating location, there was at
24 least another 32 percent chance that records would not
25 be available, that somebody would be located outside

1 of that geofence.

2 So I think the percentage is certainly below
3 30 percent, even if you just take it by statistics.
4 But we're saying that statistics are not enough here.
5 There needs to be something that directly connects the
6 warrant to the individual and the data being searched,
7 that generalities or statistics about Google's
8 popularity are not enough, that warrants must be --
9 probable cause must be individualized. And here it
10 was not.

11 THE COURT: To be fair, at least some courts
12 have relied on statistics at least to approve warrants
13 in the past; is that right?

14 MR. PRICE: If you're speaking about the
15 Illinois cases in particular, yes. One of the judges
16 in that case looked at the statistics as an important
17 factor in making that determination. But we argue,
18 Your Honor, that statistics alone can never be enough,
19 that there must be some individualized connection in
20 each case. Otherwise, it would be simple for the
21 government to recite those same statistics in every
22 single case to say the facts of the crime, to say that
23 there were cell phones involved, which is not much to
24 accomplish these days, and that Google collects a lot
25 of data, which is true. There would be no instance in

1 which the government couldn't obtain a geofence
2 warrant.

3 That is why the Fourth Amendment requires
4 that warrants be individualized, that proximate cause
5 be individualized.

6 The government mentions the possibility of
7 locating witnesses with the geofence warrant, but it
8 is pure speculation that there were witnesses that the
9 government had not yet identified. It seems that the
10 most relevant witnesses the government would have
11 already identified as being in the bank and/or through
12 the surveillance cameras that they used initially, and
13 that any additional witnesses found inside of
14 buildings nearby or apartment complexes would,
15 frankly, not have much to contribute. As one judge
16 noted, they would have to be able to see through their
17 walls, for starters.

18 The other thing I would say to that
19 specifically is that the warrant is clearly focused on
20 identifying a suspect, not on identifying witnesses.
21 Witnesses are mentioned only once in passing in the
22 context of some general information about how Google
23 works. The clear focus of this warrant, the entire
24 purpose of that three-step process, is designed to
25 find the suspect, not to identify witnesses.

1 The same can be said of co-conspirators,
2 which are never mentioned once in the warrant
3 application. And, in fact, investigators knew that
4 the suspect was seen alone coming to and from the bank
5 based on the surveillance video.

6 So, once again, there are no facts to support
7 this idea that the warrant was somehow being used for
8 witnesses or co-conspirators in addition.

9 THE COURT: Well, they're saying there's not
10 direct evidence, but they're saying because somebody
11 was using a phone, it's likely while they were in the
12 bank, at least there might be probable cause that
13 they're calling a lookout.

14 MR. PRICE: I'm sorry?

15 THE COURT: That they are calling a lookout.

16 MR. PRICE: So, in this case, it appears that
17 the government did an initial investigation and was
18 aware that there wasn't another individual in the
19 vicinity at the time. If that was the focus, it's not
20 impossible that it --

21 THE COURT: So what makes you say they did
22 the initial investigation and they knew there was not
23 somebody there?

24 MR. PRICE: I believe Detective Hylton
25 testified about the review of surveillance video they

1 did ahead of time, I believe it's in the CAST report
2 as well, showing one individual leaving their car,
3 going to the bank and back.

4 So if there was a concern that somebody else
5 dropped somebody off or picked somebody up, that was
6 already known at the time and most likely the reason
7 the warrant is not seeking information at all about
8 co-conspirators. They are not mentioned once.

9 So I think to argue that that was the point
10 of this warrant and that there was cause for that just
11 isn't supported on the record.

12 The whole point here, Your Honor, is that the
13 government had no suspects. They were conducting a
14 reverse warrant. They were starting with a bunch of
15 data and trying to find a suspect based off of that.
16 That is the reverse of how these warrants usually work
17 when the government goes to Google and asks for
18 information about a particular account or accounts or
19 at least identifiable accounts. Here the whole
20 process was turned on its head.

21 I'd like to shift gears to particularity, if
22 Your Honor doesn't have any questions about
23 overbreadth.

24 THE COURT: Well, I guess I want to confirm,
25 a lot of your arguments point out that the breadth of

1 the search is quite overpowering and that there were
2 other alternatives that the government could have
3 done. Is there a legal requirement that the
4 government use the less intrusive means to do an
5 investigation?

6 MR. PRICE: No. There's no requirement that
7 the government use the least intrusive means. I think
8 it is different, however, to use a geofence warrant in
9 the sense that it was more intrusive, but it is a way
10 of trying to take a shortcut. There are, and were in
11 this case, other avenues of investigation that the
12 government could have pursued, traditional lines of
13 investigation that they did not, and instead went to
14 Google and said, "Google, tell us who robbed the
15 bank." This was an easy way out in some sense.

16 THE COURT: So, Mr. Price, what I want to
17 understand is why you're saying the shortcut is
18 illegal. So there's no requirement for the least
19 intrusive means. So, you know, one would hope that
20 the government wouldn't waste resources in an
21 investigation.

22 MR. PRICE: I see.

23 THE COURT: So what makes this illegal? It
24 turns it on its head, but sometimes you turn something
25 on its head and that's a good thing.

1 MR. PRICE: So there's nothing illegal about
2 taking a shortcut per se, but this particular shortcut
3 was so far afield from anything that any other court
4 has signed off on. Certainly not the Supreme Court,
5 not any circuit court, and there are now two different
6 district courts, federal district courts, that have
7 agreed that these warrants are unconstitutional. And
8 so I think we're focusing not on the fact of a
9 shortcut, but that this particular shortcut is
10 completely unsupported by probable cause, and also
11 fails the particularity requirement of the Fourth
12 Amendment very badly at every step of the search.

13 Step 1, for example, goes back to this point
14 about basic questions being left unanswered and left
15 up to Google and the government to sort out. For
16 example, which database to search: Location History,
17 the Sensorvault versus Web & App Activity or Google
18 Location Services. This was something that clearly
19 the government had discussed with Google ahead of
20 time, and they were both aware of which databases were
21 going to be searched, but it wasn't in the warrant.

22 One reason it might not have been in the
23 warrant is because that would require specifying that
24 not all devices have location history enabled. So
25 just saying we're going to search Google and Google

1 has location information about people makes it seem
2 like everybody has this location information when, in
3 fact, a third of Google users have this enabled.

4 So leaving out that fact wasn't a small
5 thing. It very much dictated the overall scope of the
6 search, which, of course, then led to tens of millions
7 of people.

8 The warrant did not specify how to count if a
9 device is inside that geofence. So we know, for
10 example, from one of the Illinois cases, as well as
11 the Kansas case that just came out, that the
12 government is fully aware of this phenomenon of
13 display radius extending beyond the geofence.

14 In fact, in two other cases at least, the
15 government asked for -- explicitly told the judge that
16 the display radius will extend beyond the geofence and
17 that the government wants the data from everybody
18 whose display radius even touched the geofence.

19 Another way to do it -- I should say that
20 that method is likely to produce the largest number of
21 false positives. If you are looking for anybody whose
22 display radius intersects with that geofence in any
23 way, there's going to be a high percentage that some
24 of those people are going to never have been in that
25 geofence at all. In fact, we know that happened in

1 this case in at least one instance where somebody was
2 driving by and pulled in.

3 That's not the only way to do it. If you
4 wanted to minimize the number of false positives, you
5 could say, Return only the devices whose entire
6 display radius is inside the geofence. And that would
7 eliminate the possibility of false positives or at
8 least drastically reduce it.

9 So there are multiple ways of going about
10 this. And the government is aware of them. This
11 warrant did not specify. And it left it up to Google
12 and the government to sort out. The government says
13 that Google correctly interpreted what they were
14 intending, but none of that would be apparent to a
15 magistrate looking at the face of this warrant.

16 It was likewise unclear what that geofence
17 covers. There was no indication -- well, the
18 government says that it was unusually specific because
19 they identified a latitude and longitude and drew a
20 precise circle around that, but that area is a
21 congested urban area encompassing not just the bank,
22 but a church and roads, at least, plus the businesses
23 and apartments nearby that got swept in as a part of
24 that effective range.

25 So we know that the effective range of the

1 geofence in this case was not 150 meters, that it was
2 387 meters, more than twice the distance of the
3 original geofence, reaching not just that bank and the
4 church, but Hull Street and Price Club Drive, Ruby
5 Tuesdays, the Hampton Inn, A.M. Davis, Mini-Price
6 Storage, the Genito Glen Apartments, and the Rockwood
7 Village Senior Apartments. These are all places that
8 were effectively covered by the search that the
9 government requested here, none of which was ever
10 signed off on by a judge or a magistrate.

11 The information presented to the magistrate
12 showed a nice circle around the bank and the church
13 and didn't mention the possibility that it would
14 search people outside of that circle, and that the
15 things outside of that circle that might be searched
16 included apartment complexes, private businesses, a
17 hotel. These are constitutionally-protected spaces.
18 So that is significant.

19 And it is difficult to say that a warrant is
20 narrowly tailored when most of the devices identified
21 will have nothing whatsoever to do with the crime.

22 So even at Step 1, Your Honor, there were
23 significant basic questions left unanswered, left to
24 Google and the government to work out amongst
25 themselves.

1 In some instances, maybe that arrangement had
2 already been worked out, but it wasn't spelled out in
3 the warrant. That's for sure.

4 Step 2 and Step 3 were far more explicit
5 about the degree of discretion given to the
6 government. Step 2 explicitly says that the
7 government is going to narrow down the list and decide
8 which people will have additional contextual location
9 data revealed to the police. And that's the two hours
10 total and wherever those individuals happen to go
11 regardless of the geofence itself.

12 So it is at that stage completely up to the
13 government to decide who to search, who to get more
14 information from. Google pushed back. There was
15 certainly a back and forth between Google here that
16 illustrates this point very well, this negotiation
17 between the government and Google over what is a
18 reasonable amount of data to turn over in Stage 2.

19 But that is fundamentally a question that a
20 judge should be answering, that should not be left,
21 and cannot be left under the Fourth Amendment, up to
22 the government to decide on its own.

23 Step 3 --

24 THE COURT: Well, before you get there, I
25 have a question. So, with respect to Step 1 and the

1 identification of the 19, is there any dispute about
2 how those 19 numbers were identified or how Google
3 turned that information over to the government?

4 MR. PRICE: How it actually happened in this
5 case?

6 THE COURT: Well, you're saying it got down
7 to 19. So my question is, what is your position about
8 how it got down to 19?

9 MR. PRICE: I see. So our position is that
10 the search, the initial search, was of the numerous
11 tens of millions of people. The 19 was the data
12 seized from that search.

13 Now, there was a -- and I think is a question
14 here that relates to particularity about how Google
15 identified those 19 people. Google chose to say that
16 anybody whose center points of their location -- so
17 Google estimates location in a circle, and the
18 latitude and longitude points are simply the center of
19 that circle, wherever it happens to be.

20 The warrant in this case, the way Google
21 interpreted it, was that anybody whose center point
22 was inside the geofence was produced to the government
23 as a part of that 19. I'm saying that there were
24 other ways of going about doing that, which the
25 government is fully aware of, and it just wasn't

1 spelled out one way or the other.

2 So one privacy protective way of doing this
3 would be to say only return people whose display
4 radius was entirely within the geofence. In other
5 words, those would be much more precise readings
6 perhaps because of GPS as opposed to Wi-Fi or
7 cell-site location information. It would drastically
8 reduce the number of false positives. And, as I
9 mentioned once before, we know of one, and it's likely
10 there are at least five in this case of those 19. So
11 it wasn't -- this decision had consequences. And how
12 you count who's in the circle matters.

13 And if it matters to determining how many
14 sets of records you get to seize, then that's got to
15 be something that is clear in the warrant to begin
16 with. That can't be left up to officer discretion or
17 Google's discretion down the road. And we make no
18 distinction between Google and the government in this
19 case. They are acting together, according to that
20 warrant.

21 THE COURT: Is that what other courts have
22 done?

23 MR. PRICE: So, the Illinois cases were
24 decided. The opinions were issued there without the
25 benefit of the record that we are here. And the

1 Kansas case, which was just decided, appears to be
2 based on the records in the Illinois cases in terms of
3 the factual records.

4 So one thing that those courts did not
5 consider, perhaps because it wasn't known to them at
6 the time, was the scope of this initial search that
7 took place and how it differs, for example, from tower
8 dumps or other types of searches.

9 I think had that information been known to
10 those magistrate judges, that they would have perhaps
11 at least paid some attention to that fact. It was
12 just not before them. So I believe they were under
13 the impression that Google was able to search records
14 just in that location.

15 THE COURT: Well, I guess I was getting to
16 your comment about agency. That Google and the
17 government are -- you said Google is an agent of the
18 government. Have other courts made that finding?

19 MR. PRICE: So, we do not argue that this is
20 a private search. Google was -- which is that test
21 for a government agent. Google was acting according
22 to a warrant. It was compelled by legal process to
23 assist the government; therefore, the government was
24 not only aware of what Google was doing, but the
25 government was directing what Google was doing.

1 And if Your Honor is looking for a cite on
2 that, I would cite *Skinner v. Association of Railway*
3 *Labor Executives* for the point that if you -- as the
4 government requires, say, an employer, to conduct a
5 drug test of their employees, that even though that's
6 an employer, not the government, they're doing that
7 testing at the behest of the government according to a
8 statutory requirement, here a warrant, and therefore
9 it is government action.

10 So I would say that what Google was doing
11 here was government action. It was directed by the
12 government.

13 Steps 2 and 3. Step 3, like Step 2, gave
14 sole discretion to the government to decide which
15 users would have their identifying information
16 revealed. It is the same problem as in Step 2 in that
17 the warrant explicitly gives this power to the
18 government, which, of course, would have been obvious
19 to the government as well as the magistrate who signed
20 it.

21 There isn't a good response to that. And so
22 the government's answer to it is that the whole
23 three-step process doesn't matter at all, that this is
24 just show, and they are, in fact, entitled to Stage 1,
25 2, and 3 data on everybody identified in that initial

1 geofence.

2 The problem with that is that it guts any
3 argument that the three-step process has
4 constitutional significance. And while it might take
5 care of some of the particularity problems, it doubles
6 the problems with probable cause. To say that no, the
7 government actually had probable cause to search the
8 information of all 19 people for two hours wherever
9 they went, and to know exactly who they were, that is
10 unsupportable from the facts. There is no allegation
11 in the warrant or affidavit that other people that
12 might be identified here were involved in the crime
13 and would have evidence of criminal activity in their
14 accounts. So it really does lay bare the probable
15 cause problem if that's the answer to particularity.

16 It also would raise questions about whether a
17 magistrate looking at this warrant would reasonably
18 interpret that to be what it means. And so that is a
19 relatively new argument the government has advanced,
20 but I think if that is the route they choose to go, we
21 would have questions about whether that's an accurate
22 representation of what the warrant says.

23 Your Honor, the government also suggests that
24 the warrant be severed and that perhaps Step 2 and
25 Step 3 can be separated from Step 1. The problem with

1 severing in this case is that no part of this warrant
2 was supported by probable cause. There is nothing to
3 sever.

4 The de-anonymization doesn't matter for the
5 reasons that I explained a little bit earlier, that it
6 is possible to -- in fact, very trivial to identify
7 people based off of those Sensorvault ID numbers with
8 a mere subpoena. And that the whole process itself
9 was nothing more than a fig leaf designed to obscure
10 the magnitude of the search and seizure in this case.

11 If I can touch briefly on the question about
12 whether this was a search. I know that that's
13 something that the government has brought up as well.
14 We certainly believe that *Carpenter* is the best
15 analogy to this situation and that the Court should
16 not try and rely on relics like *Smith* and *Miller*,
17 outdated Supreme Court cases that are very far afield
18 from the facts here.

19 *Carpenter* was concerned with information that
20 reveals the privacies of life. Location history
21 reveals the privacies of life just like CSLI and GPS.
22 The government even got a warrant in this case,
23 perhaps recognizing that fact. But if we want to go
24 down that route and talk about *Carpenter*, and there
25 are two points that the government has made for why it

1 doesn't fit, one that it is voluntarily conveyed to
2 Google, and we are arguing that it is not truly
3 voluntary, that it is not truly shared in this same
4 sense that CSLI is not truly voluntary and shared with
5 the company.

6 Here the process -- the difference being it
7 is technically possible to turn on and off location
8 history; however, that process of turning it on and
9 off was highly deceptive and at the very least not
10 meaningful or informed. But even if the Court doesn't
11 want to go down that route, mapping and navigation
12 apps are an essential feature of modern smartphones.

13 This was something that the Supreme Court
14 recognized in *Riley* and in *Carpenter*, but when
15 explaining the importance of cell phones to people in
16 daily life, the Court recognized explicitly that
17 mapping and navigation services are a part of that.
18 And it's difficult to imagine a modern smartphone that
19 would not provide those types of services.

