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 1 of 11 (pages 1 - 176)

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)

VOLUME 2 (pages 177 - 416)

VOLUME 3 (pages 417 - 694)

VOLUME 4 (pages 695 - 1070)

VOLUME 5 (pages 1071 - 1326)

APPEAL,CLOSED

U.S. District Court
Eastern District of Virginia – (Richmond)
CRIMINAL DOCKET FOR CASE #: 3:19–cr–00130–MHL–1

Case title: USA v. Chatrie

Date Filed: 09/17/2019
Date Terminated: 08/19/2022

Assigned to: District Judge M. Hannah Lauck

Appeals court case number: 22–4489

Defendant (1)

Okello T. Chatrie
TERMINATED: 08/19/2022

represented by **Laura Jill Koenig**
Office of the Federal Public Defender (Richmond)
701 E Broad Street
Suite 3600
Richmond, VA 23219
(804) 343–0800
Email: laura_koenig@fd.org
LEAD ATTORNEY
ATTORNEY TO BE NOTICED
Designation: Public Defender

Michael William Price
National Association of Criminal Defense Lawyers
1660 L Street NW
12th Floor
Washington, DC 20036
NA
(202) 465–7615
Fax: (202) 872–8690
Email: mprice@nacdl.org
PRO HAC VICE
ATTORNEY TO BE NOTICED
Designation: Public Defender

Paul Geoffrey Gill
Office of the Federal Public Defender (Richmond)
701 E Broad Street
Suite 3600
Richmond, VA 23219
804–343–0800
Email: Paul_Gill@fd.org
ATTORNEY TO BE NOTICED

Pending Counts	**Disposition**
18;2113(a), 2113(d) and 2113(e); In accordance with 18;924(d) and 981(a)(1)(C) as incorporated by 28;2461(c) – FORCED ACCOMPANIMENT DURING AN ARMED CREDIT UNION ROBBERY; FORFEITURE ALLEGATION (1)	DISMISSED ON MOTION OF GOVT.

18 U.S.C. §§ 2113(a) and 2113(d); ARMED CREDIT UNION ROBBERY; FORFEITURE ALLEGATION (1s)	57 MONTHS IMPRISONMENT, 3 YEARS SUPERVISED RELEASE, $100 S/A, $196,932.01 RESTITUTION
18;924(c)(1)(A)(i) and (ii); In accordance with 18;924(d) and 981(c)(1)(C) as incorporated by 28;2461(c) – USE, CARRY AND BRANDISH A FIREARM DURING AND IN RELATION TO A CRIME OF VIOLENCE; FORFEITURE ALLEGATION (2)	DISMISSED ON MOTION OF GOVT.
18 U.S.C. § 924(c)(1)(A)(i) and (ii); USE, CARRY, AND BRANDISH A FIREARM DURING AND IN RELATION TO A CRIME OF VIOLENCE; FORFEITURE ALLEGATION (2s)	84 MONTHS IMPRISONMENT TO BE SERVED CONSECUTIVE TO CT. 1, 3 YEARS SUPERVISED RELEASE TO BE SERVED CONCURRENT TO CT. 1, $100 S/A

Highest Offense Level (Opening)

Felony

Terminated Counts	**Disposition**
None	

Highest Offense Level (Terminated)

None

Complaints	**Disposition**
None	

Movant

Google, LLC
TERMINATED: 08/19/2022

represented by **Brittany Blueitt Amadi**
Wilmer Cutler Pickering Hale & Dorr LLP (DC)
1875 Pennsylvania Ave NW
Washington, DC 20006
202–663–6022
Fax: 202–663–6363
Email: brittany.amadi@wilmerhale.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED
Designation: Retained

Alex Campbell Hemmer
Wilmer Cutler Pickering Hale & Dorr LLP (DC–NA)
1875 Pennsylvania Ave NW
Washington, DC 20006
NA
(202) 663–6387
Fax: (202) 663–6363
Email: alex.hemmer@wilmerhale.com

TERMINATED: 01/19/2021
PRO HAC VICE
Designation: Retained

Catherine Mary Agnes Carroll
Wilmer Cutler Pickering Hale & Dorr, LLP (DC)
1875 Pennsylvania Avenue NW
Washington, DC 20006
202–663–6000
Fax: 202–663–6363
Email: Catherine.Carroll@wilmerhale.com
ATTORNEY TO BE NOTICED
Designation: Retained

Movant

Magistrate Judge David M. Bishop
TERMINATED: 08/19/2022

represented by **Rachel Lynsie Yates**
Office of the Attorney General
202 North 9th Street
Richmond, VA 23219
804–692–0552
Email: ryates@oag.state.va.us
LEAD ATTORNEY
ATTORNEY TO BE NOTICED
Designation: Retained

Donald Eldridge Jeffrey , III
Office of the Attorney General
202 North 9th Street
Richmond, VA 23219
(804) 786–2071
Email: djeffrey@oag.state.va.us
ATTORNEY TO BE NOTICED

Plaintiff

USA

represented by **Kenneth R. Simon , Jr.**
United States Attorney's Office (Richmond)
SunTrust Building
919 East Main Street
Suite 1900
Richmond, VA 23219
(804) 819–5400
Email: Kenneth.Simon2@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED
Designation: US Attorney

Nathan Paul Judish
United States Department of Justice
Computer Crime and Intellectual Property Section
950 Pennsylvania Ave NW
Washington, DC 20530
NA
(202) 616–7203
Fax: (202) 514–6113
Email: nathan.judish@usdoj.gov
PRO HAC VICE
ATTORNEY TO BE NOTICED
Designation: US Attorney

Peter S. Duffey
United States Attorney's Office
(Richmond)
SunTrust Building
919 East Main Street
Suite 1900
Richmond, VA 23219
(804) 819–5400
Email: peter.duffey@usdoj.gov
ATTORNEY TO BE NOTICED
Designation: US Attorney

Date Filed	#	Docket Text
09/17/2019	1	INDICTMENT as to Okello T. Chatrie (1) counts 1, 2. (smej,) (Entered: 09/18/2019)
09/17/2019	3	Minute Entry as to Okello T. Chatrie: Before Magistrate Judge David J. Novak. Appearances: Stephen Miller, AUSA and Sheldon Poe, GJR. Indictment, a true bill, returned before a Magistrate Judge at Richmond. Government's motion for the issuance of an arrest warrant heard and so–ordered. (smej,) (Entered: 09/18/2019)
09/18/2019	4	Arrest Warrant Issued (as detainer) in case as to Okello T. Chatrie. Clerk placed in USM box for service. (smej,) (Entered: 09/18/2019)
09/20/2019	5	Petition and Order for Writ of Habeas Corpus ad Prosequendum as to Okello T. Chatrie for September 26, 2019 at 2:05 P.M.. Signed by Magistrate Judge David J. Novak on 09/20/2019. (smej,) (Entered: 09/20/2019)
09/20/2019	6	Writ of Habeas Corpus ad Prosequendum Issued as to Okello T. Chatrie for 09/26/2019 at 2:05 P.M.. Clerk placed in USM box for service. (smej,) (Entered: 09/20/2019)
09/26/2019		Oral ORDER APPOINTING FEDERAL PUBLIC DEFENDER as to Okello T. Chatrie. Laura Jill Koenig for Okello T. Chatrie appointed by Magistrate Judge David J. Novak on 9/26/2019. (cgar) (Entered: 09/26/2019)
09/26/2019	8	Minute Entry for proceedings held before Magistrate Judge David J. Novak:Initial Appearance as to Okello T. Chatrie held on 9/26/2019. Matter came on for initial appearance on Indictment. Deft advised of charges/penalties and rights. Deft requested c/a counsel. Financial affidavit executed. Carolyn V. Grady, AFPD present. FPD appointed. Govt's motion to detain deft GRANTED. Detention hearing set for 10/1/2019 at 2:05. Arraignment set for 10/1/2019 at 2:30 p.m. Deft remanded to custody. (Tape #FTR.)(cgar) (Entered: 09/26/2019)
09/26/2019		Set Hearings as to Okello T. Chatrie: Arraignment set for 10/1/2019 at 02:30 PM in Richmond Courtroom 6100 before District Judge M. Hannah Lauck. Detention Hearing set for 10/1/2019 at 02:05 PM in Richmond Courtroom 5400 before Magistrate Judge David J. Novak. (cgar) (Entered: 09/26/2019)
09/26/2019	9	CJA 23 Financial Affidavit by Okello T. Chatrie. (cgar) (Entered: 09/26/2019)
09/26/2019	10	ARREST Warrant Returned Executed on 9/26/2019 as to Okello T. Chatrie. (cgar) (Entered: 09/26/2019)
09/26/2019	11	Temporary Detention Order as to Okello T. Chatrie. Signed by Magistrate Judge David J. Novak on 9/26/2019. (cgar) (Entered: 09/27/2019)
10/01/2019	12	Minute Entry for proceedings held before Magistrate Judge David J. Novak:Detention Hearing as to Okello T. Chatrie held on 10/1/2019. Matter came on for detention hearing. Deft waived detention hearing. Waiver executed. Arraignment set for today at 2:30 p.m. Deft ordered held pending trial. (Tape #FTR.)(cgar) (Entered: 10/01/2019)
10/01/2019	13	WAIVER of Detention Hearing by Okello T. Chatrie. (cgar) (Entered: 10/01/2019)
10/01/2019	14	Minute Entry for proceedings held before District Judge M. Hannah Lauck:Arraignment as to Okello T. Chatrie (1) Count 1,2 held on 10/1/2019. Dft waived formal reading of the Indictment, entered a plea of not guilty and requested a