20 Here, I think, because of the way that Google
21 set up their opt-in process for location history,
22 because of the way that they warned users against
23 turning it off, saying their functionality of their
24 phone would be degraded, that things would no longer
25 work if they turned it off, there is a suggestion here

1 that this was essential to those basic features of the
2 phone. And it would not have been apparent to users
3 that they could turn it off and still use maps or
4 still use Google Assistant because Google didn't tell
5 them that. In fact, it told them the opposite. If
6 you turn this off, bad things are going to happen to
7 your phone.

8 So a reasonable user, looking at this, may
9 not understand what they're turning on. And Google
10 may warn them, and does warn them, against turning it
11 off, saying that a basic function of their phone is
12 going to be degraded if they do that. So, in that
13 sense, we would argue that, as in *Carpenter*, this
14 information was not voluntarily provided.

15 THE COURT: So, Mr. Price, I don't want to
16 ask this question in a confusing manner, but I
17 probably will. So, I think, for instance, this
18 argument, you are suggesting that Google is
19 essentially burying information about how to turn off
20 location history and suggesting that turning off
21 location history is problematic to the working of the
22 phone, and at the same time you're saying only a third
23 of folks have it turned on. So aren't those
24 propositions contradictory?

25 MR. PRICE: Well, I think the ease of turning

1 it on might explain some of the volume there. But
2 it's not necessary at the end of the day to find that.
3 I think even if some -- there are going to be people
4 in this world who actively want location history on
5 their phone. Perhaps Mr. McGriff wants it on his
6 phone.

7 I do not believe that doing so means that he
8 has no expectation of privacy in that data, that only
9 people that get duped into turning it on have an
10 expectation of privacy. I think, as Google explains,
11 this is user content. This is user property in the
12 same way that email and photos stored with Google are
13 user property and user content. And, therefore,
14 searching any bit of that, even a little bit, is a
15 search.

16 Google likens it to keeping a travel diary.
17 So if you are interested in this feature, and you turn
18 it on, Google says, Well, we're storing it in your
19 account. Just like you might create a map with
20 pushpins of where you've been, here's a digital
21 equivalent that you can go back, and you can look at,
22 and it's in your account, and it's accessible in the
23 same way as your email, as your photos. And they
24 treat it the same way. They treat it as user content.
25 According to Google, it's not a business record.

1 What business record -- companies do not
2 generally let customers delete their business records,
3 yet that is something that Google permits with
4 location history here. You can edit your location
5 history.

6 THE COURT: Right. So I understand those
7 points. So my question was the dissonance between
8 saying both that it is not voluntary to give it over
9 because it's so hard to turn off placed next to the
10 fact that two-thirds of folks don't have it on, which,
11 presumably, means they've turned it off.

12 MR. PRICE: Certainly some people are not
13 enabling location history. Some people may not have
14 occasion to or need to enable Google Assistant or may
15 be wise at this juncture to what location history is.

16 I think either way you look at it, under sort
17 of expectations of privacy test under *Carpenter* or as
18 user data, user content that is their property, it's a
19 search. So what I'm saying is there are two ways of
20 getting there. And it's not necessary to find that
21 somebody got duped in order to reach the conclusion
22 that the Fourth Amendment protects this information.

23 THE COURT: Okay.

24 MR. PRICE: The idea that -- the other
25 argument the government advances is that *Carpenter*

1 shouldn't apply because the length of time here was
2 shorter than the seven days that the Court was talking
3 about in *Carpenter*. I want to address that briefly,
4 first by noting that the reason the Supreme Court
5 chose seven days was not because it's a magic number.
6 It was the shortest amount of time of all of the court
7 orders for location history. So the shortest one was
8 for seven days. That's the one the Court considered.
9 And it is worth noting that in response to that court
10 order, the government only actually received two days'
11 worth of location information.

12 But the Court was clearly recognizing that
13 CSLI requires some stitching together in order to
14 paint this mosaic, to paint a picture of somebody's
15 daily life, because any one location point from
16 Southside location information is going to give only a
17 fairly rough estimate of where somebody is.

18 The Supreme Court talks about putting
19 somebody inside of a pie wedge that's, you know, a
20 couple miles wide. And we would say that CSLI, at
21 least a little bit of it, is probably enough to
22 identify somebody's neighborhood or the ZIP code that
23 they're in, but it is not going to be sufficient to
24 say which house they were in.

25 And so the Court was looking for a way to

1 say, Well, how much of this do we need before it
2 becomes a problem, before you can figure out where
3 somebody was and what they were doing? And that's how
4 we end up with seven days.

5 But the test, what they're fixated on, is
6 what that information reveals. How much of that
7 information do we need to get to the privacies of
8 life? And our argument here is that geofence data is
9 far more potent than CSLI.

10 Even a little bit of Google's location
11 history data is going to be sufficient to identify
12 somebody inside of their home or a church or another
13 business nearby, and you don't need as much data to
14 get the same sort of information.

15 I would also add that because of the
16 precision involved here, because it does rely on GPS,
17 and it does pinpoint people inside of their homes, as
18 we demonstrated to the Court, that there's an
19 additional consideration here that wasn't present in
20 *Carpenter*, which is monitoring people inside of
21 constitutionally-protected spaces.

22 The Supreme Court has been clear on this a
23 number of times. The best examples are *Kyllo* and
24 *Karo*, K-Y-L-L-O and K-A-R-O. In *Kyllo*, the Court
25 looked at the use of new technology, the thermal

1 imager. Even though it was only trained on a house
2 for a few moments, a couple minutes at most, law
3 enforcement was able to determine what was happening
4 inside that house, whether there were people inside
5 that house. And that was enough for the Court to say
6 it's a search. There is something special about homes
7 under the Fourth Amendment. They are the first among
8 equals, so to speak.

9 And using technology to pierce those walls
10 and see what's going on inside and learn information
11 you wouldn't otherwise be able to learn is a search,
12 even if you do it for a little bit of time.

13 Karo was the same sort of case with an
14 electronic beeper that had been hidden inside of a
15 drum of chemicals inside the back of a car. That car
16 was driven onto private property. And then the
17 government was able to tell when that drum of
18 chemicals was moved.

19 And that was, once again, information that
20 the government would have been unable to know
21 otherwise because it was occurring within a
22 constitutionally-protected area that they didn't have
23 a warrant to go and search. And the Court said you
24 can't achieve by other means what you wouldn't be able
25 to otherwise do, that the use of technology doesn't

1 give you a free pass. It, in fact, invites more
2 scrutiny. And that's been the lesson ever sense,
3 especially with *Jones* and *Riley* and *Carpenter*.

4 So I would also say that the government had
5 to know it would get this information through either
6 the effective range of Step 1, or, clearly, in Step 2
7 when people are going about their business and coming
8 home, or going to home, and then we see that dot just
9 sitting right on top of their house.

10 That was something that should have been
11 obvious to anyone asking for this sort of warrant that
12 even if it didn't get constitutionally-protected
13 spaces in Stage 1, it was certainly going to get them
14 in Stage 2. But, once again, even in Stage 1, the
15 geofence encompasses the entirety of a church in
16 addition to the bank. And so I don't think it's for
17 nothing that the vast majority of data points
18 attributed to Mr. Chatrue, all but two, from location
19 history put him either inside the church or right next
20 to it in a car.

21 And so the idea that this can't reveal
22 information about people in constitutionally-protected
23 spaces is false. And it should have been obvious that
24 that was what was going to go happen to anyone who was
25 seeking such a warrant.

1 THE COURT: So are you asserting at all that
2 any of the data turned over placed Mr. Chatrie in his
3 house?

4 MR. PRICE: No. We're not asserting that the
5 data here placed Mr. Chatrie in his house, no.

6 THE COURT: Okay.

7 MR. PRICE: The government argues that this
8 is just like the search of one place. That they name
9 Google. They said they put down Google's corporate
10 address, that that's one place, and it's just like
11 searching one place. They get to search everywhere in
12 that one place.

13 I think that's a sleight of hand. It ignores
14 the mechanics of the search here. This was not like
15 searching one house. This was like searching
16 10 million houses, or safe deposit boxes may be even a
17 better example. If you want to look at what this
18 might be like in the physical world, it would be like
19 going to a bank and asking the bank, saying, We're
20 looking for a weapon. We think it's in one of your
21 safe deposit boxes. We would like you to open up
22 every single safe deposit box in the country and look
23 for this weapon.

24 That is the equivalent of what happened here.
25 It wasn't a search of one place. It was a search of

1 10 million places or numerous tens of millions of
2 places. And to try and say that this was just a
3 search of one place at Google's headquarters is to
4 ignore the nature of this data, to ignore that it
5 belongs to numerous tens of millions of individuals
6 and not to Google.

7 Lastly, Your Honor, I'd like to discuss good
8 faith briefly, unless you have additional questions.

9 So we argue that *Leon* should not apply. That
10 three, at least, of the exceptions that *Leon*
11 specifically identifies apply in this case. And all
12 three exceptions relate back to the probable cause and
13 particularity problems that we've discussed so far,
14 that the judge in this case, the magistrate in this
15 case, acted -- abandoned his judicial role, acted as a
16 rubber stamp. Looked at this warrant for 15 -- 30
17 minutes behind closed doors. Didn't ask a single
18 question before signing off on it. Didn't care to ask
19 how many people might be searched or how the
20 government would handle the selection process in
21 Stages 2 and 3.

22 This was a warrant that doesn't look like any
23 other warrants yet the judge asked no questions. This
24 was a warrant that explicitly gave the government the
25 authority to decide who to search and did not ask any

1 questions.

2 These are basic questions about probable
3 cause and particularity. But instead of addressing
4 them as magistrate judges in Illinois and Kansas did,
5 the judge here simply signed off and left everything
6 up to Google and the government to work out.

7 The warrant was so lacking in probable cause,
8 so overbroad, that no officer could reasonably rely on
9 it. There wasn't probable cause to search one
10 person's Google account. There certainly wasn't
11 probable cause to search 19, and there was not
12 probable cause to search tens of millions. Even if
13 the government didn't understand that it was going to
14 search numerous tens of millions of people, it
15 certainly would have understood that the search they
16 had in their mind was still going to bring in a vast
17 majority of people who were not involved in the crime
18 at all, for whom they had no probable cause to search
19 and would not have been able to get a warrant to
20 search under other circumstances.

21 It was only because of this fig leaf of a
22 three-step process that made it seem like this is
23 something that's okay. Looking at it, it is
24 plainly -- plainly they had no suspects. They did not
25 have probable cause to search Mr. Chatric's account or

1 anyone else's. This was a fishing expedition. That
2 should have been known to anybody looking at this
3 warrant.

4 Likewise, it was so obviously deficient in
5 particularity that it also fails under *Leon*. Giving
6 this sort of discretion to law enforcement alone is
7 what the particularity requirement was designed to
8 prevent, to make sure that every petty officer didn't
9 have the authority to go rummaging through everyone
10 else's private papers, yet that is exactly what
11 happened here.

12 No, it would not be objectively reasonable to
13 believe that officers would have unbridled discretion
14 to search through the location history of millions of
15 people, especially when they didn't have any suspects.

16 So, Your Honor --

17 THE COURT: Well, let me ask you this because
18 a not insignificant amount of your briefing suggests
19 that this task force officer really didn't know what
20 he was doing, didn't know that what he was asking for
21 asked for more specific information when he got a
22 group of 19 in the first instance, and that he should
23 have known it was his requirement to narrow it down.
24 So I'm trying to figure out how that feeds in to what
25 you're saying about the discretion should not go to

1 the government when it appears that you're saying it's
2 Google who's doing all this, or at least most of it,
3 the thought processing and the narrowing down. Is
4 that entirely dependent on your argument that Google
5 is an agent of the government so they functionally are
6 the government even if this task force officer really
7 didn't understand how the process worked?

8 MR. PRICE: Right. So I think it's
9 significant that the government and Google had worked
10 out some of these details ahead of time. Even if
11 Officer Hylton didn't know all of them personally,
12 this was a go by.

13 THE COURT: When you say "Google," you're
14 talking about the corporate level interaction with the
15 Department of Justice? Is that what you mean?

16 MR. PRICE: Well, initially, it was developed
17 between CCIPS and Google's legal team, and then here
18 we had specific back and forth with respect to this
19 warrant as well.

20 So, yes, we're saying that Google was
21 functionally acting at the government's discretion
22 here, that Google was compelled to act as a result of
23 that warrant. Google was attempting to follow that
24 warrant. That's what they were saying in response to
25 Detective Hylton when he asked for all 19 at Stage 2

1 twice. And Google said, Well, we're complying with
2 this warrant that we're legally obligated to follow,
3 and you're not following the process.

4 So I think it reiterates that Google is
5 acting in a manner that is compelled by law, that they
6 are trying to, at least, follow the letter of that
7 warrant, even if the government wasn't. But that,
8 more generally, the questions that Detective Hylton
9 maybe had about this process are attributable to the
10 fact that this is not a normal process. This is not
11 something they receive training on. This is not
12 something that there are policies about. This is not
13 something that is normally done. And so one would
14 expect, then, there to be some confusion and questions
15 about how it is executed.

16 This is a reverse warrant. This is not
17 something like Detective Hylton or others would have
18 normally seen or used when you're obtaining
19 information about an individual, an individual account
20 with a warrant that identifies that account. That is
21 the way that this normally happens.

22 THE COURT: Doesn't this record show that he
23 had done three geofence warrants before? Am I wrong
24 about that?

25 MR. PRICE: I don't believe it was three

1 before, but --

2 THE COURT: I thought it was one federal and
3 two state.

4 MR. PRICE: I thought it was at least one,
5 maybe two.

6 THE COURT: So anyhow, he's done it before.
7 So it's not normal, but it's not new either, right?

8 MR. PRICE: I suppose that is fair. It's
9 fairly new. Even if this is only the second or third
10 time. This is only the first time that we've actually
11 had an opportunity to discuss this stuff in front of a
12 judge. So all of the decisions prior to this, as Your
13 Honor knows, were done *ex parte* based solely on the
14 records available from this case at the time and
15 whatever the government submitted. We still don't
16 actually have copies of the warrants in any of those
17 cases. They're all still under seal.

18 THE COURT: I just want to ask sort of random
19 questions to make sure I don't forget them.

20 The United States argues that as far as the
21 opt-in process, that this court should be bound by the
22 testimony of Mr. McGriff because he was able to
23 testify to the specific time frame under which Mr.
24 Chatrie would have been using his phone, and so that
25 your expert, who spoke about different opt-in trees,

1 consent flows, that I should disregard those. Are you
2 in agreement with that?

3 MR. PRICE: No, Your Honor. I think
4 Mr. McGriff was able to identify the date and time at
5 which location history was enabled, which is only
6 information that Google has, but Mr. McGriff was not
7 able to say explicitly which consent flow or how it
8 would have appeared to somebody like Mr. Chatrie. And
9 we put forth both of those possibilities. At the time
10 there was the "saves a private map" language and the
11 "saves where you go with your device" language, which
12 happened -- the change happened close in time to when
13 location history was enabled. Mr. McGriff was unable
14 to say exactly which one because he didn't know the
15 operating system and software -- sorry. The operating
16 system version that was running on Mr. Chatrie's
17 phone.

18 So I think the implication there is that
19 there's some sort of rollout process, and that it
20 doesn't all happen literally at once like flipping a
21 switch.

22 So, I guess, taking a step back from that,
23 what I would say is that either of those two consent
24 flows take you to the same place. That neither of
25 them describe location history in a sufficient way to

1 give users informed consent over what they were
2 agreeing to. In both instances it was less than a
3 sentence worth of text that somebody was required to
4 look at. And in the case of Google's Assistant, it
5 was bundled with two other choices about enabling
6 Voice & Audio Activity as well as device information,
7 both of which would have been necessary to run Google
8 Assistant, according to Google.

9 So, in either instance, whether you want to
10 go with "saves a private map" or "saves where you go
11 with this device," we do not believe that that would
12 be sufficient to give informed consent. And we do
13 believe that the testimony that Mr. McInvaille
14 provided to the Court and the research that he
15 provided or he was able to present to the Court, which
16 the government did not contradict and Google did not
17 contradict, I think both Google and the government
18 were asked if they had any information to contradict
19 Mr. McInvaille's testimony, and they said no to both.

20 THE COURT: All right. So, you mention a
21 couple of times, perhaps more than that, both in
22 argument and in briefing, that through the steps that
23 this warrant proceeded from, Step 1 to 2, to Step 2 to
24 3 with no supervision, is it the case that by
25 requiring an officer, an executing officer or law

1 enforcement officer, to have each return at Step 1
2 reviewed, and then before you go on to Step 2 or at
3 Step 2, would that solve the constitutional concerns?

4 MR. PRICE: I think it might alleviate one
5 concern with particularity. What it does not address
6 is the Step 1 confusion, let's put it that way, about
7 what is to be searched and seized in the first
8 instance, which database is going to be searched, what
9 are you counting, what area are you actually
10 searching. All of those at Stage 1 were still left up
11 to Google and the government to decide.

12 So Stage 2 and Stage 3 is more obvious
13 because it explicitly leaves that decision up to the
14 government. But Stage 1 is just as deficient in
15 particularity. Even if it doesn't explicitly leave
16 that decision up to Google and the government, it
17 effectively did.