		trial by jury. Agreed Discovery Order entered. Jury Trial scheduled for December 3–5, 2019 at 9:00 a.m. (Court Reporter Diane Daffron, OCR.)(khan,) (Entered: 10/02/2019)
10/01/2019	15	Agreed Discovery Order as to Okello T. Chatrie. Signed by District Judge M. Hannah Lauck on 10/1/19. (khan,) (Entered: 10/02/2019)
10/01/2019	16	Detention Order Pending Trial as to Okello T. Chatrie. Signed by Magistrate Judge David J. Novak on 10/1/2019. (cgar) (Entered: 10/02/2019)
10/02/2019		Set/Reset Hearings as to Okello T. Chatrie: Jury Trial set for 12/3/2019 at 09:00 AM in Richmond Courtroom 6100 before District Judge M. Hannah Lauck. (khan,) (Entered: 10/02/2019)
10/22/2019	17	MOTION in Limine *of Irrelevant and Unduly Prejudicial Character Evidence* by Okello T. Chatrie. (Koenig, Laura) (Entered: 10/22/2019)
10/22/2019	18	MOTION to Suppress *Evidence Obtained from Willis Street Search* by Okello T. Chatrie. (Koenig, Laura) (Entered: 10/22/2019)
10/22/2019	19	MOTION to Suppress *Evidence Obtained from Mason Dale Drive Search* by Okello T. Chatrie. (Koenig, Laura) (Entered: 10/22/2019)
10/22/2019	20	MOTION to Suppress *Evidence Obtained from Mr. Chatrie's Google Accounts Search* by Okello T. Chatrie. (Koenig, Laura) (Entered: 10/22/2019)
10/22/2019	21	MOTION to Suppress *Evidence Obtained from Buick Lacrosse Search* by Okello T. Chatrie. (Koenig, Laura) (Entered: 10/22/2019)
10/22/2019	22	MOTION to Suppress *Evidence Obtained from Cell Site Simulator* by Okello T. Chatrie. (Koenig, Laura) (Entered: 10/22/2019)
10/22/2019	23	MOTION for Discovery *Regarding Government's Use of Cell Site Simulator* by Okello T. Chatrie. (Koenig, Laura) (Entered: 10/22/2019)
10/22/2019	24	Consent MOTION for Extension *of Motions Deadline on One Issue that Will Result in Two Additional Motions* by Okello T. Chatrie. (Attachments: # 1 Proposed Order)(Koenig, Laura) (Entered: 10/22/2019)
10/23/2019	25	ORDER – It is hereby ORDERED that the Defendant's Motion to Extend Motions Deadline on One Issue Which Will Result in Two Additional Motions in this case is GRANTED. The defense shall file the two additional motions relating to the state search warrant using "geofencing" and Google's "sensorvault" data by October 29, 2019. The government's response deadline and the defense's reply deadline are adjusted accordingly. Signed by District Judge M. Hannah Lauck on 10/23/2019. (smej,) (Entered: 10/23/2019)
10/29/2019	26	Motion to appear Pro Hac Vice by Michael William Price and Certification of Local Counsel Laura Jill Koenig by Okello T. Chatrie. (Attachments: # 1 Proposed Order Pro Hac Vice Application)(Koenig, Laura) (Entered: 10/29/2019)
10/29/2019		Notice of Correction re 26 Motion to appear Pro Hac Vice by Michael William Price and Certification of Local Counsel Laura Jill Koenig: Clerk has notified filing attorney of proper filing procedures for pro hac vice motions. No further action is required. (smej,) (Entered: 10/29/2019)
10/29/2019	27	ORDER granting 26 Motion for Michael William Price to appear as Pro hac vice for Okello T. Chatrie. Signed by District Judge M. Hannah Lauck on 10/29/2019. (smej,) (Entered: 10/29/2019)
10/29/2019	28	MOTION for Discovery *Regarding Government's Use of Google's Sensorvault Data* by Okello T. Chatrie. (Koenig, Laura) (Entered: 10/29/2019)
10/29/2019	29	MOTION to Suppress *Evidence Obtained from a "Geofence" General Warrant* by Okello T. Chatrie. (Koenig, Laura) (Entered: 10/29/2019)
10/31/2019	30	Consent MOTION for Extension of Time to File Response/Reply as to 28 MOTION for Discovery *Regarding Government's Use of Google's Sensorvault Data*, 17 MOTION in Limine *of Irrelevant and Unduly Prejudicial Character Evidence*, 18

		MOTION to Suppress *Evidence Obtained from Willis Street Search*, 20 MOTION to Suppress *Evidence Obtained from Mr. Chatrie's Google Accounts Search*, 19 MOTION to Suppress *Evidence Obtained from Mason Dale Drive Search*, 21 MOTION to Suppress *Evidence Obtained from Buick Lacrosse Search*, 29 MOTION to Suppress *Evidence Obtained from a "Geofence" General Warrant*, 23 MOTION for Discovery *Regarding Government's Use of Cell Site Simulator*, 22 MOTION to Suppress *Evidence Obtained from Cell Site Simulator* by USA as to Okello T. Chatrie. (Attachments: # 1 Proposed Order Proposed Order)(Simon, Kenneth) (Entered: 10/31/2019)
11/01/2019	31	ORDER as to Okello T. Chatrie that the Court GRANTS the United States' 30 motion for extension of time. Accordingly, the United States must respond to the defendant's motions on or before November 19, 2019. See Order for details. Signed by District Judge M. Hannah Lauck on 11/1/2019. (jsmi,) (Entered: 11/01/2019)
11/07/2019	32	ORDER – This matter comes before the Court on the Parties' joint request for a status hearing. At **11:00 a.m. on November 12, 2019**, the Parties SHALL appear in Courtroom 6100 of the Spottswood W. Robinson III and Robert R. Merhige, Jr. United States Courthouse for an in–person status conference to discuss the trial date in this matter. Signed by District Judge M. Hannah Lauck on 11/07/2019. (smej,) (Entered: 11/07/2019)
11/07/2019		Set/Reset Hearings as to Okello T. Chatrie: Status Conference set for 11/12/2019 at 11:00 AM in Richmond Courtroom 6100 before District Judge M. Hannah Lauck. (khan,) (Entered: 11/07/2019)
11/12/2019	33	NOTICE OF ATTORNEY APPEARANCE: Paul Geoffrey Gill appearing for Okello T. Chatrie (Gill, Paul) (Entered: 11/12/2019)
11/12/2019	34	Minute Entry for proceedings held before District Judge M. Hannah Lauck:Status Conference as to Okello T. Chatrie held on 11/12/2019. Oral Motion to Delay Reply until 12/9/19 – GRANTED. Dft's Motion for Continuance of Trial Beyond the Speedy Trial Act Cut–Off Date – GRANTED. Status Conference set 12/12/19 at 2:00 p.m. Dft remanded to custody. (Court Reporter Diane Daffron, OCR.)(khan,) (Entered: 11/12/2019)
11/12/2019		Set/Reset Hearings as to Okello T. Chatrie: Status Conference set for 12/12/2019 at 02:00 PM in Richmond Courtroom 6100 before District Judge M. Hannah Lauck. (khan,) (Entered: 11/12/2019)
11/12/2019	35	MOTION for Continuance of Trial Beyond the Speedy Trial Act Cut–Off Date by Okello T. Chatrie. (khan,) (Entered: 11/18/2019)
11/12/2019		ORAL ORDER as to Okello T. Chatrie granting 35 MOTION for Continuance of Trial Beyond the Speedy Trial Act Cut–Off Date filed by Okello T. Chatrie. Signed by District Judge M. Hannah Lauck on 11/12/19. (khan,) (Entered: 11/18/2019)
11/19/2019	36	MOTION for Leave to File Excess Pages by USA as to Okello T. Chatrie. (Attachments: # 1 Proposed Order)(Simon, Kenneth) (Entered: 11/19/2019)
11/19/2019	37	RESPONSE in Opposition by USA as to Okello T. Chatrie re 18 MOTION to Suppress *Evidence Obtained from Willis Street Search*, 19 MOTION to Suppress *Evidence Obtained from Mason Dale Drive Search* (Simon, Kenneth) (Entered: 11/19/2019)
11/19/2019	38	RESPONSE in Opposition by USA as to Okello T. Chatrie re 28 MOTION for Discovery *Regarding Government's Use of Google's Sensorvault Data* (Simon, Kenneth) (Entered: 11/19/2019)
11/19/2019	39	RESPONSE to Motion by USA as to Okello T. Chatrie re 17 MOTION in Limine *of Irrelevant and Unduly Prejudicial Character Evidence* (Simon, Kenneth) (Entered: 11/19/2019)
11/19/2019	40	RESPONSE to Motion by USA as to Okello T. Chatrie re 23 MOTION for Discovery *Regarding Government's Use of Cell Site Simulator*, 22 MOTION to Suppress *Evidence Obtained from Cell Site Simulator* (Simon, Kenneth) (Entered: 11/19/2019)