18 THE COURT: So I want to confirm, you say
19 that the government and Google had agreed to certain
20 parameters, for instance, searching Sensorvault. Is
21 it the case that my record shows that the government
22 agreed to that or that Google just did that knowing
23 that the other repositories wouldn't have responsive
24 information?

25 MR. PRICE: So I don't think we have as much

1 visibility as we would like into the origins of these
2 warrants with CCIPS and Google discussing, but I don't
3 think that ultimately matters to the outcome here.

4 THE COURT: So that's what I was trying to
5 get to before. When you're saying that there's a
6 discussion between Google and the government about
7 what is going to be searched, i.e., Sensorvault,
8 you're not saying that Task Force Officer Hylton had
9 that discussion with anybody at Google. You're saying
10 Google legal office had that conversation with CCIPS.

11 MR. PRICE: It appears that that's what
12 happened. What I am saying at the end of the day is
13 that a judge didn't say it one way or the other, which
14 is what's required. I don't know who suggested what
15 first, but the information was never presented in the
16 warrant or application. It never mentions location
17 history once, and that's a fundamental decision about
18 what gets searched that should have been up to a judge
19 and not some combination of Google and the government.

20 THE COURT: At any level, corporate level --

21 MR. PRICE: Correct.

22 THE COURT: -- or with this particular
23 warrant.

24 So, with respect to the --

25 MR. PRICE: I was just going to go grab a

1 note.

2 THE COURT: You can go ahead. Maybe it
3 addresses some of my questions.

4 MR. PRICE: First, I wanted to add to Your
5 Honor's question about which consent flow would have
6 been operative at the time. Mr. McGriff on pages 295
7 to 297 of the transcript acknowledges that he was
8 uncertain of what language was baked in at that point
9 in time into the phone. So that's the source of the
10 uncertainty as to which particular language was or
11 would have been seen.

12 And as we've mentioned, either way it
13 shouldn't effect the outcome, I think, too, too much.
14 The consent flow issue is also interesting here
15 because we talked about what happens when you attempt
16 to turn it off, and those sort of warnings that you
17 get. However -- and this speaks to the voluntariness
18 point as well -- merely turning it off does not delete
19 the stored information that Google may have. So even
20 if I turned off my location history right now, if I
21 didn't actively then go and delete everything, the
22 search would still run against me as everyone else.

23 Similarly, even if you delete that
24 information, it doesn't actually turn off location
25 history. So enabling or when Google enabled an auto

1 delete feature long after the facts of this case, you
2 might be mistaken for thinking that that would have
3 some effect on the collection of location history. In
4 fact, it does not. And it further adds to the
5 confusion here.

6 And lastly, we'd say that the consent flow
7 isn't as probative of the expectations of privacy as
8 the way that Google treats that data. So Google
9 considers location history to be user content. It
10 stores it as user content in user accounts. That's
11 why their system is indexed this way because it
12 belongs to the users. It is not Google's business
13 record. And whatever weight the Court wants to put on
14 that consent flow, it doesn't change the fact that
15 that is individual data, the modern equivalent of
16 their private papers stored in an individualized
17 account.

18 THE COURT: All right. So my first question
19 is, with respect to good faith, if Task Force Officer
20 Hylton had gotten even one geofence warrant before and
21 there is even one case that says that it's
22 permissible, why doesn't that satisfy good faith?

23 MR. PRICE: There was no case saying it was
24 permissible at the time. All of these Illinois cases
25 came after this case. In fact, they were using some

1 of the early record in this case to base their
2 decisions on. So there was no court decision on this.

3 In fact, I would say the -- if anything,
4 however, the Supreme Court's focus on probable cause
5 and particularity for the last few hundred years would
6 signal to a reasonably well-trained officer that they
7 need both probable cause supporting their warrant and
8 that it must be particularized. Both of those things
9 were glaringly absent here and that should have been
10 apparent on its face to both Detective Hylton and to
11 the magistrate who signed it. And the fact that
12 Detective Hylton had done this once or twice before, I
13 don't think changes that whatsoever. Especially, if
14 there was no pushback or --

15 THE COURT: We don't know, right? All we
16 know is that he had at least one approved, right?

17 MR. PRICE: We know, Your Honor, that Google,
18 at least, reports having received quite a few of
19 these. And it is interesting to note that this is the
20 first case where it's actually being tested in court.
21 Part of the reason that happens is because the
22 geofence warrants are not always successful in
23 identifying a suspect.

24 There was a different arson case being
25 investigated in North Carolina where the geofence

1 warrant was reported in the news but failed to
2 actually identify a suspect. And that could have been
3 for any number of reasons, but one good one would be
4 he was one of those two-thirds that did not have
5 location history enabled.

6 There's a large number of these warrants that
7 do not produce results. It is a fishing expedition.
8 You're not always going to get a fish every time.

9 THE COURT: So what of the cases that we now
10 have do you think I should look to most closely when
11 reviewing your position?

12 MR. PRICE: I'm sorry? Which --

13 THE COURT: Which of the reported or
14 unreported but available geofence cases that we now
15 have is the one or two that you think I should look to
16 most closely when reviewing this case?

17 MR. PRICE: I think Judge Weisman's opinion
18 and Judge Fuentes's opinion are both very informative
19 and well reasoned based on the facts that were
20 available to them. I would say none of these opinions
21 attempt to grapple with the scope of the search at
22 Stage 1, which, simply, I don't believe was apparent
23 at the time. But of the four that are out there now,
24 certainly Judge Weisman and Judge Fuentes have very
25 strong reasoned opinions when it comes to probable

1 cause and particularity.

2 THE COURT: All right.

3 MR. PRICE: Thank you very much, Your Honor.

4 THE COURT: I think those are my questions
5 for now.

6 MR. PRICE: Okay. Thank you very much.

7 THE COURT: Okay. Thank you.

8 All right. So I think this is a good time to
9 take a brief break. And we'll be back in 15 minutes,
10 which takes us to 11:40. All right? And we'll begin
11 with the government's position. We'll take a recess.

12 (Recess taken from 11:25 a.m. to 11:40 a.m.)

13 THE COURT: All right. I'll hear from the
14 government.

15 MR. JUDISH: Thank you, Your Honor. Nathan
16 Judish on behalf of the United States.

17 As we've argued consistently in this matter,
18 there are three separate and independent reasons why
19 this court should deny the defendant's motion to
20 suppress.

21 First, that the defendant had no reasonable
22 expectation of privacy in any of the information the
23 government obtained from Google.

24 Second, that the government obtained it
25 pursuant to a valid warrant.

1 And third, that investigators relied on the
2 warrant in good faith.

3 I think the logical way to talk through this
4 is to start with the question of a reasonable
5 expectation of privacy. So I will begin with that.

6 I think that whether someone has a reasonable
7 expectation of privacy turns in large part on the
8 nature of the disclosure. And the Supreme Court has
9 repeatedly held that one retains no reasonable
10 expectation of privacy in information voluntarily
11 disclosed to a third party.

12 And so I think it's really important to take
13 a close look at the notion of the services Google
14 provided here. And, essentially, Google's function
15 here is as a location-based service provider. And so
16 the real question is, what does a user of
17 location-based services disclose to a location-based
18 service provider in order to obtain location-based
19 services? And I think the answer is pretty clear.
20 The user discloses location information.

21 So consider what Google actually -- the
22 services they -- the nature of the services they
23 actually provide to the defendant. The main service
24 that you disclose your location for is to get
25 recommendations with your commute; driving

1 instructions and such.

2 So what does that mean? This isn't -- this
3 isn't a case of someone just having Google store their
4 location in order to create a map, although that may
5 be one thing that they do, but you also disclose your
6 location so Google, as a service provider, can help
7 you get from one place to another quickly. And that
8 involves not only Google knowing where you are and
9 where you're going, but also Google knows where
10 everyone else is going at the same time as well. So
11 what you have, generally, is vast numbers of people
12 disclosing their location to Google from which Google
13 can assess where they are and how fast they're going
14 and from which Google can spot traffic problems and
15 tie-ups, one way or another, and then Google sends out
16 advice.

17 You know, I'm driving down here last night on
18 I-95 and Google says there's an accident up ahead.
19 You can save 21 minutes by taking another route.
20 Google doesn't know that just from my location.
21 Google knows that from the location information it's
22 getting from everyone.

23 So what we see here is that Google is using
24 everybody's location to essentially provide useful
25 advice to everyone. This is not people keeping their

1 location secret or private or anything like this.
2 This is a big communal effort to pool location
3 information in a way which lets Google then provide
4 generally beneficial advice to everyone. And so it's
5 just not kept to yourself.

6 And it's true that Google doesn't normally
7 disclose any particular individual's advice [sic] to
8 others in giving out that advice, but it's clear from
9 controlling Supreme Court precedent in the *Miller* case
10 that that doesn't matter. The point is, users
11 disclose their information over to Google, and then
12 Google, you know, is free to use that information and
13 act on it, and so on.

14 THE COURT: Well, I do think you have to
15 address the fact that, you know, *Miller*, and what
16 we're discussing here, are facts of a different order.
17 Right? So it is not the case, or I guess I should ask
18 you, do you think that folks are knowingly or
19 willingly giving over information about their location
20 that Google updates every two minutes? I just don't
21 think you can say that.

22 Most folks don't know, I think, that Google
23 is keeping this on a two-minute loop.

24 MR. JUDISH: Well, as an initial matter, you
25 can deduce just from the driving services that they're

1 looking at your location pretty much directly. I
2 mean, it is really like there's something going on
3 right now, and they act on it right now. Google has
4 to know your information right now and act on it.

5 And beyond that, I mean, Google says, and
6 it's also clear that we know from the *Smith v.*
7 *Maryland* case that it doesn't matter whether you know
8 or not that they're going to store information. The
9 fact that you disclose it is sufficient.

10 So in *Smith*, you know, there was an argument
11 that, well, customers didn't know that the phone
12 company would actually keep records of that
13 information, and there it didn't matter.

14 But, you know, as far as the -- and in
15 addition to sort of being able to tell from using the
16 service --

17 THE COURT: So I'm going to stop you there.
18 Are you saying there is no aspect of the facts in
19 either *Smith* or *Miller* or our case that differentiates
20 them? The numbers we're dealing with here, if they
21 are exponentially more than those in the other cases,
22 that it doesn't matter?

23 MR. JUDISH: I mean, I don't think the
24 frequency of storage makes much difference. I mean,
25 you can store -- I would say, one, are users aware of

1 it? Well, they certainly can be because unlike with
2 the phone company where you can't really see all the
3 information the phone company has traditionally stored
4 about you, your records are available to you at
5 Google. You can log on, look at your account. You
6 can go and see everything that they have stored. So,
7 that's, I mean --

8 THE COURT: So, I'm going to say, sir, you
9 are speaking really quickly. And I can see that my
10 reporter is trying to keep up with you, but I can hear
11 everything you're saying. We just have to be sure
12 that the record follows, too.

13 MR. JUDISH: I will try to slow down, Your
14 Honor.

15 THE COURT: Okay. Thank you.

16 MR. JUDISH: So, anyway, with Google you can
17 see everything that you see stored. And so, you know,
18 users can be aware of exactly what there is.

19 And, in addition, once you agree to Google
20 saying "saves where you go with your devices," I think
21 the frequency of it just doesn't make that much
22 difference after that.

23 I mean, you can store whether it's -- you
24 know, because people move quickly. In order for that
25 to work well, they have to store relatively often.

1 And just a small, you know, small intervals, I think
2 just don't have a great deal of significance.

3 So, another, I think, noteworthy aspect of
4 how Google uses the information is in their
5 advertising and the radius targeting that they do.

6 So Google, from location history, they
7 make -- to begin with, they make certain inferences
8 about your interests, and they target useful
9 advertisements to you based on that. Again, that's
10 more than just a storage service, but it goes beyond
11 that. The radius targeting part is they will sell to
12 customers or to advertisers the ability to place
13 advertisements to people within a certain radius. And
14 then in order to measure the effectiveness of that,
15 they will subsequently examine location history
16 information of users to see whether they have actually
17 visited the particular store that was doing the
18 advertising.

19 So that's -- I mean, that's really
20 essentially the equivalent to a geofence because it's
21 around the particular store that has done the
22 advertising. So Google is doing with its own data
23 that users provide to it, and they're quite up front
24 about this, something which is remarkably similar to
25 geofencing, you know, a geofence around the individual

1 advertiser's stores in order to, you know, provide
2 this store visit conversion statistic to the users.

3 THE COURT: Yeah, but they don't identify --
4 I mean, they explicitly don't tell the advertisers who
5 they are identifying.

6 MR. JUDISH: They don't.

7 THE COURT: So it's not generally the same.

8 MR. JUDISH: Well, again, the equivalent for
9 the purpose of showing that the information is
10 disclosed to Google, and it's really not necessary for
11 the third-party doctrine for Google to, then, normally
12 in the ordinary course of business disclose it to
13 others. Just like a bank doesn't normally disclose
14 your expenses to third parties outside the bank, but
15 what you look at is what is disclosed to the party
16 from whom the government got information.

17 And I think it's clear from that advertising
18 function that you are disclosing your location
19 information to Google.

20 And then that's just -- this so far has just
21 been analyzing the nature of the service Google
22 provides. It's also worth looking more carefully at
23 the opt-in process and what it takes.

24 And as Mr. McGriff pointed out in his
25 testimony and affidavits, it really takes a

1 multiple-step process before Google knows -- will
2 ultimately store someone's location history.

3 So you start off with a cell phone. It's
4 just a little electronic device sitting there. It
5 doesn't know its location unless you first turn on the
6 feature for your cell phone to get it to determine its
7 location. So that's the first step you have to take.

8 Now the phone knows its location, but it's
9 not telling anyone because you haven't told it to
10 share that information with anyone. So the next step
11 you have to take is you have to tell it to -- adjust
12 your phone so it will share that information with apps
13 so apps can provide you location-based services. So
14 you do that and now the information may be shared with
15 a Google app.

16 Well, okay. Google -- that's fine. Google
17 may be able to use that location information, but it
18 still doesn't know who you are because you haven't
19 signed on to the Google app on your device. So that's
20 another step you have to take before Google will end
21 up with location information.

22 Okay. So you sign in on your device and now
23 Google can determine your location.

24 THE COURT: Slow down.

25 MR. JUDISH: Slow down. This is still too

1 fast? All right.

2 So now Google can determine your location
3 information. And it still won't store that
4 information unless you take the additional step of
5 opting in to location history. So all those things
6 are affirmative steps you have to make before Google
7 will store your location history.

8 And so then I want to address, because we
9 have it in such detail, the actual opt-in process for
10 location history. And here I think it's important --
11 I just want to say a bit about the record.

12 So, McGriff testified first through a sworn
13 affidavit, and then he affirmed with his testimony
14 that he stuck by his affidavits. This is from
15 Government's Exhibit 3C at paragraph 7. Under the
16 supported consent flow as of July 9, 2018, across all
17 applications and services and across all Android
18 devices and operating systems a user who opted in to
19 LH, location history, either directly from within
20 device settings or when attempting to use a feature
21 powered by LH, such as features within the Google Maps
22 application.

23 THE COURT: So when you read, you're even
24 faster, which is what every human being does.

25 MR. JUDISH: Would be presented with an

1 opt-in screen containing the following text.

2 So McGriff said, you know, this was across
3 all devices, across all operating systems. This was
4 necessary opt-in language. And what he said also in
5 his testimony was that this consent copy has been
6 static. That's on page 271 of the transcript. He
7 said there was possible additional descriptive copy
8 which could change, and that, the descriptive text, he
9 personally could not be sure about, but the actual --
10 this actual consent copy, he said, was static and was
11 essential in order to opt-in. So that's why I think
12 this court can look at the -- this consent opt-in he
13 presented in his affidavits and be sure that that is,
14 in fact, what he would have seen when he -- what the
15 defendant would have seen when he opted in. And what
16 that says is "saves where you go with your devices"
17 and "this data may be saved and used in any Google
18 service you are signed in to give you more
19 personalized experiences. You can see your data,
20 delete it, and change your settings at
21 account.google.com."

22 So, I think this text really gives the core
23 of what you're agreeing to. It says that Google's
24 going to save where you go with your devices, and it
25 says that Google can use that is information to

1 provide you with services. And that's what happens
2 with Google's location-based services. And to that
3 you're given a choice, either "no thanks" or "turn
4 on," and we know because the defendant opted in on
5 July 9, 2018, that he did, in fact, say to turn it on.

6 All right. So, I think all of this shows
7 that the defendant did, in fact, voluntarily disclose
8 his information. What does the law say here? Well,
9 the principle that -- over and over in every single
10 case, the Supreme Court that has addressed it, it's
11 held that one retains no reasonable expectation of
12 privacy in information voluntarily disclosed to third
13 parties.

14 To be clear, this is not just about business
15 records. The defendant keeps characterizing --
16 they're saying, well, these are not business records.
17 I don't think it -- I mean, I think Google is clearly
18 using the records for a business purpose, but the
19 third party doctrine does not depend on whether or not
20 something is a business record. It applies to
21 conversations you do in the presence of others, for
22 example. We know that from the *Hoffa* case.

23 The Supreme Court has affirmed it in multiple
24 other contexts. We have it for everything you give to
25 an accountant. That's the *Couch* case. We have it for

1 telephone dialed number information in *Smith v.*
2 *Maryland*. We have it for bank records in *Miller*. And
3 the Supreme Court has never, ever rejected that
4 principle.

5 Now, *Carpenter*, the Supreme Court, obviously,
6 did not find it applied, but the key point about
7 *Carpenter* is that the reason it didn't apply is that
8 the Supreme Court found that the cell-site records
9 were not voluntarily disclosed to the phone company.
10 And it did that for three reasons. And if you look at
11 those three reasons, none of them apply to the
12 location history or location information disclosed to
13 a provider of location-based services.

14 First, the cell-site records are collected
15 automatically if you just power up the device. No
16 other affirmative action is necessary. So if you want
17 to make phone calls, send texts, you get a cell phone.
18 It just happens behind the scenes automatically, and
19 there is no special opt-in process. There's certainly
20 nothing that looks like what we have here.

21 The Supreme Court also noted the
22 impossibility of deleting your cell-site records,
23 whereas here, not only, you know, you can delete your
24 location history stored by Google any time you want.
25 And it's -- significantly, this fact is emphasized

1 over and over again by Google, even in its very
2 minimal consent, you know, short brief text in the
3 opt-in process. It highlights the fact you can review
4 and delete your information at account.google.com. If
5 you look at the Google privacy policy, it further has
6 a long section explaining all the different ways you
7 can delete your Google data. You know, individual
8 data, service by service data, getting rid of your
9 account, all that is explained at length in the Google
10 privacy policy. So, that is not at all like cell-site
11 records.

12 And, finally, the Supreme Court noted that
13 having a cell phone was indispensable for
14 participation in modern society. Well, I think it's
15 quite clear that that's not the case of Google
16 location history. Obviously, one way to establish
17 that is empirically. We know now that only about a
18 third of Google customers have their location history
19 enabled. And the second way you can establish that
20 it's not essential to participation in modern society
21 is looking at the features associated with Google
22 location history. They're okay. They're helpful in
23 some circumstances, but they're just not that big a
24 deal. The tips on your commute, finding your phone,
25 you know, useful advertising all may be nice to some

1 customers, but they're not indispensable to
2 participation in modern society.

3 THE COURT: Well, to be fair, you should
4 address why Mr. Chatrrie is turning to that argument.
5 It's because Google requires a warrant under the
6 Stored Communications Act. And so they're saying
7 that's an indication that Google is calling it a
8 business record. Right? Isn't that what they're
9 saying?

10 MR. JUDISH: They're saying Google says it's
11 not a business record, but I don't think whether it's
12 a business record or not has bearing on whether it's
13 indispensable for participation in modern society.
14 So --

15 THE COURT: Yeah, but they're not arguing --
16 they're arguing under the Stored Communications Act
17 that it's content. Right? That's what they are
18 arguing.

19 MR. JUDISH: That's what Google is arguing.
20 So I think whether something is classified as content
21 under the Stored Communications Act is not that
22 important here. It affects the rules, the statutory
23 rules, for what kind of process the government can use
24 to get information, but I think as a Fourth Amendment
25 matter, it's not critical. The question is whether

1 Google has -- whether the records are voluntarily
2 disclosed to Google or not.

3 So, and the same thing, the conversations in
4 *Hoffa* were certainly content. That's people speaking.
5 But because it was voluntarily disclosed to the
6 persons who heard them, it didn't affect the -- the
7 Fourth Amendment was not impacted when the hearer
8 disclosed that information to the government.

9 So the -- whether its content has some, you
10 know, legal significance on the kind of process you
11 get. So I recently saw that Google had objected to a
12 proposed state law in Texas that would allow warrants
13 to get prospective location information from Google.
14 They say because it's content, actually the federal
15 law requires a wire tap order. I mean, all this is
16 complicated statutory stuff, but not really implicated
17 in this case. This case is about the Constitution and
18 the Fourth Amendment, not statutory definitions or
19 statutory rules.

20 I would note another point -- well, I guess,
21 on just -- it's worth saying a little bit about
22 *Carpenter*. *Carpenter* is, as the Supreme Court
23 emphasized, you know, a narrow case. It's about
24 protecting long-term comprehensive location
25 information. The Supreme Court was clear that it said

1 a warrant would be required for seven days or more.

2 The defense here is citing *Carpenter*,
3 essentially, for the notion that anything -- private
4 or sensitive information requires a warrant. That is
5 not *Carpenter*. That's not what *Carpenter* held, nor is
6 it what any court subsequently has decided. I think,
7 you know, *Carpenter* is no longer a totally new case.
8 This week is its third anniversary a couple of days
9 ago. I'm not aware of any courts who have interpreted
10 it so broadly.

11 Instead, it's a uniformly -- courts have
12 taken the Court, you know, at its word and treated it
13 as a narrow opinion designed to protect comprehensive,
14 long-term location information.

15 THE COURT: So address what they just argued.
16 Right? They said, yes, that nobody has broadened it
17 because we're the first folks that now know exactly
18 what Google is doing, and we know how in depth it is,
19 and that it covers, even if it's only a third of
20 users, it's tens of millions. And if a court had
21 known that, they might have come out differently.

22 Just agree, first of all, that other courts
23 did not have that information.

24 MR. JUDISH: So, I don't think other courts
25 had that information, other courts who have ruled thus

1 far. So, I think, I mean, that's very different than
2 the *Carpenter* issue because, first, *Carpenter* is, you
3 know -- we aren't obtaining comprehensive, long-term
4 information about all those other people. In fact, I
5 think it's quite doubtful that there is any Fourth
6 Amendment significance at all for anyone whose
7 information we did not return or who was not returned
8 for other than the 19 people. I mean, I don't think
9 it's a search with respect to the 19.

10 THE COURT: Wait. You're going way too fast.
11 I didn't hear the last sentence at all.

12 MR. JUDISH: So leaving aside the 19 people,
13 just talking about all of the others, I don't think
14 that there's any Fourth Amendment significance at all
15 to a provider the way a provider like Google uses
16 automated processes to find very narrow specific
17 information in a large database. You know, I don't
18 think there's any significance for people whose
19 information is not returned to the government. So --

20 THE COURT: Wait. Wait. I'm going to ask a
21 question about that.

22 So with respect to how Google does the
23 search, first of all, they are saying that Google is a
24 government agent. Do you agree with that? Under the
25 law, that they are treated as an agent.

1 MR. JUDISH: I don't think it's clear. When
2 you're talking about compulsory process -- and from
3 Google's point of view, this works an awful lot like a
4 subpoena. And I'm not sure that someone responding,
5 complying with compulsory process of one sort, is
6 really quite the same as other kinds of agency
7 relationships.

8 So I don't think -- I wouldn't concede that
9 it's an agency relationship. I think things are
10 different in terms of compulsory process. You know,
11 when you're in litigation, and the other side receives
12 a subpoena, are they really your agent when they're
13 complying with a subpoena? I don't think it's clear
14 on that. I don't think there are cases -- I'm not
15 aware of cases that specifically address that.

16 THE COURT: Right. Okay. So they're saying
17 you're not aware of it because we're the first folks
18 that know that when the government says we want to do
19 a geofence for this particular period of time, now we
20 know that it's functionally Google who says, Okay,
21 we're going to look at this area, and we're going to
22 do it in this time frame, and it's our algorithm about
23 how it works, and you don't get to know the algorithm.
24 Right?

25 So, if you get a subpoena, it is not the

1 case -- well, maybe there are cases, but it's not the
2 case that a business can say to you "I'm not going to
3 tell you how I search for documents," right?

4 MR. JUDISH: Well, I mean, Google is
5 telling -- Google's quite clear now about how they
6 respond to the process. I mean, we give them the
7 coordinates, and they look at each data point in their
8 system, and they decide whether it falls within the
9 range or not.

10 I mean, the part that Google is more
11 secretive about is how they calculate the people's
12 location in the first instance. I mean, that's the
13 part which -- you know, so how did they come up with
14 the particular numbers in their system for all those
15 data things. But once they get -- they work here
16 quite clearly, everything they did, once they got the
17 warrant from us.

18 THE COURT: Well, that may be a little bit
19 too simplistic because they said there is a range.
20 They said that they found a range. They said there's
21 a probabilistic return rate, like 68 percent they
22 found appropriate for advertising, right? So I have
23 to say, useful advertising is more a Google term than
24 it might be a user term, but, anyhow, it's
25 advertising. They target advertising.

1 So it is -- they're not saying that in a way
2 that the government can test that it's reliable.
3 Right? So this is what Mr. Price was just saying. He
4 was just saying, Yeah, we don't know about the ones
5 that haven't made hits or why because they haven't
6 made hits.

7 So why is the government allowed to just say,
8 Google, we think you're doing it right, and we'll use
9 it when it hits? Isn't that something the government
10 should have some input in? It's different than a
11 subpoena.

12 MR. JUDISH: All of that stuff happened prior
13 to the government getting the process in this case.
14 Google has its own internal algorithms which they use
15 to estimate where its users are.

16 THE COURT: I know, but you get the warrant
17 knowing they have this system you don't understand,
18 correct?

19 MR. JUDISH: Well, I mean, we've looked at
20 the data that they produce, and we've seen that it's
21 pretty accurately what --

22 THE COURT: It's 68 percent. Or are you
23 saying it's better than 68 percent?

24 MR. JUDISH: I'm saying that it seems
25 consistent with the notion that 68 percent of the time

1 the user falls within the display radius at the point
2 that Google estimates that they are. And I believe we
3 had testimony saying that the rest of the time it's
4 not like it's super far off. It's often near the
5 outside bounds of that, of the circle that Google has.

6 So it's not like it could be, you know, you
7 think it's in Richmond, and you're right 68 percent of
8 the time it's near the bank, and the other time it's,
9 you know, across town or in another state or something
10 like that. That's not the way it works at all.

11 And so what you have here, essentially, is
12 information which is, you know, like all information,
13 you know, it has some uncertainty in it, but it goes
14 to -- it would ultimately go to the weight given the
15 evidence, not the admissibility, because we've
16 observed the information and it seems to be -- work
17 the way Google describes it. That it --

18 THE COURT: Do I have any evidence about how
19 often the geofence fails? Like how often there's just
20 a zero hit?

21 MR. JUDISH: You mean, like we get a geofence
22 and it ultimately proves unsuccessful in locating
23 anyone or any evidence? I don't think there's
24 anything in the record about that, Your Honor.

25 THE COURT: So here's the commonsensical

1 layperson's perspective. And so I'm really trying to
2 give you an opportunity to explain it away. If there
3 were drug testing that were 68 percent reliable, would
4 it be admitted?

5 MR. JUDISH: I mean, I think -- I mean, I
6 don't know about the context of drug testing, but, I
7 mean, I think it's, you know, the definition of
8 evidence is fairly broad. And so I would say it's
9 evidence, but it's not all that reliable evidence, and
10 you would hope there would be more reliable evidence.

11 And so, you know, in a case like this, if we
12 go to trial, you would certainly want more than just
13 the geofence information, and yet it's still evidence
14 that the government collects, and then it helps direct
15 their further investigation, which, if things go well,
16 comes up with evidence which is even stronger and
17 better and more probative of guilt or innocence. But
18 it's clear that this meets the standards of what is
19 evidence because, you know, it is helpful information
20 which helps prove the facts which are at issue in the
21 case.

22 THE COURT: Okay.

23 MR. JUDISH: So, a bit more -- I wanted to
24 touch a bit more on the law associated with the
25 third-party doctrine.

1 First, the defense was just -- made a point
2 saying that sometimes you can use this information to
3 place a person in a private space, which they suggest
4 is a problem under *Knotts* and *Karo*, but *Knotts* and
5 *Karo* aren't third-party doctrine cases. *Knotts* and
6 *Karo* involve installing surreptitious transponders and
7 tracing them. In those circumstances, we if get
8 information from a private space without a warrant,
9 that's a problem because it's a search.

10 Here, however, when we rely on the
11 third-party doctrine, that's not an issue because the
12 leading or a leading third-party doctrine case is the
13 landline telephone case *Smith v. Maryland* where every
14 time someone makes a landline call from their house,
15 we place them in their house. And the Supreme Court
16 says that does not matter. It's still information
17 which is voluntarily disclosed to a third party. That
18 issue is explicitly addressed in *Smith v. Maryland*.

19 Again, I just note that subsequent to
20 *Carpenter*, the cases have all interpreted it narrowly.
21 Within the last few weeks we had a Seventh Circuit
22 case, *Hammond*, which held that there is no reasonable
23 expectation of privacy in getting like six hours or so
24 of prospective latitude-longitude-GPS-type data from
25 an individual cell phone.

1 And the Court looks at *Carpenter* and says
2 *Carpenter* is only about long-term location
3 information. And so that *Hammond* case is three times
4 the duration of the information at issue here. And
5 still the Court found that the Fourth Amendment was
6 not violated.

7 THE COURT: But isn't *Hammond* different in
8 that they had a suspect in mind? What the defense is
9 saying here is that it's a reverse search. It's like
10 we don't know who it is.

11 MR. JUDISH: *Hammond* was a specific person,
12 but as far as whether one has a reasonable expectation
13 of privacy in the information in the first place, I
14 just don't see -- I don't think it makes a difference.
15 I mean, I think that it would be -- it would be -- you
16 know, those are very different kind of warrants
17 between a warrant for an individual's location and
18 this type of warrant. But as far as whether one has a
19 reasonable expectation of privacy in the information,
20 really, I don't see how that can turn on the
21 particular kind of legal process the government got to
22 obtain it or didn't get to obtain it.

23 The question of whether there's a reasonable
24 expectation of privacy, I think, is sort of prior to
25 whatever kind of process the government uses to obtain

1 it.

2 One final thing on this point, just referring
3 to *Smith* and *Miller* as relics, I mean, you know, most
4 Supreme Court cases don't, like -- they don't, like,
5 age out after a little while. They get reversed by
6 the Supreme Court or they remain binding law. The
7 Supreme Court actually affirmed them in *Carpenter* that
8 they were still -- their continuing validity. So I
9 just don't think you can dismiss continued binding
10 Supreme Court precedent.

11 THE COURT: They're not talking necessarily
12 about the law. They're talking about the technology
13 involved. I mean, you have to concede this is
14 different technology. The scope is what they're
15 talking about, the breadth, the numbers, the detail.
16 So, you know, in the hearing that I saw, and I think
17 Google suggests, that if you were to go backward, as
18 these folks are, you have -- you can make a map of
19 where you were. You can make a little line of where
20 you were within a period of time. And so two hours.

21 The question is, if you're voluntarily giving
22 over your information, is the notice that Google is
23 giving putting you on notice that at any two-hour
24 period you can be mapped exactly where you are?
25 That's their point, right? That, sure, if you're

1 driving down on 95, maybe intellectually you can say,
2 Oh, you know, I have maps on. There's a
3 tractor-trailer crash, and they're going to take me
4 down Route 1 instead. But does that really -- does
5 that really put a user on notice that every two hours
6 of their life Google can track what you're doing in a
7 comparable way? So you're saying yes.

8 MR. JUDISH: "Saves where you go with your
9 devices" doesn't have qualifications with it. There
10 are no limitations. I mean, I think, you know, that's
11 what they do. That's what they say they'll do, and
12 that's what they do, and that's what they show you
13 they do if you log -- if you go where they direct and
14 look at the data that's stored.

15 I just don't know. "Saves where you go with
16 your devices" and we really mean it? I mean, I think
17 the defense kind of explored this, and what you end up
18 if you start trying to cover much more than that is
19 the wall of text, which nobody would read.

20 THE COURT: The what? I'm sorry?

21 MR. JUDISH: The wall of text was the phrase
22 that Mr. McGriff used when defense counsel suggested a
23 rather lengthy description that they thought that
24 Google should provide. And if they did anything like
25 that, we'd hear, well, nobody reads that. So,

1 instead, what Google does is they provide a very
2 concise description, "saves where you go with your
3 devices," which captures what it is, and then they
4 have an arrow, an expansion arrow, which goes into
5 more detail, and they have a link where you can go to
6 the website and actually see the data. I just
7 don't -- I don't think you can do more to explain, you
8 know, than that to effectively get across what's
9 happening here. You tell them what you're doing and
10 you let them see the data.

11 THE COURT: Well, not to mince words, but do
12 you think it would make a difference to a user if it
13 said "updated every two minutes"?

14 MR. JUDISH: No, I don't. People want the
15 service. And if you don't do it every two minutes,
16 it's not going to be all that effective. It's saving
17 where you go with your device. People move quickly
18 quite frequently and make brief stops in places, and
19 so it wouldn't actually serve its purpose if they did
20 much less.