11/19/2019	41	RESPONSE in Opposition by USA as to Okello T. Chatrie re 29 MOTION to Suppress *Evidence Obtained from a "Geofence" General Warrant* (Simon, Kenneth) (Entered: 11/19/2019)
11/19/2019	42	RESPONSE in Opposition by USA as to Okello T. Chatrie re 20 MOTION to Suppress *Evidence Obtained from Mr. Chatrie's Google Accounts Search* (Simon, Kenneth) (Entered: 11/19/2019)
11/19/2019	43	RESPONSE in Opposition by USA as to Okello T. Chatrie re 21 MOTION to Suppress *Evidence Obtained from Buick Lacrosse Search* (Simon, Kenneth) (Entered: 11/19/2019)
11/20/2019	44	ORDER – For good cause shown, the Court GRANTS the United States' 36 Motion for Leave to File Excess Pages. Accordingly, the United States may file its omnibus responsive brief that is in excess of thirty pages. Signed by District Judge M. Hannah Lauck on 11/20/2019. (smej,) (Entered: 11/20/2019)
11/25/2019	45	REPLY TO RESPONSE to by Okello T. Chatrie re 18 MOTION to Suppress *Evidence Obtained from Willis Street Search*, 19 MOTION to Suppress *Evidence Obtained from Mason Dale Drive Search*, 37 Response in Opposition (Koenig, Laura) (Entered: 11/25/2019)
11/25/2019	46	REPLY TO RESPONSE to by Okello T. Chatrie re 20 MOTION to Suppress *Evidence Obtained from Mr. Chatrie's Google Accounts Search*, 42 Response in Opposition (Koenig, Laura) (Entered: 11/25/2019)
11/25/2019	47	REPLY TO RESPONSE to by Okello T. Chatrie re 43 Response in Opposition, 21 MOTION to Suppress *Evidence Obtained from Buick Lacrosse Search* (Koenig, Laura) (Entered: 11/25/2019)
11/26/2019		Jury Trial continued as to Okello T. Chatrie: (khan,) (Entered: 11/26/2019)
12/09/2019	48	REPLY TO RESPONSE to by Okello T. Chatrie re 41 Response in Opposition (Attachments: # 1 Exhibit A, # 2 Exhibit B, # 3 Exhibit C, # 4 Exhibit D)(Koenig, Laura) (Entered: 12/09/2019)
12/09/2019	49	REPLY TO RESPONSE to by Okello T. Chatrie re 38 Response in Opposition (Koenig, Laura) (Entered: 12/09/2019)
12/11/2019	50	NOTICE *Regarding Initiation of Forensic Examination* by Okello T. Chatrie (Simon, Kenneth) (Entered: 12/11/2019)
12/12/2019	52	Minute Entry for proceedings held before District Judge M. Hannah Lauck:Status Conference as to Okello T. Chatrie held on 12/12/2019. Goggle Amicus brief due 12/20/19; parties response 1/3/20. Discovery motion scheduled 1/21/20 at 11:00 a.m.; Motion to Suppress scheduled 2/21 & 21/20 at 10:00 a.m. ECF 17, 22, 23 DENIED AS MOOT WITHOUT PREJUDICE. Dft remanded to custody. (Court Reporter Diane Daffron, OCR.)(khan,) (Entered: 12/13/2019)
12/13/2019	51	ORDER – The Court DENIES AS MOOT and WITHOUT PREJUDICE Defendant Okello T. Chatrie's Motion in Limine 17 , Motion to Suppress 22 , and Motion for Discovery 23 ; SCHEDULES this matter for a hearing on **January 21, 2020, at 11:00 a.m.** regarding Chatrie's Motion for Discovery Regarding Government's Use of Google's Sensorvault Data 28 ; SCHEDULES this matter for a hearing, beginning at **10:00 a.m. on February 20, 2020, and continuing through February 21, 2020** regarding Chatrie's remaining pending motions, (ECF Nos. 18 , 19 , 20 , 21 , 29). SEE ORDER FOR DETAILS AND DEADLINES. Signed by District Judge M. Hannah Lauck on 12/13/2019. (smej,) (Entered: 12/13/2019)
12/13/2019		Set/Reset Hearings as to Okello T. Chatrie: Discovery Hearing set for 1/21/2020 at 11:00 AM in Richmond Courtroom 6100 before District Judge M. Hannah Lauck. (khan,) (Entered: 12/13/2019)
12/13/2019		Set/Reset Deadlines re Motion or Report and Recommendation in case as to Okello T. Chatrie 29 MOTION to Suppress *Evidence Obtained from a "Geofence" General Warrant*, 28 MOTION for Discovery *Regarding Government's Use of Google's Sensorvault Data*, 21 MOTION to Suppress *Evidence Obtained from Buick Lacrosse Search*, 18 MOTION to Suppress *Evidence Obtained from Willis Street Search*, 19 MOTION to Suppress *Evidence Obtained from Mason Dale Drive Search*. Motion