21 THE COURT: All right.

22 MR. JUDISH: So, moving on to the warrant, if
23 you don't have any more questions on the expectation
24 of privacy.

25 THE COURT: If I do, I'll go back.

1 MR. JUDISH: All right.

2 So the magistrate here had a substantial
3 basis for issuing this warrant. And the question here
4 for this court is not would this court issue the
5 warrant exactly like this. It's whether the
6 magistrate had a substantial basis for issuing the
7 warrant. And so, you know, several -- there have been
8 in recent times several magistrate judges, federal
9 magistrate judges, who've issued opinions on this.

10 They sometimes want more in the way -- they
11 say I want more particularity in this way. This
12 application is too broad. Those do nothing to show
13 that there's a problem here, because, you know, the
14 facts of those cases are different.

15 In one case, the geofence extends out into a
16 denser urban area. In one case it involves a facility
17 with several layers of apartments above it. And so
18 getting a geofence there is just factually very easily
19 distinguished from here.

20 So if you -- the question is, first, did the
21 magistrate have a substantial basis for finding
22 probable cause? And the question here is, was there a
23 fair probability that Google had evidence of crime?
24 And the facts set forth in the affidavit were
25 sufficient to establish that.

1 The affidavit showed that a crime had been
2 committed, that the robber appeared to be using a cell
3 phone, and then established that most people have --
4 or that most cell phones are smartphones, that all --
5 nearly all Android and some Apple smartphones will be
6 linked to Google, and that Google can store location
7 information. That established a fair probability that
8 Google would, in fact, have evidence of the crime.

9 And I think it's important to note here that
10 evidence is not just about identifying the robber,
11 but, you know, one of the purposes of it was to form a
12 fuller geospatial understanding of the -- that's from
13 page 5 -- of the warrant and timeline related to the
14 investigation.

15 And so I sort of see the geofence warrant in
16 this case as sort of similar in quality to
17 surveillance videos. It gives you a picture of what
18 went on at this armed bank robbery, at the time of it,
19 sort of the people, where they were, where they're
20 coming and going. So it's a way of going and
21 essentially getting a new perspective on a crime
22 scene. And it certainly does that. And so that's
23 good evidence and, you know, a fair probability that
24 there was evidence of a crime.

25 Again, it can be used to identify

1 accomplices. You know, it mentioned other potential
2 witnesses, and they may not have been able to spot any
3 other witnesses before they sought the warrant, but
4 there could have been someone sitting in the car there
5 back where the defendant parked. And so the notion
6 that it was too late to -- sorry. I don't mean
7 witness. Accomplice. That it was too late to look
8 for other accomplices. Absolutely not. It was a
9 totally appropriate part of this warrant to look for
10 accomplices. It was -- that's included and is the
11 basis for the warrant and is part of the reason why
12 there was probable cause to get this particular
13 warrant.

14 All this, the sort of a broad interpretation
15 of what is acceptable for a search warrant, is
16 confirmed by the Supreme Court's decision in
17 *Messerschmit v. Millender* where they talk about sort
18 of the broad -- sort of different reasons you might
19 want to gather evidence, including things like
20 (unintelligible) defenses and stuff.

21 THE COURT: You are really --

22 MR. JUDISH: I apologize for that, Your
23 Honor.

24 THE COURT: I didn't hear what you said.

25 MR. JUDISH: So, in -- a broad conception of

1 evidence is confirmed by the Supreme Court's decision
2 in -- I'll just call it *Millender* -- in which they
3 look at a warrant and look at the reasons behind the
4 warrant, and it's things like rebutting possible
5 defenses. So it's a very broad conception of what
6 constitutes evidence under a search warrant.

7 And this warrant sought this location
8 information not just to identify the robber, but also
9 for these other purposes, which are explicitly
10 mentioned in the affidavit. So the notion of the
11 affidavit being all about finding the robber just
12 isn't true. You know, we don't look to, like, well,
13 it's mostly about this other topic, and, therefore,
14 this thing mentioned in the affidavit doesn't count.
15 That's not the way things work.

16 THE COURT: So I'm just going to totally
17 change courses so that I can have you address this on
18 this record. And I'm going to tell you right now, I
19 don't think it's an issue, but this is obviously a
20 state warrant from a state magistrate. And so this
21 magistrate was fully empowered to do what he did.

22 I guess I would want you to say this
23 magistrate, who had, I don't know, a couple years
24 experience, did not have a law degree, right? He had
25 a college degree. And it's a pretty broad warrant.

1 And so my question is, do you think that the Virginia
2 law should hold under this circumstance, right? I
3 mean, federal magistrate judges have law degrees. And
4 it's not clear to me that the General Assembly, when
5 it was figuring out how magistrates work in the
6 commonwealth of Virginia, were anticipating that they
7 could sign warrants that searched tens of millions of
8 user records. So I just want you to state this on the
9 record.

10 MR. JUDISH: I think the magistrate was
11 authorized under Virginia law to issue warrants, and
12 the government doesn't always get to pick and choose.
13 I think we have testimony in the record that there
14 was -- the preference of the Virginia courts was to go
15 to the magistrates rather than the state judges. So
16 when judges -- we do what we're told, Your Honor. And
17 this is constitutionally permissible under *Tampa v.*
18 *Shadwick*, and this was a judge authorized for Virginia
19 to issue warrants.

20 I still -- I still -- I disagree with the
21 characterization of this being a search of tens of
22 millions of people. I think the government obtained
23 no information about those -- about anyone other than
24 the 19.

25 The government can't tell, you know, if

1 you're not among those 19, anything about where you
2 were that day. It doesn't know whether or not you
3 have a Google account. What does the government know
4 about those 19 people? It doesn't know whether you
5 have a Google account or not. It doesn't know whether
6 you activated location history or not. It can't tell
7 anything about those people.

8 THE COURT: Why don't you distinguish the
9 example he used about, okay, we're going into a bank.
10 We know one of your boxes has a gun, but we want to
11 look at them all.

12 MR. JUDISH: Well, I think the difference is
13 that this is, you know, among other things, this is a
14 database which Google has free access and free rein
15 to, and so it's entirely appropriate in a context
16 where Google operates freely within a database to --
17 for it to have Google go through and make a very -- to
18 search through it and -- search through it not in the
19 Fourth Amendment sense, in the computer science sense,
20 to look through the database in order for that -- to
21 find that narrowly targeted information.

22 A couple of points on this. You know, this
23 is not an entirely new thing. I mentioned in our
24 brief the *Ameritech v. McCann* case. I think a
25 subpoena for the phone records of everyone in the

1 country would be a very troubling subpoena and
2 overbroad under almost any circumstance you can
3 imagine. However, for decades, you know, because
4 phone companies store local calling information, index
5 it only by the outgoing number and not the incoming
6 number. When they receive a subpoena asking them who
7 called -- you know, if they asked, like, "Who called
8 Nathan Judish?" They have to look through their
9 entire database and sort through that entire thing in
10 order to get the limited information about who
11 actually did that.

12 So searching through a giant database to find
13 limited information is not a new thing. *Ameritech v.*
14 *McCann* is not about a Fourth Amendment challenge.
15 It's about who pays for that, whether the government's
16 on the suit for the cost. No one has thought that
17 there's a Fourth Amendment problem with looking
18 through the huge database in order to get this very
19 narrow targeted set of information.

20 Also, you know, another point that comes out
21 of *Smith v. Maryland* is that Fourth Amendment
22 protections really should not depend on a service
23 provider's internal business practices which are not
24 visible to the public.

25 THE COURT: Not -- I'm sorry?

1 MR. JUDISH: Which are not in any way visible
2 to the public. And so in *Smith*, you know, the issue
3 was whether it mattered that phone companies did not
4 normally keep a record of the local phone calls that
5 people dialed. And the Supreme Court says that
6 doesn't matter. It has no constitutional
7 significance. It would make a crazy quilt of the
8 Fourth Amendment for that kind of thing to matter.

9 THE COURT: It would make it -- I'm sorry?

10 MR. JUDISH: A crazy quilt is the official
11 term.

12 And so here, the fact that Google indexes its
13 database like this is entirely invisible to the
14 public. You know, as we've pointed out, Google could
15 just as easily have stored this data in a different
16 manner partitioned not by account but by location.
17 The database would have the exact same information.
18 It would search -- sorting through it would produce
19 the exact same outcome from the government, and yet
20 the Google's computers would not have to look at all
21 the data at all. All they would have to look at is
22 the data for whatever relevant partitions had the data
23 for the geofence.

24 So the fact that this could be done without
25 sorting through everyone's data strongly suggests that

1 there's no great Fourth Amendment significance to the
2 fact that Google sorts through the data before turning
3 over to the government only this tiny subset of the
4 information. So, it doesn't make it a search.

5 I don't think I was searched by this geofence
6 warrant. I don't think anyone whose information the
7 government got back nothing from, I don't think the
8 government learned anything about the rest of us. I
9 just don't see how that's an invasion of a reasonable
10 expectation of privacy when the government learns
11 nothing about you. I don't think --

12 THE COURT: But that presumes that Google is
13 not an agent of the government.

14 MR. JUDISH: I don't know if it presumes that
15 or not. I mean, it's really -- it's -- I can't think
16 of any case involving a search so insignificant that
17 the Supreme Court would think of that as a search.
18 What you learn is just so -- I don't even think you
19 learn anything.

20 THE COURT: Well, they say what you learn is
21 an anonymized number that's static that is a person or
22 an account. And so you can readily with a subpoena
23 find out who that is. So you're learning something,
24 they're saying.

25 MR. JUDISH: We learn something about those

1 19 accounts. It is, to some extent, anonymized, but
2 I'm talking about the supposed tens of millions of
3 other searches. Those we learn nothing about. And so
4 that's what I'm saying I just don't think that has any
5 Fourth Amendment significance.

6 The defense now -- a lot of its argument is
7 about all the people who have location history about
8 whom the government learned nothing, not an anonymized
9 account number, not whether they exist or not,
10 nothing. We learned information about 19 accounts. I
11 think it's fair to debate whether that's a search or
12 not. But what did we learn about those supposed tens
13 of millions? Where was the invasion of privacy when
14 the government learned nothing? And Google learned
15 nothing that they already didn't know. There's a
16 giant database which they search through anyway. They
17 didn't learn anything from it.

18 So, I want to go to the discretion issue
19 associated with the warrant. The first thing I would
20 say is this warrant just left no discretion whatsoever
21 to Google. Google did exactly what it was directed
22 to. The warrant directed Google to disclose location
23 information within a particular -- of devices which
24 were present in a specified circle of 150 meters
25 during -- in a disclosed two hours of location

1 information for them during the time of the robbery.

2 And Google had no discretion about what
3 database it looked through. Google should look
4 through every database it has which contains
5 information which is responsive to the warrant.

6 THE COURT: All right. So you know what? I
7 want to be sure we're paying attention to time. When
8 did we start? 11:40. All right. We can keep with
9 this discretion issue, and then we'll probably take a
10 break.

11 MR. JUDISH: So, Google did what they were
12 directed to do. And everything they did is what the
13 warrant directed. So, it isn't --

14 THE COURT: So, Mr. Judish, you have to
15 address more specifically what they said. Right? So
16 you can say Google did exactly what it was supposed to
17 do. Right? So that's fine. But they don't say that.
18 So you have to tell me why they're wrong.

19 What they say is that it just said search
20 your databases, and somehow Google only searched
21 Sensorvault. And there's nothing on the record that
22 says why didn't they search Web & App Activity.
23 Right? So they're saying somewhere there's discretion
24 there or an agreement, but nobody knows where.

25 MR. JUDISH: Sorry, Your Honor. There is

1 stuff in the record. What's in the record is McGriff
2 saying that the Sensorvault database is the only
3 database which contains sufficiently granular
4 information to be responsive to the warrant.

5 THE COURT: Sufficient what information?

6 MR. JUDISH: I don't know the exact words,
7 but he says both in his -- that it's the only -- it's
8 the only database with sufficiently granular
9 information to be responsive to the warrant. So
10 that's why they don't search the others.

11 As a recipient of compulsory process, they're
12 supposed to, you know, know what they have that's
13 responsive. As a -- someone who helps prosecute other
14 cases, I was hoping we'd learn in this case that they
15 had more information that they hadn't been disclosing
16 to us that would be helpful in other investigations.
17 Turns out, according to McGriff, they don't have that
18 information. So what else -- if there's nothing else
19 responsive, then they've done their job pursuant to
20 the warrant and disclosed what they were directed to
21 disclose.

22 THE COURT: So you're saying it's okay that
23 Google knows that, but that the government doesn't
24 know that they have only searched one?

25 MR. JUDISH: I'm saying that it was

1 appropriate for Google to do what the warrant said and
2 give all the information they had about information
3 which falls within the scope of the warrant. And
4 Google -- the providers always know their databases
5 best. And so the warrant is very specific about
6 information it wants. And so Google, then, should
7 look through all the information it has. And it's
8 okay for Google to know that and not us. I mean, they
9 don't always tell us everything --

10 THE COURT: So do you think that the phrase
11 "sufficiently granular" is at all subjective?

12 MR. JUDISH: I mean, the -- that's McGriff's
13 testimony. He says there aren't other databases which
14 are responsive to the warrant.

15 THE COURT: Well, he says that aren't
16 sufficiently granular. So how do we test that?

17 MR. JUDISH: Well, I mean, Google receives
18 the warrant, and it complies. I mean, I think that he
19 explained that it would be like databases which would
20 tell you that someone is in Richmond. Obviously, a
21 database that tells you some information that tells
22 you someone is in Richmond isn't going to be
23 responsive because it's not going to place someone in
24 this circle.

25 And so the warrant itself is quite clear. We

1 want information about, you know, where you can --
2 about location within this circle. And so Google had,
3 and apparently complied, with its obligation to go
4 look at whatever data it had which could place someone
5 within a circle like that. So --

6 THE COURT: And so neither the magistrate nor
7 the agent needs to know that?

8 MR. JUDISH: No, I don't think so, Your
9 Honor. We know that Google has location information.
10 And so like Google's internal names for it and things
11 like that, I don't think that's critical. Whatever
12 information they had which can place someone in the
13 geofence is going to be evidence of crime, and it's
14 appropriate to ask them for that information.

15 So as far as the three-step process goes, do
16 you want to take a break before we move on to the
17 discretion associated with the three-step process or
18 shall we continue?

19 THE COURT: You know what? I think we should
20 take a break. So it's now twenty of one. We should
21 take a 40-minute break so people can eat if they want
22 to. So we'll go until 1:20. All right? We'll take a
23 lunch recess.

24 (A luncheon recess is taken from 12:40 p.m.
25 until 1:25 p.m.)

1 THE COURT: All right. Mr. Judish, I'm not
2 sure if this gets to what you're going into, but I am
3 going to just be sure that I've covered the questions
4 that I think pertain to what you just argued.

5 So I spoke to you about sort of the frequency
6 with which Google updates and stores the information,
7 and I used two minutes. I think that's on the record,
8 but I know that in our data return it was as quick as
9 30 seconds.

10 So in response to my question, you said, "I
11 don't think it would matter to users if they knew it
12 was every two minutes." So I'd like you to address
13 the evidence that I saw and heard that Google was
14 concerned about that. The emails that said, "Count me
15 among the Googlers that had no idea we were doing
16 this." And that Google actually changed its policies
17 as far as notification because, in part, of that
18 process, which all happened after Mr. Chatrpie's case
19 as far as I know.

20 MR. JUDISH: Your Honor, I think it's hard to
21 attribute the specific changes in Google's terms and
22 service and banners and all that to any specific
23 thing. I mean, McGriff explained there was an ongoing
24 process and a continued attempt to improve their
25 process. So I just don't think you can draw any

1 particular inferences on any particular language from
2 anything in the record.

3 I do think that it's just -- the thing to
4 look at is -- you know, one way of looking at it is do
5 what people do fall within the scope of the consent
6 given by people who opted into it. You know, "saves
7 where you go with your devices" really means saves
8 where you go with your devices. And so whether it is,
9 you know --

10 THE COURT: So it's not -- even though Google
11 employees who work for the company that said "saves
12 where you go with your devices" were surprised, that
13 doesn't matter?

14 MR. JUDISH: I mean, there's a lot of
15 employees who work for Google. There's a lot of
16 people in the country, but I think the real question
17 to look at, that we normally look at in Fourth
18 Amendment consent situations, does this fall within
19 the scope of the consent. And if you say "saves where
20 you go with your devices," then you agree to that,
21 then Google can save where you go with your devices.
22 There is, you know, in the world of computers, lots of
23 data gets generated in almost everything we do. To
24 me, the unremarkable thing about this case is just how
25 little data the government obtained.

1 THE COURT: You're going afar from what my
2 question is. So you're saying that it's within the
3 scope of the consent because this one sentence was
4 enough, and it wouldn't have mattered if you said it
5 is updated every two minutes because it's incorporated
6 within that sentence, and it wouldn't have mattered as
7 far as it being consent that it was updated every 30
8 seconds because it's incorporated because "Saves where
9 you go with your devices" says "Saves where you go
10 with your devices."

11 So what do I do, if anything, with the
12 reality that no one reads that stuff? Nobody reads
13 the privacy policy. What do I do with that?

14 MR. JUDISH: I mean, courts do pay attention
15 to privacy policy (unintelligible) --

16 THE COURT: You definitely have to speak up.
17 I don't know if the microphone is too far away from
18 you or what.

19 MR. JUDISH: I'm sorry.

20 Courts certainly do pay attention to privacy
21 policy in terms of service. The *Adkinson* case in the
22 Seventh Circuit is an example of that. But this is
23 more than just an obscure privacy policy thing.

24 The noteworthy thing about the opt-in process
25 is how it is done through a relatively small amount of

1 text that Google has worked hard to get people to
2 read. It's not long. "Saves where you go with your
3 devices." This isn't a case where you're getting
4 bogged down by, you know, those gigantic
5 scroll-down-click-through things that we often have to
6 look at.

7 So, I mean, I don't think it's fair to assume
8 that people won't actually read that one little
9 sentence before they agree to it. And, I mean, in any
10 case, people are generally bound by their agreements,
11 but Google really does a much better job than most
12 other providers in getting people to agree to terms of
13 service in trying to do this in a way that people will
14 actually read and pay attention to.

15 That's one thing I took away from the McGriff
16 testimony is they're trying hard, and they have done a
17 pretty good job, I think. If I were to sit back and
18 try to think what will people actually see? It's not
19 the wall of text. It's something like what Google did
20 here with the, like, "Saves where you go with your
21 devices," and like one or two or three other lines for
22 further explanation. And then if people want more,
23 it's available. That's pretty good.

24 THE COURT: So tell me -- I mean, it doesn't
25 matter whether you and I think it's good. The

1 question is whether or not it's constitutional and
2 appropriately giving notice.

3 So where is an individual on notice about how
4 precise the geolocation is? So one issue is if you're
5 getting a phone number, right, you're getting a phone
6 number. But we heard testimony that this location can
7 be as specific as within 2 meters. So if you're
8 getting updated every two minutes, if it's two
9 minutes, I mean, our return had some that were 30
10 seconds, if you're getting updated every 30 seconds
11 within 2 meters, are you saying that's not
12 qualitatively different as far as a notice and an
13 opt-in process? Where does it say we know exactly
14 where you are?

15 MR. JUDISH: Well, there is mention in GPS
16 data somewhere in all this. I'd have to look to see
17 where it is. But people know that GPS is accurate to
18 within a few meters. And there's mention of Wi-Fi. I
19 don't know if it's as readily known, but people who
20 know anything about this know that Wi-Fi is accurate,
21 but not as accurate as GPS, but it's still reasonably
22 accurate. And also it says because -- and this is,
23 again, quite remarkable. Google says from the little
24 opt-in screen "You can review your data" and it gives
25 you a link. And you can go and you can actually see

1 the data. So that's distinguishes it from the
2 information stored by phone companies. And even in
3 the *Smith* days, you didn't know what data you had.
4 Here you really can. Google will tell you every bit
5 of data it stores about you. You can download it all
6 in one piece if you want and take a look at it or you
7 can look at it online. So Google's not hiding the
8 ball.

9 THE COURT: So most of the GPS cases that I
10 am aware of that say it's constitutional involve
11 instances where folks are being followed on public
12 roads. So I think what the defense is saying here is
13 that one of the issues is that this GPS data, or
14 whatever it is, within 2 meters can include
15 constitutionally protected spaces like a church. So
16 that's what I have in front of me.

17 They're not claiming that we found
18 Mr. Chatrrie in his house. But they're saying he was
19 in a church. You can't do that.

20 MR. JUDISH: Again, Your Honor, I think I
21 covered this point before, but *Knotts* and *Karo* are
22 about surreptitious tracking. They're not about
23 information disclosed to a third party.

24 In *Smith v. Maryland*, that involved a
25 landline telephone. There were people sitting in

1 their house making phone calls. You can place a
2 person, in those days, on a call on a landline phone
3 also within a few meters, because how long were the
4 phone cords? Not that long, typically. But in any
5 case, they certainly placed people within a private
6 space. And the Supreme Court said it didn't matter,
7 that you could determine people were in their home
8 within a private space because the person was
9 disclosing the information to a third party.

10 And here people are choosing to disclose
11 their information to Google in order for Google to
12 provide them with location-based services. So it
13 doesn't violate the Fourth Amendment when Google then
14 shares that information with the government.

15 THE COURT: So if you're making a phone call
16 out of your house, you're in a private space. So I
17 guess if you make five phone calls in one day, the
18 government is aware you're in your house five times in
19 one day or at least a phone number is being dialed out
20 in one day. But with respect to most of the tower
21 dump cases, right, isn't it the case that it's not
22 seeking a single data point, right? It's like
23 watching a phone go down a street. Am I right about
24 that? So you're going to different towers?

25 MR. JUDISH: Most of the published cases have

1 involved searching multiple towers. Certainly not all
2 tower dump cases are like that. Sometimes we're just
3 interested in dumps at a particular place and a
4 particular time.

5 Mostly that's going to be useful if there's,
6 you know, a place where there's not a lot of people.
7 I remember one case that I consulted on, someone had
8 dumped a body in an obscure location sometime between
9 midnight and 6:00 a.m. In that case, a single place
10 tower dump would be helpful.

11 THE COURT: Right. So when you get a tower
12 dump, is it the case -- and I guess I want you to
13 compare what's happening in this with us here.

14 So I think what you're saying is Google looks
15 at not tens of millions, but lots of records that the
16 government doesn't really see. Do they disclose the
17 bigger amount?

18 MR. JUDISH: No, Your Honor, not at all.

19 THE COURT: Stage I is not disclosed at all?

20 MR. JUDISH: Stage 1, we get information
21 about the 19 individuals who had data points present
22 in the geofence during the hour of the bank robbery.
23 That's it. They don't give us any information about
24 tens of millions. We don't know how many people there
25 are. We don't know how many people have location

1 history enabled or anything like that. All we get
2 information on is 19 people. There's nothing beyond
3 that.

4 THE COURT: So if you're getting a tower
5 dump, when you're dumping the towers, are you getting
6 just the 19 people three times or are you getting
7 everything on the tower? Is the government doing the
8 comparing?

9 MR. JUDISH: The government does the
10 comparing on tower dumps. So typical tower dumps
11 often involve hundreds of thousands of records. So
12 that's why, as we explained in our briefs, this
13 process -- the geofence warrants tend to be much more
14 limited than a tower dump because in tower dumps, we
15 actually learn information about a lot more people
16 being in the vicinity for each tower dump we get.

17 THE COURT: But that discounts that Google is
18 looking at that information, right?

19 MR. JUDISH: Yes.

20 THE COURT: They're saying Google is the
21 agent. So the government is getting information.
22 They're just only turning it over to another part of
23 the government, the 19 names?

24 MR. JUDISH: I would not say the government
25 is getting any information about those other people.

1 THE COURT: I know you wouldn't say that.
2 That wasn't my question. My question was, they're
3 saying that Google is the agent, and so when they're
4 looking at those, that they are at least accessing
5 information about numerous individuals.

6 MR. JUDISH: Yes, Your Honor. I would note
7 that Google accesses that information anyway. That's
8 how their system works. So Google isn't learning
9 anything it wouldn't use or didn't already know.

10 It's in their Sensorvault database, which
11 they access frequently for whatever purposes they
12 have. They're looking to try to do what they call
13 semantic information, being able to analyze someone's
14 location history to determine things which would be
15 useful for Google for advertising purposes and stuff
16 like that. So Google looks through the location
17 history. So it's --

18 THE COURT: So are you saying that Google
19 does that through separate searches, that it's not an
20 algorithm that just works that out? This is
21 different, isn't it? I mean, Google doesn't go in and
22 say, or do they, who is near the federal courthouse so
23 that I can advertise, as a lawyer, on average in a
24 particular period of time?

25 MR. JUDISH: I think that's exactly what you

1 can do if you want. That's what Google calls radius
2 targeting. You can say I want --

3 THE COURT: You can't say "you." You have to
4 say who can say, who's controlling it.

5 MR. JUDISH: Sorry. An advertiser can say to
6 Google, "I want to target people within a kilometer of
7 the federal courthouse." And then Google will target
8 ads to those people. Google describes this process on
9 its website.

10 And then afterwards, if you have your law
11 office at some particular place, Google will then do a
12 geofence of people who visit your law office to see
13 those people who it targeted advertisements to, which
14 of them subsequently visit your law office. And then
15 it will tell you how many there are in that. So that
16 really requires Google to do a geofence of people
17 visiting your law office. You know, it's checking to
18 see of these people who they targeted the
19 advertisements to, do they later visit this very
20 specifically defined location. So it's really very
21 closely related to what is done here with a geofence
22 warrant and --

23 THE COURT: You keep referring to the *Smith*
24 case, and I may not be remembering it well, but didn't
25 the *Smith* case involve use of an operator?

1 MR. JUDISH: No. No, Your Honor. I mean, it
2 would have been an electronic pen register device in
3 *Smith*.

4 THE COURT: Okay. All right.

5 So I'm just going to ask you to address as
6 you go forward, *Carpenter* is focusing on what reveals
7 the privacies of life, right? So I want you to use
8 that lens as you describe to me how you're going
9 through the stages.

10 MR. JUDISH: All right. So I just want to
11 put on the record one citation before I move on to the
12 three-step process. We talked about where Mr. McGriff
13 explained that location history was the only
14 information sufficiently granular to respond to a
15 geofence warrant. You can find that in his first
16 affidavit, which is Government's Exhibit 3 at
17 paragraph 20.

18 So the three stages, the three-step process,
19 the first thing I'd say is that I actually, you know,
20 as the Magistrate Judge Harjani in Illinois explained
21 in his opinion, the multi-step process really does
22 lack constitutional significance.

23 I mean, the key thing here is that we
24 establish probable cause and specify with
25 particularity for all of the information that we

1 potentially could have obtained. Google very much
2 likes the three-step process. And I think it's an
3 affirmatively good thing that has some additional
4 ability to provide sort of practical privacy
5 protections while still enabling our investigations to
6 proceed. But that doesn't mean that it's
7 constitutionally significant. That's exactly what
8 Magistrate Judge Harjani said. You know, it could
9 have practical benefits, not constitutionally
10 significant. But the key issue before this court is
11 whether the issuing magistrate had a substantial basis
12 for his determination that the evidence the government
13 could potentially obtain was, in fact, evidence of
14 crime and for that reason it established probable
15 cause for it.

16 But anyway, the way it works is that the
17 first step of the three-step process, all that we got
18 pursuant to that is the latitude and longitude
19 coordinates, which were in the specified geofence, the
20 circle with the radius of 150 meters.

21 THE COURT: You just, you know, you have to
22 be slower. You just do. Because I don't know what
23 those numbers were. I read them, but our court
24 reporter has to get them as you say them.

25 MR. JUDISH: All right.

1 All we get from the first step of the
2 geofence is the latitude and longitude coordinates,
3 which actually fall within the geofence during the
4 hour of the robbery.

5 So if people, to the extent people came and
6 went from outside during the Step 1 information, we
7 don't get that. It's just if the latitude and
8 longitude points in the Sensorvault database fall
9 within the circle during that hour, then we get those
10 along with an anonymized reference number from which
11 we cannot, without more from Google, determine any
12 identity information.

13 So that, you know, as far as privacy of life
14 goes, I just don't think that's all that private.
15 Certainly going to a bank is not a particularly
16 private activity.

17 I do feel obliged to note that I don't think
18 that -- to say *Carpenter* is about protecting the
19 privacies of life, it can't go that far. You'd have
20 to overrule *Smith* and *Miller*. Who you dial on a
21 telephone, that's private. Your financial
22 transactions, those are private things. I think we
23 really do have to take *Carpenter's* word that it's
24 about long-term location information.

25 But anyway, addressing the Court's question

1 as to how private the information is, your presence in
2 that 150-meter radius, I think, is not all that
3 private. Obviously, there is a church there. It is
4 hard for me to believe that one can protect oneself
5 from a bank robbery by choosing to rob a bank next to
6 a church and using the church parking lot. And there,
7 I guess, I would point to the Fourth Amendment
8 principle that you can't rely -- it has to be about
9 violation of your Fourth Amendment rights. You don't
10 have standing to challenge Fourth Amendment violations
11 of others.

12 And whatever the defendant was doing the day
13 of the bank robbery, I don't think he's claimed that
14 he was going to church. So he -- so I don't think
15 that has any impact --

16 THE COURT: Does he have to claim that?
17 What's his obligation?

18 MR. JUDISH: I mean, if the issue is to try
19 and assert that his privacy interests were invaded, he
20 needs to explain how his privacy interests were
21 invaded. And so that's the issue which I think he
22 fails on because the defense keeps talking about the
23 potential privacy invasion of people being found
24 inside their home. They don't claim that he was found
25 inside his home. They talk about privacy issues

1 associated with church. They don't say he was
2 associated with church. He's got to claim his privacy
3 invasion, that his privacy interests were invaded.

4 So one case I can cite on that is the Seventh
5 Circuit case *Patrick*, which involved use of a
6 cell-site simulator to locate the subject of an arrest
7 warrant. And *Patrick* tried to claim that use of the
8 cell-site simulator violated the privacy interests of
9 others nearby because the cell-site simulator, which
10 is a device which has essentially a direction antenna,
11 which locates where nearby cell phones are, violates
12 the privacy of others nearby.

13 The Seventh Circuit says no, under *Rakas*, you
14 don't have standing to assert any privacy violations
15 of others.

16 THE COURT: So are you saying that factually
17 Mr. Chatrie was not in the church?

18 MR. JUDISH: I don't -- to my knowledge he
19 parked near the church. I have no knowledge that he
20 was in the church. I don't know of anything in the
21 record on that. I mean --

22 THE COURT: Was he within 2 meters of the
23 church?

24 MR. JUDISH: He may have been, Your Honor. I
25 don't think -- I think there may be stuff in the

1 record. I think his coordinates are plotted. And so
2 that would be the place to look for that. I can't
3 state with certainty. So that's the first step.

4 The second step of the warrant, you know,
5 that enabled the government to get all of the location
6 history over a two-hour interval of the individuals
7 whose information was disclosed in the first step.
8 And so that does, you know, potentially implicate
9 greater privacy interests because you can't have
10 people going to and from the area. But, again, I
11 don't think Mr. Chatrue has pointed out any
12 particularly heightened privacy interests of his which
13 were infringed.

14 And in any event, I think the real issue is,
15 was there a substantial basis for the magistrate's
16 determination that this would be evidence of crime?
17 And, you know, the additional contextual information
18 is extremely helpful in showing what people's roles in
19 the criminal activity was. And so it was evidence of
20 crime, and therefore appropriately fell within the
21 scope of the warrant.

22 THE COURT: And so I may be getting ahead of
23 where you are about to argue, but explain to me -- my
24 understanding is that with this degree of certainty of
25 the radius, there is a 150-meter radius, but then a

1 broader radius that may actually be implicated. Am I
2 right?

3 MR. JUDISH: Google has, you know, there's
4 chance for errors in the data. There's no question
5 about that. The warrant directed Google to disclose
6 the points where the points calculated by Google fell
7 within the radius, but there was certainly some chance
8 of false positives in that. And, again, I just think
9 that that would go to the weight given the evidence as
10 opposed to whether or not it is actually evidence of
11 crime.

12 THE COURT: Well, what they're saying is one
13 of the issues is that if you're signing a warrant -- I
14 mean, I think they say it's almost twice as much, like
15 378 meters, 387 meters, that a magistrate is not on
16 notice that it could be actually twice as large, the
17 area that you're searching, given the rate of
18 potential certainty.

19 MR. JUDISH: First, I just want to go into
20 the facts. I think they significantly exaggerate the
21 actual inaccuracy. There are a few individual points
22 which have large errors associated with them, but if
23 you look at the actual data, which is in the record,
24 every single one of those will have another point for
25 the same device with the same center and a much

1 smaller radius.

2 And as Agent D'Errico testified, what that
3 actually means in practice is that the phone started
4 at the smaller place and then went somewhere, and
5 Google isn't sure where. So it's not that these are
6 devices which may have been the whole time super far
7 away. It's that the way that Google -- you know, they
8 have indication that a device is on the move, but they
9 don't know where. So they, you know, they keep
10 estimating the same center point. But their
11 uncertainty grows.

12 But the more general point, as far as the
13 magistrate and what was in the affidavit, I think
14 people understand that cell phone measurements are
15 inaccurate, and, thus, I think a commonsense
16 magistrate would know not every location information
17 point is going to be perfect. So I don't think -- and
18 I understand the defense has dropped its argument that
19 it was a, you know, somehow a violation that we didn't
20 include this information in the affidavit. I think
21 that showed up in some of their briefs, but not their
22 final one.

23 One other point I'd like to make about the
24 three-step process is that it's clear from the Playpen
25 cases that doesn't violate the Fourth Amendment if the

1 government chooses to obtain less than the maximum
2 amount of information it's authorized to under a
3 warrant.

4 In the Playpen cases, we were going after a
5 child pornography website on the Dark Web, and we
6 obtained a warrant authorizing us to use code to
7 identify people who logged on to the site. We made
8 explicit in our affidavit that we were authorized to
9 use this code to identify anyone who accessed the
10 site.