		Hearing set for 2/20/2020 at 10:00 AM before District Judge M. Hannah Lauck. (khan,) (Entered: 12/13/2019)
12/16/2019	53	ORDER – This matter comes before the Court on Defendant Okello T. Chatrie's Motion for Discovery Regarding Government's Use of Google's Sensorvault Data 28 . In Chatrie's reply to the United States' response to this motion, 49 , Chatrie raises several new arguments. Because a response to these new arguments from the United States would assist the Court, the United States SHALL file a sur–reply–no longer than 10 pages–no later than December 30, 2019. Signed by District Judge M. Hannah Lauck on 12/16/2019. (smej,) (Entered: 12/16/2019)
12/18/2019	54	NOTICE *of Attachment to Response in Opposition to Motion to Suppress – Google Geofence State Search Warrant* by USA as to Okello T. Chatrie re 48 Reply to Response, 29 MOTION to Suppress *Evidence Obtained from a "Geofence" General Warrant*, 41 Response in Opposition (Attachments: # 1 Exhibit)(Simon, Kenneth) (Entered: 12/18/2019)
12/19/2019	55	STATUS REPORT *regarding Filing of Search Warrants at Issue in this Matter* by USA as to Okello T. Chatrie (Simon, Kenneth) (Entered: 12/19/2019)
12/19/2019		Minute Entry for proceedings held before District Judge M. Hannah Lauck:Telephone Conference as to Okello T. Chatrie held on 12/19/2019 (Court Reporter Gil Halasz, OCR.)(khan,) (Entered: 12/19/2019)
12/19/2019	56	RESPONSE by Okello T. Chatrie re 55 Status Report (Koenig, Laura) (Entered: 12/19/2019)
12/20/2019	57	Motion to appear Pro Hac Vice by Catherine Carroll and Certification of Local Counsel Brittany Amadi (Filing fee $ 75 receipt number 0422–6996925.) by Google, LLC as to Okello T. Chatrie. (Amadi, Brittany) (Entered: 12/20/2019)
12/20/2019	58	Motion to appear Pro Hac Vice by Alex Hemmer and Certification of Local Counsel Brittany Amadi (Filing fee $ 75 receipt number 0422–6996939.) by Google, LLC as to Okello T. Chatrie. (Amadi, Brittany) (Entered: 12/20/2019)
12/20/2019	59	MOTION to File Amicus Brief *In Support Of Neither Party* by Brittany Amadi. by Google, LLC as to Okello T. Chatrie. (Attachments: # 1 Amicus Brief, # 2 Proposed Order)(Amadi, Brittany) (Entered: 12/20/2019)
12/23/2019	60	ORDER Granting Motion for Leave to File Brief of Amicus Curiae Google LLC in Support of Neither Party. Having considered the motion of proposed amicus curiae Google LLC for leave to file an arnicus brief, and good cause appearing, it is hereby ORDERED that the motion is GRANTED. The Clerk is directed to accept the proposed arnicus brief for filing. SO ORDERED. Signed by District Judge M. Hannah Lauck on 12/23/2019. (sbea,) (Entered: 12/23/2019)
12/23/2019	61	REPLY TO RESPONSE to USA as to Okello T. Chatrie re 56 Response *to Status Report regarding Filing Search Warrants at Issue* (Simon, Kenneth) (Entered: 12/23/2019)
12/23/2019	73	Amicus Brief by Google, LLC as to Okello T. Chatrie. Filed per Order entered 12/23/2019. (smej,) Modified on 1/13/2020 (smej,). (Entered: 01/13/2020)
12/30/2019	62	ORDER granting 57 Motion for Catherine Mary Agnes Carroll to appear as Pro hac vice for Google, LLC as to Okello T. Chatrie. Signed by District Judge M. Hannah Lauck on 12/27/2019. (smej,) (Entered: 12/30/2019)
12/30/2019	63	ORDER granting 58 Motion for Alex Campbell Hemmer to appear as Pro hac vice for Google, LLC as to Okello T. Chatrie. Signed by District Judge M. Hannah Lauck on 12/27/2019. (smej,) (Entered: 12/30/2019)
12/30/2019	64	Supplemental Memorandum by USA as to Okello T. Chatrie re 28 MOTION for Discovery *Regarding Government's Use of Google's Sensorvault Data* (Simon, Kenneth) (Entered: 12/30/2019)
12/30/2019	65	ORDER that this matter comes before the Court on the United States of America's Status Report Regarding Filing Search Warrants at Issue in this Matter 55 . Given the disagreement expressed in the parties' filings, Counsel for both parties, along with their supervisors, SHALL appear for an in–person status conference on January 8, 2020 at