11 We, in fact, were likely to target our code
12 more narrowly than that, and that's ultimately what we
13 did. And this was challenged just as a vast number of
14 cases -- I think there's over 100 Federal District
15 Court cases and there are 11 Federal Court of Appeals
16 cases dealing with challenges to this warrant. I
17 don't think any court has found that that language was
18 problematic.

19 THE COURT: Well, what is different, though,
20 is that every person who logged on to that account
21 violated the law 100 percent. So not 100 percent of
22 people who were near the bank violated the law, like
23 way, way less than 100 percent.

24 MR. JUDISH: Yes, that's absolutely right.
25 But the key, what they have in common, is that there

1 was a substantial basis for the magistrate judge's
2 determination that all of the evidence you're entitled
3 to, all of the information we were entitled to, was
4 evidence of a crime. And that's what counts. And so,
5 again --

6 THE COURT: It counts because it was an
7 illegal website. How is that not a completely
8 different situation?

9 MR. JUDISH: Well, the warrants are used to
10 seize evidence of crime, and that can be direct
11 evidence that someone is guilty, but it can also be
12 other information as well. And so the issue is
13 whether a magistrate has a substantial basis to think
14 it was okay or proper that all of the user location
15 information we were authorized to seize would in fact
16 be evidence of crime. It doesn't have to all -- all
17 the people don't have to be guilty. The question is,
18 is what we're authorized to get evidence? And here it
19 was.

20 It's like I said. It gives us an ability to
21 reconstruct the scene of this crime. It helps us
22 identify accomplices. It helps us find witnesses.
23 It's all appropriate evidence of crime, which can
24 appropriately be seized pursuant to a warrant.

25 And, yes, there's not all criminals in this

1 case, but it is all evidence, and as long as we
2 establish probable cause and identify with
3 particularity evidence, I think it's entirely okay for
4 us to then be selective within what the subset of what
5 would establish probable cause and identify with
6 particularity what we ultimately take away.

7 I think that happens, you know, all the time
8 in search warrants is, you know, we have a warrant.
9 You don't have to, you know, raze a house to find
10 every bit of evidence in a house that you're searching
11 even though, you know, you can keep looking harder and
12 harder and find more of the key thing that you
13 establish probable cause and identify with
14 particularity the things that you are authorized to
15 seize.

16 In any event, if the Court does have a
17 problem with Step 2 of the warrant, I think the
18 appropriate thing is severance. This is a warrant
19 which is usually conducive to sever. The process was
20 done. The language of the warrant is separate. The
21 process is done in separate steps. This is a warrant
22 which is just enormously easy for the Court to --
23 would be enormously easy for the standard severance
24 doctrine to apply. From the Step 1 information in
25 this case, it was sufficient to identify which account

1 likely belongs to the robber, and so the fruit of the
2 poisonous tree would not extend to our subsequent
3 investigation and all of the subsequent evidence we
4 obtained in this case after we first obtained the
5 geofence warrant information.

6 THE COURT: So you're saying because you had
7 19 names, you have had enough to identify Mr. Chatrie?

8 MR. JUDISH: Because we had 19 sets of
9 location information in that 150-meter radius, and we
10 could -- and from the other information obtained at
11 the scene of the robbery, including surveillance
12 videos and eyewitnesses, we knew where Chatrie had
13 come from and, you know, parked, gone into the bank
14 and returned. And the location information of
15 Mr. Chatrie from the geofence warrant was sufficiently
16 consistent with that testimony that we could still
17 tell that he was the one, the robber.

18 THE COURT: So why did you ask for further
19 information on all 19?

20 MR. JUDISH: I mean, there's other
21 possibilities which need to be explored, ruled out,
22 like having co-conspirators. And so I think that a
23 lot of that is -- that is helpful to, you know --
24 investigators tend to be thorough. And they wanted
25 to, you know, be able to get that information because,

1 you know, some of that information was not entirely
2 inconsistent or, you know, some of that information,
3 you know, suggested that it had some aspect that one
4 might be a co-conspirator like, you know, data
5 suddenly halting suggesting someone turned off their
6 phone.

7 THE COURT: So, wait. I'm sorry.

8 MR. JUDISH: I think because there was a
9 possibility of co-conspirators is one possibility to
10 search or to obtain additional information.

11 THE COURT: So, I guess, then, I'm going to
12 ask you, clearly the terms of the warrant said narrow
13 it down, and your task force officer didn't. And then
14 Google said you have to narrow it down. And explain
15 to me what happened there.

16 MR. JUDISH: I mean, the warrant says attempt
17 to narrow it down. And, you know, and we ultimately
18 did narrow it down. And so I don't quite -- so, if
19 you look at the actual execution, we did narrow it
20 down. So I don't see any, as an initial matter, I
21 don't see any significance with the, you know, with
22 the fact that it was contemplated to obtain more than
23 we actually did. I don't recall what was in the
24 record regarding why we initially asked for all 19.

25 THE COURT: Well, I mean, there were other

1 things in the record like Google saying they didn't
2 think the agent knew what he was doing. That's the
3 only explanation we have it may be wrong, but that is
4 in the record. So --

5 MR. JUDISH: I don't recall. I mean, I think
6 it's really -- I'm not aware of the Fourth Amendment
7 violation from contemplating but not executing a
8 warrant in an improper way even if it would be
9 improper.

10 THE COURT: I'm just trying to get the record
11 straight.

12 MR. JUDISH: I'm sorry. I don't recall.

13 THE COURT: So how did we get to nine?

14 MR. JUDISH: Those were the ones which the
15 agent thought were most -- the greatest continued
16 relevance to the case.

17 THE COURT: And do we know why? Are there
18 parameters that direct to the agent about why?

19 MR. JUDISH: The warrant very much leaves
20 this to the government's discretion. And I say,
21 again, I think these are of no constitutional
22 significance. You know, part of the reason why is
23 definitely the question of whether these people could
24 actually be additional co-conspirators. And I think
25 that's a primary reason for a continued look at other

1 suspects.

2 THE COURT: Okay.

3 MR. JUDISH: I'll turn now to good faith if
4 you don't have further questions on the warrant
5 itself.

6 THE COURT: If I do, I'll come back to them.

7 MR. JUDISH: All right. So, suppression, the
8 Supreme Court has said, is a remedy of last resort and
9 used only where its benefits outweigh its heavy cost.
10 And what you have here really is a new investigative
11 technique.

12 So when a new investigative technique comes
13 along, there's not a lot of case law to look at
14 because -- well, there's no case law to look at. And
15 so what is an agent supposed to do?

16 And so the Fourth Circuit looked at this in
17 *McLamb* in the context of the Playpen cases, and what
18 the Fourth Circuit said is that in these, you know,
19 the agent should consult with the expert prosecutors,
20 and if they do that, then it's appropriate to apply in
21 good faith.

22 Well, it's not because it's not -- they
23 consulted with the prosecutors, and the prosecutors
24 think it's okay. And then they also take it to a
25 judge, and the judge thinks it's okay. And that's

1 exactly what Agent Hylton did in this case.

2 And I think it's worth noting, particularly
3 in the context of you going to the state magistrate,
4 that this was not the first time that Hylton had
5 obtained one of these warrants. He had actually
6 gone -- this was his fourth. It actually is in the
7 record, and we've disclosed two of those warrants to
8 the defense. The third remains under seal. That one
9 hasn't been disclosed. But he had previously gone to
10 both a United States magistrate judge and to two
11 Virginia state judges, and they hadn't raised any
12 problems with it. They had signed off on it.

13 So, what more can an agent do? The
14 prosecutors have no objection to it, a federal judge
15 has no objection to it, two state judges have no
16 objection to it. At this point it's hard to
17 understand why it would be objectively unreasonable
18 for the agent to believe that it's appropriate to seek
19 a geofence warrant.

20 That is exactly what the Fourth Circuit has
21 suggested that he do. And in *McLamb*, and under those
22 circumstances, suppression, the cost -- the harms of
23 suppression will very much outweigh the benefits. If
24 ultimately the courts -- other courts who look at this
25 decide that it shouldn't be done that way, then,

1 obviously, it's going to stop.

2 That's what -- in the *Carpenter* case, that
3 stopped the practice of using historical cell-site
4 location information. But *Carpenter* himself, the
5 Court did not ultimately suppress the cell phone
6 location information obtained and used against
7 *Carpenter* because of the good faith exception.

8 The benefits don't have to outweigh the harms
9 when you're talking about -- in the context of new
10 investigative techniques. It's also worth noting and
11 closely related to this is we heard from Google more
12 than 8,000 of these over the course of, I believe, a
13 year. So it's clear from that the decisions made by
14 the judges that Hylton has consulted with are not
15 significantly different than the decisions being made
16 by a whole host of other judges around the country,
17 state and federal.

18 Or, alternatively, we can apply the
19 traditional *Leon* good faith analysis to this. Under
20 the *Leon* good faith analysis, there's no suppression
21 if we rely on good faith on a warrant. And there's a
22 few exceptions to that, but none of those exceptions
23 really apply here.

24 And one is that the affidavit is so lacking
25 in indicia of probable cause that reliance on the

1 warrant is unreasonable.

2 But there is probable cause here. We had a
3 robbery. We had a guy with a cell phone. And the
4 affidavit linked that directly to Google having
5 evidence of the cell phone's location. And that
6 establishes a fair probability that Google had
7 evidence of crime, but it's certainly not wholly
8 lacking in indicia of probable cause. So under the
9 *Leon* good faith, the evidence should not be
10 suppressed.

11 Similarly, in terms of particularity, the
12 warrant is not so lacking in particularity that
13 reliance is unreasonable. It specifies exactly the
14 information that the warrant is seeking. The two
15 hours of location information or devices which fall
16 within this 150-meter circle during the hour of the
17 robbery. And that's really quite particular. That's
18 stuff that Google's algorithm can go through and
19 separate. It's just -- it's not wholly unreasonable
20 to think that as to a particular warrant, I mean,
21 clearly, some variation of that sort of thing
22 thousands of judges around the country are agreeing
23 that it's appropriate. And at the time there was no
24 contrary decision. And now we have just like a
25 handful of those, like there's three or four

1 magistrates who have written on this, one of whom
2 thinks it's wholly unreasonable, and others who sort
3 of based on the facts of the case think the government
4 should do a slightly better job. It doesn't suggest
5 that there's anything wholly unreasonable about the
6 government's reliance on the warrant in this case.

7 So, those cases, you know, generally suggest
8 that, certainly the Weisman decision and the Kansas
9 decision the defense just circulated, suggest that
10 there's nothing fundamentally wrong with geofence
11 warrants. The government just needs to be very
12 careful about establishing probable cause in
13 particularity.

14 By that standard, the warrant in this case
15 clearly passes the good faith. I mean, the probable
16 cause here is unusually strong because, you know, the
17 robber was seen actually carrying and using a cell
18 phone. That actually hasn't been the cases, in those
19 other cases. They've just tended to make that
20 assumption. But here we've actually got that. So
21 it's just not wholly lacking in probable cause, not
22 wholly lacking in particularity.

23 And similarly, there's no evidence here that
24 the judge abandoned his judicial role. The judge did
25 what judges are supposed to do. He reviewed the

1 affidavit and then he signed the warrant. I mean, the
2 kind of case that the Supreme Court talks about for
3 someone abandoning their judicial role is the case --
4 the example they give is *Leon*. And what that actually
5 involves is a judge who decided to help with the
6 execution of the warrant, that he actually went to the
7 scene to be searched and decided what could and
8 couldn't be seized.

9 Well, that's what the Supreme Court means
10 when it says a judge who abandons his judicial role,
11 you know, that you don't apply the *Leon* good faith.
12 And there's nothing like that here. This magistrate
13 reviewed the warrant affidavit and signed the warrant,
14 and that's entirely appropriate, and so *Leon* good
15 faith applies in this case.

16 And if you don't have any further questions,
17 we'd ask the Court to deny the suppression motion.

18 THE COURT: I do have a question. I think I
19 can discern from what you're arguing what case you
20 think I should rely on for purposes of my evaluation
21 of this case, but why don't you just tell me on the
22 record.

23 MR. JUDISH: The Harjani opinion is one
24 geofence case issued by a magistrate judge who
25 bothered to write up his opinion, and I think that

1 there's a lot to commend that. And there's also the
2 cell-tower dump. *James* is reasonable similar as a
3 case, you know, at least involving evaluation of
4 probable cause and particularity.

5 The District Court opinion in that case finds
6 that cell-tower dump warrants are appropriate.

7 THE COURT: All right. So I think I've heard
8 maybe both sides a little bit talk around or near or
9 maybe directly suggest two things. One is that this
10 warrant might be stronger if Google stored its
11 information in a different way, if it was stored by
12 location. So the question is, what's the upshot of
13 that? Does any court have the power to say that?
14 Would there have to be a congressional determination
15 to make that happen? And I think I want to ask
16 generally, I see that the government is steering away
17 from the Stored Communications Act, and I want to
18 confirm that you are resting this entirely on a
19 constitutional analysis.

20 I mean, one of the issues is, of course,
21 right, there is no statute that addresses geofencing.
22 Right? And, in fact, there's been no statute
23 addressing almost any more recent electronic
24 surveillance process because it develops so quickly
25 that almost as soon as something gets passed, say, in

1 two and a half years, it's obsolete.

2 So I want to hear what you have to say about
3 what I have the power to do or the appropriate action
4 I should be taking, and if there's any statutory
5 obligation with respect to what's going on.

6 MR. JUDISH: I do think they'll start with
7 the Stored Communications Act part. I do think this
8 compelled disclosure of the information is governed by
9 the Stored Communications Act. I just don't think it
10 matters for purposes of a motion to suppress because
11 the act itself has no statutory suppression remedy.
12 And so it just doesn't matter.

13 Whenever you get into a Fourth Amendment --
14 the Stored Communications Act matters enormously --

15 THE COURT: Wait. You have to slow down.

16 MR. JUDISH: Sorry.

17 THE COURT: Okay. Just start right over and
18 act like I don't know what you're about to say.

19 MR. JUDISH: All right.

20 The Stored Communications Act contains no
21 suppression remedy. It contains a section 18 U.S.C.
22 Section 2707, which specifies that the remedies in the
23 statute are the only available remedies for the
24 violation of the statute. And 2707 includes various
25 damages provisions, but not a suppression remedy. And

1 there are various cases confirming, in fact, there is
2 no suppression for a statutory violation.

3 And, you know, I think the *Smith* case in the
4 Ninth Circuit, I think. Anyway, but here because the
5 only issue for this court is whether the evidence
6 should be suppressed, the Court just doesn't need to
7 focus deeply on the questions of how this information
8 falls within the --

9 THE COURT: Does it need to or can't?

10 MR. JUDISH: I'm not sure why it would be
11 relevant. I mean, you certainly -- I'm never going to
12 tell a judge what it can or can't do. But I just
13 don't see the relevance to this case. I mean,
14 sometimes we can argue that that's an additional
15 reason against suppression. But, you know, like a
16 good faith reliance on a statute. But here the
17 government has not advanced that position. We have
18 argued good faith based on *Leon*.

19 So -- and as far as the structure of Google's
20 database, I don't think, you know, I never want to
21 willingly waive the government's authorities or
22 powers, but I'm certainly not in a position of making
23 any claim that a court has authority to tell them how
24 to structure their database.

25 I think the main argument that we make based

1 on the structure of their database is the argument
2 that Fourth Amendment rights should not turn on
3 internal prior practices which are not visible to the
4 public, and the structure of their database is one of
5 those things. And, thus, the fact that this could be
6 done in a way which would allow Google to -- Google's
7 machines to filter very narrowly, strongly suggests
8 that there is no search of millions of people when its
9 database requires a broader filter.

10 THE COURT: And with respect to -- does the
11 government have any position about whether or not a
12 review at each step by a neutral magistrate would be
13 necessary or beneficial or better?

14 MR. JUDISH: I mean, I think if we can, as I
15 believe we did here, establish probable cause for all
16 of the evidence from the start, it's fine to do so. I
17 don't think it does any harm to have additional steps.
18 It could be structured to require to have a magistrate
19 make an additional finding along the way, and there
20 would be no problem with that.

21 So I think it's not necessary, but not in any
22 way problematic to involve a magistrate in multiple
23 decisions.

24 THE COURT: Right. And so if -- I guess I
25 want you to unpack exactly why the ability to delete

1 the information, if Mr. Chatrie could figure that out,
2 how it affects my analysis.

3 MR. JUDISH: I think one way it affects your
4 analysis is it distinguishes this from *Carpenter* and
5 why *Carpenter* said the third-party doctrine didn't
6 apply. *Carpenter* had three reasons for why third
7 party didn't apply to cell-site information. One of
8 them was that it could be deleted.

9 THE COURT: All right. And so I'm not quite
10 sure how to phrase this, but -- so if there's probable
11 cause here, obviously, there's video surveillance that
12 a robbery occurred. Is the government's position that
13 there would still be probable cause to do this
14 geofence if there were no video or any indication that
15 Mr. Chatrie had a phone?

16 MR. JUDISH: It can be. I mean, cell-tower
17 dumps in the *James* case, for example, there was no
18 evidence that the defendant had a phone, and the Court
19 still found that probable cause was established. I
20 mean, probable cause is a common sense determination
21 by the magistrate whether there's a fair probability
22 that the target had prior evidence of crime. And so
23 you certainly can have that.

24 In another of the cases, I think the Harjani
25 opinion, that involves criminal activity of the sort

1 that it looks like it was probably more than one
2 person involved, and so that gives rise to an
3 inference of a likely cooperation among people, and
4 people use cell phones to communicate and cooperate.
5 So you have to look at the facts of any particular
6 case and make a determination of whether they
7 establish a fair probability.

8 So sometimes I think you can establish
9 probable cause regardless of whether a person has a
10 phone. It's really --

11 THE COURT: So I guess I'm trying to find out
12 where it stops. Like when don't you have probable
13 cause if you don't have evidence of using a phone,
14 probable cause for a geofence?

15 MR. JUDISH: I think it's really -- it's -- I
16 think it just depends on the facts of the case and
17 whether you think there will be evidence of crime.
18 And this is a determination made by magistrate judges.
19 This court obviously doesn't need to confront that in
20 this case because this is a case with a cell phone.
21 But I do think that, you know, the fact that if there
22 really is, you know, a fair probability that Google
23 will have location information of someone who
24 committed a crime, a warrant should issue, and it
25 shouldn't be an argument that, well, that happens a

1 lot. It is true that we're able to solve lots of
2 crimes because we establish probable cause in lots of
3 circumstances. That is an affirmatively good thing.

4 So I don't think that an argument I've seen
5 from at least one magistrate judge in the recent
6 Kansas opinion that we can't have too many of these
7 geofence warrants is correct. I think the issue is,
8 can we establish probable cause? And you can't say
9 this isn't probable cause because you're going to
10 solve too many crimes that way.

11 THE COURT: I think that's a little different
12 from saying when isn't there probable cause, right? I
13 mean, no one is going to say let's not solve crimes.
14 Right?

15 MR. JUDISH: Right.

16 THE COURT: Defense counsel is not going to
17 say that. That's not what they're arguing.

18 MR. JUDISH: I apologize, Your Honor. I
19 guess the way I should say it, the Court seems to
20 think that warrants shouldn't issue because they would
21 issue in too many cases, and -- but that's not --

22 THE COURT: I'm not asking that question.
23 I'm asking when doesn't it issue? I'm saying, give me
24 an example.

25 MR. JUDISH: I mean, there's -- I mean, I

1 guess you could have an example where it's clear that
2 a guy wasn't carrying a cell phone. You know, if
3 someone walks in with, you know, pocketless gym shorts
4 and a T-shirt and commits a crime, you can probably
5 tell by looking at him or from video surveillance
6 footage that there is no phone on this guy. And in
7 that case, I think there wouldn't be probable cause.

8 THE COURT: All right. Okay. I think that's
9 it.

10 MR. JUDISH: All right. Thank you, Your
11 Honor.

12 THE COURT: Can I ask you how long you think
13 your response is going to be?

14 MR. PRICE: I will try and keep it very
15 brief, Your Honor.

16 THE COURT: Well, that is about as particular
17 as whether it's granular.

18 MR. PRICE: Sorry about that. I have three
19 points. I think less than 10 minutes.

20 THE COURT: Okay.

21 MR. PRICE: Counsel tells me maybe 15.

22 THE COURT: Maybe 15. All right. I'm going
23 to give Ms. Daffron a little bit of a break. I just
24 think that, you know, maybe she'll buy me a cupcake
25 after.

1 All right. We'll take a 15-minute recess.

2 (Recess taken from 2:22 p.m. until **2:40 p.m.**)

3 MR. JUDISH: Your Honor, I just want to make
4 -- correct the transcript in one place. I did not do
5 a great job explaining this.

6 THE COURT: That's fine. Please approach the
7 podium to do that.

8 MR. JUDISH: Thank you, Your Honor.

9 Regarding the reasons behind the second stage
10 of the search, they are explained by Agent D'Errico at
11 page 546 of the transcript. So I'll stop there.

12 THE COURT: Wait. I'm sorry.

13 MR. JUDISH: Okay. So -- all right. I won't
14 stop there.

15 THE COURT: Yes.

16 MR. JUDISH: So, Agent D'Errico was asked why
17 go back at the second stage. And at 546, he says
18 there are several reasons. I know I need to talk more
19 slowly. I'm sorry.

20 So the first reason is, this is a device that
21 was present in the area of the bank prior to the bank
22 robbery. And we know that sometimes when people want
23 to hide their location, they will turn their phones
24 off. And if their phone is turned off, no additional
25 location history would be reported for that device.

1 So it's significant to us that there is a point inside
2 the geofence that occurred prior to the bank robbery
3 with no points after the bank robbery because we also
4 believe that after a subject has robbed a bank, that
5 they are going to flee the area and not have any
6 additional location history records within the
7 geofence several minutes after the bank robbery.

8 THE COURT: All right.

9 MR. JUDISH: That's all, Your Honor.

10 THE COURT: All right. Thank you, sir.

11 MR. PRICE: Good afternoon, Your Honor. Can
12 you hear me okay?

13 THE COURT: I can.

14 MR. PRICE: All right. I'd like to begin by
15 correcting a few points for the record.

16 The first is that radius targeting, which is
17 that form of advertising the government was talking
18 about, does not use location history according to
19 Google.

20 THE COURT: Wait. Say that again. Radius --

21 MR. PRICE: Radius targeting, this idea that
22 you can advertise to everybody around the courthouse
23 if you're a lawyer. While that may be possible,
24 Google has stated -- it's at page 197 to 98 of the
25 transcript -- that location history is not used for

1 that purpose.

2 Second, with respect to traffic predictions,
3 once again, pages 407 to 408 of the transcript
4 explains how Google does not use location history but
5 uses aggregated data and percentages with added,
6 quote, noise to prevent any possibility of ID'ing
7 individual devices.

8 And then, finally, with respect to the
9 questions about how the government narrowed things
10 down in Step 2 and then Step 3, we should note that
11 one of the three finalists, so to speak, was, in fact,
12 one of the false positives. So somebody who was just
13 driving by, likely never within that geofence at all,
14 and was reported as being inside of it, therefore it
15 had Stage 2 data under the government's reveal, and
16 then Stage 3 data as well. That was one of the false
17 positives.

18 THE COURT: Okay.

19 MR. PRICE: So I want to touch briefly on a
20 few points.

21 First, this idea that location history is
22 voluntary because of the process involved, and the
23 mere fact that it is stored with Google, a third
24 party.

25 Almost everything the government said about

1 the voluntariness of enabling location history can be
2 said of Gmail, of Google email. It is stored by
3 Google. It is transmitted by Google. Google
4 advertises off of emails. And yet even the government
5 agrees that email deserves Fourth Amendment
6 protection. I suppose they have to after the Six
7 Circuit's decision in *Warshak* and their representation
8 to the Supreme Court in *Carpenter* that email requires
9 a warrant to get.

10 That is not something that the Supreme Court
11 has weighed in on. And under a strict reading of the
12 Stored Communications Act, as it still exists, the
13 government did, in fact, argue they did not need a
14 warrant to obtain email that was older than 180 days.

15 The Sixth Circuit in *United States v. Warshak*
16 found that email, despite being housed on Google's
17 servers or on other servers, deserved the same kind of
18 privacy as one's papers and effects. That is the
19 modern day scion of one's private papers and effects.

20 All of those points we can attribute, as
21 well, to location history. The Stored Communications
22 Act, while not determinative, is certainly relevant to
23 the reasonable expectation of privacy analysis.

24 Google considers location history to be
25 content and users understand that content is their

1 data and it is protected from unauthorized disclosure.

2 Likewise, this is different from a subpoena,
3 fundamentally different from a subpoena, because
4 Google is not searching its own business records. The
5 government is not asking to search preexisting records
6 that Google already has in the same way that a cell
7 company might have data about how many people use a
8 tower in order to figure out whether to add another
9 tower or why calls might be getting dropped.

10 Google never runs a search to figure out who
11 was around the bank or who was around. They don't
12 have towers. They have no need for this, to have
13 location data sorted by location. It is considered,
14 once again, user content, and that is why the
15 database -- the Sensorvault is structured in that way.
16 It is a reflection of this idea that location history
17 is content. It belongs to users. It is their data.
18 They can manipulate it. They can delete it. It is
19 not Google's data.

20 I want to touch briefly on the idea that
21 *Carpenter* hasn't been applied or expanded since
22 *Carpenter* was decided. The government cites *Hammond*,
23 which is a case about realtime cell-site information,
24 as well as historical cell-site information; 127 days
25 of it actually. And there the Court found that a

1 search of the 127 days of historical cell-site
2 information was a search, but that the good faith
3 doctrine applied. Why? Because the 2703(d) order was
4 issued prior to *Carpenter* being decided.

5 So, in fact, the vast majority of cases that
6 have been decided since *Carpenter* follow a similar
7 pattern recognizing that these cases take some time to
8 percolate up. And some of the searches that we're
9 still seeing right now were executed prior to June of
10 2018.

11 So those cases are just coming up now, and
12 the vast majority of them holding that *Carpenter*
13 doesn't apply do so on good faith grounds.

14 The other case that the government cites,
15 also a Seventh Circuit case, *Adkinson*, did involve a
16 tower dump, but the government didn't conduct it. The
17 suspect in that case, the defendant in that case, was
18 accused of robbing multiple T-Mobile stores. So
19 T-Mobile, on its own, looked at its own cell-site
20 records to try and figure out which T-Mobile customers
21 had used their towers near those stores. So it wasn't
22 government action in the same way that we have here.

23 And I think that leads in nicely to this
24 larger point that Google was acting as a government
25 agent. There would be no Step 1 data without Google's

1 participation. And Google would not have done any of
2 this had it not received compulsory legal process.
3 Google, in this sense, can't be anything but a
4 government agent at Step 1. The government is
5 outsourcing the search function to Google. It's that
6 simple.

7 Finally, I want to touch on the *McLamb*
8 Playpen good faith argument. As Your Honor correctly
9 pointed out, that case turned -- was based on the fact
10 that there was probable cause for every computer that
11 was searched. So the issue there was not probable
12 cause. The issue in *McLamb* was a very complicated
13 jurisdictional question about the reach of Rule 41 and
14 whether judges in one district could issue warrants
15 that applied extraterritorially to other
16 jurisdictions.

17 At the time there were multiple conflicting
18 court decisions in the country about this. And it
19 was, admittedly, something of a close call. So in
20 that case, consulting with attorneys and prosecutors
21 would make a lot of sense. But there was no question
22 about whether probable cause was necessary. That is a
23 fundamental question, a fundamental Fourth Amendment
24 question that has to be answered in every single case.
25 And it is antithetical, I think, to the Fourth

1 Amendment to say that the government can get away with
2 a warrant that doesn't have probable cause or lacks
3 particularity simply because they checked with the
4 prosecutor.

5 That rule, if read that broadly, would
6 eviscerate the Fourth Amendment. Anything that a
7 government agent wanted to do, they could just clear
8 with the prosecutor, and so it would be good faith at
9 the end of the day. I don't think that's the rule in
10 *McLamb*.

11 Once again, the Court was not looking at a
12 basic question like were these warrants supported by
13 probable cause. It was a very technical, legal
14 question about the reach of Rule 41.

15 THE COURT: Well, to be clear, they're saying
16 that, regardless of anything in *McLamb*, they had
17 probable cause here because they had a video of
18 somebody robbing a bank using a phone.

19 MR. PRICE: I don't think that having a phone
20 in and of itself is enough to establish probable
21 cause. If only a third of Google users have location
22 history enabled, and not all people who have cell
23 phones have Google phones, and some of the people who,
24 because of the way that the 68, 32 percent error rate
25 works, at least some of those people who might have

1 been there will not show up there within the geofence
2 because of this idea of false positives and false
3 negatives. So I think there's actually a few more
4 steps to do to go from having a phone to probable
5 cause.

6 And as we know from *Riley*, and the
7 government's own statistics, having a cell phone is a
8 fairly common thing. And I have no doubt that in a
9 case where the suspect was not seen with a cell phone,
10 perhaps wearing gym shorts and a T-shirt, that the
11 government would say he left the phone in his car or
12 that they might need to get a warrant or look for
13 witnesses or co-conspirators anyways.

14 I think there is a lot of work to be done on
15 the probable cause front to go from a cell phone was
16 seen to there's probable cause for searching location
17 history.

18 THE COURT: Okay.

19 MR. PRICE: That's all. Thank you very much,
20 Your Honor.

21 THE COURT: I'm going to ask you one question
22 based on their argument. It seems that part of what
23 they're saying is that the probable cause was based on
24 the fact that there was a crime and that getting the
25 results of the geofence would help reconstruct the

1 crime. That it's just an investigative tool. And so
2 there's probable cause to know that the way that folks
3 were operating around, it's just a different type of
4 surveillance, and that it would, at least probably,
5 show evidence that a crime had been committed.

6 MR. PRICE: I think there's a lot of
7 information that might be helpful in the abstract.
8 And nobody is preventing the government from obtaining
9 this information. The idea is simply that they must
10 have probable cause to do it.

11 So it may be useful to get the location
12 history data of people inside the bank, but then
13 identify those people inside the bank and seek a
14 warrant for their location history information if all
15 you're trying to do is just get a better sense of the
16 scene. In the same way that you would go and identify
17 the surveillance cameras in the area and get the video
18 from there, you wouldn't start with every surveillance
19 video camera in the country, and then narrow it down
20 to the ones around the bank.

21 So I think while there may be lots of
22 information that's useful in terms of solving crimes,
23 the Fourth Amendment limits what the government can
24 get based on probable cause and particularity. Thank
25 you.

1 THE COURT: Thank you.

2 All right. Well, I want to thank you all for
3 your efforts and for your argument.

4 I am, not surprisingly, going to issue a
5 written opinion. You all have submitted lots of
6 documents, and I've heard testimony, and I want to be
7 sure you have a decision that you can read and either
8 agree with or disagree with, and then move on from
9 there.

10 I certainly will do so as swiftly as I can.
11 And, certainly, we've been working on it, and we will
12 continue working on it. So we're not behind the ball,
13 but we're not where you guys are. We haven't
14 finishing our briefing.

15 So how is it, with that understood, how is it
16 that you want to proceed?

17 MS. KOENIG: Good afternoon, Your Honor.

18 THE COURT: Good afternoon.

19 MS. KOENIG: I think Ms. Daffron is probably
20 grateful that I wasn't talking very much today.

21 But I think in terms of the defense
22 perspective, obviously there are other motions that
23 are pending. I will say that the Court's
24 determination of this motion, I think, will make
25 dispositive some other issues in the case regardless

1 of how the Court rules.

2 So from the defense perspective, I would ask
3 that the Court continue to hold the other motions in
4 abeyance until after the decision on this motion. I
5 don't believe at this point we need to reset a trial,
6 but if that becomes necessary, obviously we can do
7 that once the Court makes a decision.

8 THE COURT: Right. Does the government have
9 a perspective?

10 MR. SIMON: Judge, we don't mind the Court
11 holding those motions in abeyance. To the extent the
12 Court wanted to rule from the four corners of the
13 search warrant, I don't believe we intend to elicit
14 additional evidence on those motions. So we'll just
15 defer to the Court on whether it holds it in abeyance
16 or not.

17 THE COURT: All right.

18 Well, what I will certainly do is not rule on
19 those issues without notice. I think that's fair.
20 And so I will decide this particular motion, which is
21 clearly the heart of what we're discussing, and then
22 we will handle the other motions accordingly, but not
23 by surprise. So you can presume that I would handle
24 it that way.

25 I'm not going to schedule a trial date. So

1 this means that this motion is under advisement,
2 including all the findings that I've made with respect
3 to the complexity of the case, the fact that we've had
4 testimony from across the country, unusual sets of
5 affidavits.

6 It is the fact that the speedy trial
7 continues to be held in abeyance for a bit because it
8 outweighs the public's interest in a speedy trial, and
9 Mr. Chatrie's, given the weight and the seriousness of
10 the issues before me.

11 But I do tell you all that we are on it, and
12 I am aware that, especially with COVID and with folks
13 being unable to travel from California to testify in
14 person, that this is an unusually long pendency in a
15 case, and I am taking that into account as I approach
16 it. All right?

17 Is there anything else I need to cover?

18 MR. SIMON: Nothing further, Judge.

19 MS. KOENIG: Not from the defense, Your
20 Honor. Thank you.

21 THE COURT: All right. Well, you all have
22 done a tremendous job. And thank you for your time,
23 and I will issue my opinion. Thank you.

24 (The proceedings were adjourned at 3:00 p.m.)

25 I, Diane J. Daffron, certify that the foregoing is

1 a correct transcript from the record of proceedings
2 in the above-entitled matter.

3 /s/

4 _____
5 DIANE J. DAFFRON, RPR, CCR

6 _____
7 DATE

This page intentionally left blank for double-sided pagination and printing