		2:30 p.m.as to Okello T. Chatrie. Signed by District Judge M. Hannah Lauck on 12/30/19. (jtho,) (Entered: 12/30/2019)
12/30/2019		Set/Reset Hearings as to Okello T. Chatrie: Status Conference set for 1/8/2020 at 02:30 PM in Richmond Courtroom 6100 before District Judge M. Hannah Lauck. (khan,) (Entered: 12/30/2019)
12/31/2019	66	Consent MOTION for Extension of Time to File Response/Reply as to 51 Order on Motion in Limine,,, Order on Motion to Suppress,,, Order on Motion for Discovery,, 59 MOTION to File Amicus Brief *In Support Of Neither Party* by Brittany Amadi. by Okello T. Chatrie. (Attachments: # 1 Proposed Order)(Koenig, Laura) (Entered: 12/31/2019)
12/31/2019	67	ORDER – Upon motion of defense counsel, with good cause having been shown and noting no objection by the Government it is hereby ORDERED that the Defendant's Motion to Extend Deadline to Respond to Google's Amicus Brief in this case is GRANTED. The parties must file any response to Google's Brief of Amicus Curiae by January 10, 2020. Signed by District Judge M. Hannah Lauck on 12/31/2019. (smej,) (Entered: 12/31/2019)
01/03/2020	68	MOTION to Seal *Raw Data Returns Provided by Google* by Okello T. Chatrie. (Koenig, Laura) (Entered: 01/03/2020)
01/07/2020	69	ORDER – The Court GRANTS the Motion to Seal 68 . The Court DIRECTS the Clerk to file Exhibit A to the Motion to Seal, the raw returns, under seal. The Court CANCELS the January 8, 2020 Status Conference. SEE ORDER FOR DETAILS. Signed by District Judge M. Hannah Lauck on 1/7/2020. (smej,) (Entered: 01/07/2020)
01/07/2020		Status hearing as to Okello T. Chatrie on 1/8/20 CANCELLED. (khan,) (Entered: 01/07/2020)
01/10/2020	71	RESPONSE by USA as to Okello T. Chatrie re 73 Amicus Brief. (Simon, Kenneth) Modified on 1/13/2020 (smej,). Modified on 1/13/2020 (smej,). (Entered: 01/10/2020)
01/10/2020	72	RESPONSE in Opposition to Motion by Okello T. Chatrie re 59 MOTION to File Amicus Brief *In Support Of Neither Party*. (Koenig, Laura) Modified to correct docket text on 1/13/2020 (smej,). (Entered: 01/10/2020)
01/13/2020		Notice of Correction re 73 Amicus Brief: Amicus Brief filed by the Clerk as of the date the Order 60 was entered on 12/23/2019. Relationship between docket entry 73 and 71 has been corrected. (smej,) (Entered: 01/13/2020)
01/21/2020	76	*Defendant's Proposed* EXHIBIT LIST by Okello T. Chatrie (Koenig, Laura) (Entered: 01/21/2020)
01/21/2020	77	Minute Entry for proceedings held before District Judge M. Hannah Lauck:Motion Hearing as to Okello T. Chatrie held on 1/21/2020 re 28 MOTION for Discovery *Regarding Government's Use of Google's Sensorvault Data* filed by Okello T. Chatrie. Motion to SEAL – GRANTED. Dft adduced evidence, RESTED. Govt. RESTED. Arguments heard. Court findings –– additional briefing due 1/24/20. Cross motions due 2/18/20 – cross responses due 2/25. Hearing to be scheduled once the Court has all of the information. Motion to Suppress scheduled 2/20 & 21/20 is continued. Dft remanded to custody. (Court Reporter Diane Daffron, OCR.)(khan,) (Entered: 01/22/2020)
01/22/2020	78	ORDER – The Court: ORDERS the Parties to file, no later than January 24, 2020, a statement regarding the Chesterfield County magistrate who signed the June 14, 2019 Geofence Warrant; ORDERS Chatrie to provide, no later than February 10, 2020, expert disclosures of any proposed experts Chatrie intends to call at the hearing on the Motions to Suppress; CANCELS the February 20–21, 2020 Hearing on the Motions to Suppress. To the extent this this Order conflicts with the Court's December 13, 2019 Order, 51 , this Order SHALL supersede the December 13, 2019 Order. SEE ORDER FOR DETAILS. Signed by District Judge M. Hannah Lauck on 1/22/2020. (smej,) (Entered: 01/22/2020)

01/22/2020		Discovery Motion held as to Okello T. Chatrie: (khan,) (Entered: 01/22/2020)
01/24/2020	79	STIPULATION by Okello T. Chatrie *(Joint Stipulation with the Government)* (Koenig, Laura) (Entered: 01/24/2020)
01/30/2020	81	TRANSCRIPT of Proceedings held on January 21, 2020, before Judge M. Hannah Lauck. Court reporter Diane Daffron, Telephone number 804–916–2893. **NOTICE RE REDACTION OF TRANSCRIPTS:The parties have thirty(30) calendar days to file with the Court a Notice of Intent to Request Redaction of this transcript. If no such Notice is filed, the transcript will be made remotely electronically available to the public without redaction after 90 calendar days. The policy is located on our website at www.vaed.uscourts.gov Transcript may be viewed at the court public terminal or purchased through the court reporter before the deadline for Release of Transcript Restriction. After that date it may be obtained through PACER Redaction Request due 3/2/2020. Redacted Transcript Deadline set for 3/31/2020. Release of Transcript Restriction set for 4/29/2020.(daffron, diane) (Entered: 01/30/2020)**
02/04/2020	82	MOTION for Issuance of Subpoenas *Duces Tecum* and Memorandum in Support by Okello T. Chatrie. (Attachments: # 1 Proposed Order) (Koenig, Laura) Modified docket text on 2/5/2020 (smej,). (Entered: 02/04/2020)
02/07/2020	83	ORDER – Although the United States has until February 18, 2020, to file its response pursuant to Local Rule 7(F) for the United States District Court for the Eastern District of Virginia, in the interests of justice and because the United States has previously suggested that Chatrie pursue a Rule 17 subpoena, the United States SHALL file a response to the Motion for Subpoena no later than February 11, 2020. SEE ORDER FOR DETAILS. Signed by District Judge M. Hannah Lauck on 2/7/2020. (smej,) (Entered: 02/07/2020)
02/07/2020	84	RESPONSE to Motion by USA as to Okello T. Chatrie re 82 MOTION for Issuance of Subpoenas *Duces Tecum* (Simon, Kenneth) (Entered: 02/07/2020)
02/07/2020	85	ORDER (Granting Defendant's Motion for Issuance of Subpoena Duces Tecum) – Defendant's Motion for Issuance of Subpoena Duces Tecum 82 , pursuant to Fed. R. Crim. P. 17(c), requiring production of the states document(s), is GRANTED. SEE ORDER FOR DETIALS. Signed by District Judge M. Hannah Lauck on 2/7/2020. (smej,) (Entered: 02/07/2020)
02/07/2020	86	Subpoena Duces Tecum Issued as to Google, LLC 82 . Clerk placed in USM box for service. (smej,) (Entered: 02/07/2020)
02/18/2020	87	Supplemental Memorandum by Okello T. Chatrie re 28 MOTION for Discovery *Regarding Government's Use of Google's Sensorvault Data* (Attachments: # 1 Exhibit A (CellHawk template), # 2 Exhibit B)(Koenig, Laura) (Entered: 02/18/2020)
02/18/2020	88	Supplemental Memorandum by USA as to Okello T. Chatrie re 28 MOTION for Discovery *Regarding Government's Use of Google's Sensorvault Data* (Simon, Kenneth) (Entered: 02/18/2020)
02/20/2020	89	MOTION to Defer Google's Subpoena Compliance Deadline to Close of Business on Friday, March 6, 2020 re 85 Order on Motion for Issuance of Subpoenas, 86 Subpoena(s) Issued by Okello T. Chatrie. (Attachments: # 1 Proposed Order)(Koenig, Laura) (Entered: 02/20/2020)
02/21/2020	90	ORDER – Upon motion of defense counsel, with good cause having been shown, it is hereby ORDERED that the Defendant's Motion to Defer Google's Subpoena Compliance Deadline to Close of Business on Friday, March 6, 2020, in this case is GRANTED. The time in which Google must comply with the February 7, 2020, subpoena duces tecum in ECF No. 86 is deferred to Friday, March 6, 2020, by the close of business Eastern Standard Time. Signed by District Judge M. Hannah Lauck on 2/21/2020. (smej,) (Entered: 02/21/2020)
02/24/2020	91	Subpoena Returned on 2/12/2020 re 86 Subpoena Duces Tecum Issued. (smej,) Modified to correct docket text on 2/25/2020. Incorrect docket event selected (smej,). (Entered: 02/25/2020)

02/25/2020	92	RESPONSE by Okello T. Chatrie re 88 Supplemental Memorandum (Koenig, Laura) (Entered: 02/25/2020)
02/25/2020	93	RESPONSE by USA as to Okello T. Chatrie re 87 Supplemental Memorandum (Simon, Kenneth) (Entered: 02/25/2020)
03/06/2020	94	Second MOTION re 85 Order on Motion for Issuance of Subpoenas, 90 Order on Motion for Miscellaneous Relief,, by Okello T. Chatrie. (Attachments: # 1 Proposed Order)(Koenig, Laura) (Entered: 03/06/2020)
03/06/2020	95	ORDER granting 94 Motion as to Okello T. Chatrie (1): Upon motion of defense counsel, with good cause having been shown, it is hereby ORDERED that the Defendant's Second Motion to Defer Google's Subpoena Compliance Deadline to Close of Business on Wednesday, March 11, 2020, in this case is GRANTED; thetime in which Google must comply with the February 7,2020, subpoena duces tecum in EOF No. 86 is deferred to Wednesday, March 11, 2020, by the close of business Eastern Standard Time (signed by District Judge M. Hannah Lauck on 3/6/2020) (rpiz) (Entered: 03/06/2020)
03/11/2020	96	RESPONSE by Google, LLC as to Okello T. Chatrie re 95 Order on Motion for Miscellaneous Relief,, (Attachments: # 1 Attachment A, # 2 Attachment B)(Amadi, Brittany) (Entered: 03/11/2020)
03/12/2020	97	NOTICE *of Satisfaction with Google Response to Subpoena Duces Tecum* by Okello T. Chatrie re 96 Response, 86 Subpoena(s) Issued (Koenig, Laura) (Entered: 03/12/2020)
03/25/2020	98	ORDER – Chatrie SHALL file a statement regarding the effect of Google's response to the subpoena on the pending Motion for Discovery. Chatrie's statement SHALL identify which discovery requests (by number or subpart, when applicable) have been fulfilled and which remain unsatisfied. Because Chatrie has received responsive information from Google, he SHALL also identify whether he continues to argue that Google is a member of the prosecution team under either Rule 16 of the Federal Rules of Criminal Procedure or the Supreme Court of the United States' decision in Brady v. Maryland, 373 U.S. 83 (1963). Chatrie SHALL file this statement no later than April 10, 2020, and SHALL limit his response to no more than three (3) pages. SEE ORDER FOR DETAILS. Signed by District Judge M. Hannah Lauck on 3/25/2020. (smej,) (Entered: 03/25/2020)
04/10/2020	99	NOTICE *of Satisfaction of Requests in Geofence Discovery Motion* by Okello T. Chatrie re 98 Order,,, (Koenig, Laura) (Entered: 04/10/2020)
04/13/2020	100	RESPONSE by USA as to Okello T. Chatrie re 99 Notice (Other) (Simon, Kenneth) (Entered: 04/13/2020)
04/13/2020	101	ORDER that the Court DENIES as MOOT the Motion for Discovery (ECF No. 28) and SCHEDULES an in person hearing on Geofence Motion to Suppress (ECF No. 29) on July 2, 2020 at 9:30 a.m. SEE ORDER FOR DETAILS. Signed by District Judge M. Hannah Lauck on 4/13/20. (khan,) (Entered: 04/13/2020)
04/13/2020		Set/Reset Deadlines re Motion or Report and Recommendation in case as to Okello T. Chatrie 29 MOTION to Suppress *Evidence Obtained from a "Geofence" General Warrant*. Motion Hearing set for 7/2/2020 at 09:30 AM in Richmond Courtroom 6100 before District Judge M. Hannah Lauck. (khan,) (Entered: 04/13/2020)
05/12/2020	102	Consent MOTION for Extension *of Supplemental Briefing Deadlines* by Okello T. Chatrie. (Attachments: # 1 Proposed Order)(Koenig, Laura) (Entered: 05/12/2020)
05/13/2020	103	ORDER – It is hereby ORDERED that the Defendants Motion to Extend Supplemental Briefing on Geofence Motion to Suppress By One Week, in this case is GRANTED. Mr. Chatrie must file his supplement to his Geofence Motion to Suppress by May 22, 2020. The governments supplemental response deadline is extended to June 5, 2020. Signed by District Judge M. Hannah Lauck on 5/13/2020. (smej,) (Entered: 05/13/2020)
05/22/2020	104	Supplemental Memorandum by Okello T. Chatrie re 29 MOTION to Suppress *Evidence Obtained from a "Geofence" General Warrant* (Koenig, Laura) (Entered: 05/22/2020)

05/26/2020	105	Motion to appear Pro Hac Vice by Nathan Judish and Certification of Local Counsel Kenneth Simon, Jr. by USA as to Okello T. Chatrie. (Simon, Kenneth) (Entered: 05/26/2020)
05/28/2020	106	Consent MOTION for Extension of Time to File Response/Reply as to 104 Supplemental Memorandum by USA as to Okello T. Chatrie. (Attachments: # 1 Proposed Order Proposed Order)(Simon, Kenneth) (Entered: 05/28/2020)
05/28/2020	107	ORDER granting 105 Motion for Nathan Paul Judish to appear as Pro hac vice for USA. Signed by District Judge M. Hannah Lauck on 5/28/2020. (smej,) (Entered: 05/28/2020)
05/28/2020	108	ORDER – Upon Motion of the United States of America, by and through attorneys. G. Zachary Terwilliger. United States Attorney for the Eastern District of Virginia, Kenneth R. Simon, Jr. and Peter S. Duffey. Assistant United States Attorneys, for an extension of time to file a response to the defendant's supplemental memorandum in support of his motion to suppress 104 from June 5, 2020 to June 12, 2020, and the defendant having no objection and for good cause shown, the Court GRANTS the United States' motion. Accordingly, the United States must respond to the defendant's motions on or before June 12, 2020. Signed by District Judge M. Hannah Lauck on 5/28/2020. (smej,) (Entered: 05/28/2020)
06/12/2020	109	RESPONSE by USA as to Okello T. Chatrie re 104 Supplemental Memorandum (Simon, Kenneth) (Entered: 06/12/2020)
06/17/2020	110	MOTION for Leave to File *Supplemental Declaration of Marlo McGriff* by Google, LLC as to Okello T. Chatrie. (Attachments: # 1 Supplemental Declaration of Marlo McGriff, # 2 Proposed Order)(Amadi, Brittany) (Entered: 06/17/2020)
06/22/2020	111	Objection by Okello T. Chatrie re 110 MOTION for Leave to File *Supplemental Declaration of Marlo McGriff and Motion to Strike Such Declaration* (Koenig, Laura) (Entered: 06/22/2020)
06/24/2020	115	MEMORANDUM ORDER – This matter comes before the Court on Google LLC's ("Google ") Motion for Leave to File Supplemental Declaration of Marlo McGriff (the "Motion ") 110 . The Court GRANTS the Motion, 110 ; CONTINUES GENERALLY the July 2, 2020 Hearing on Chatrie's Geofence Motion to Suppress. SEE ORDER FOR DETAILS. Signed by District Judge M. Hannah Lauck on 6/24/2020. (smej,) (Entered: 06/24/2020)
06/24/2020	116	ORDER – The Parties SHALL file no later than July 8, 2020, a statement, not to exceed ten (10) pages, on these effects, if any. If they so choose, the Parties SHALL file no later than July 15, 2020, a response, not to exceed ten (10) pages, to the other party's statement. The Parties SHALL address any additional information they have gained about Mr. Bishop in their initial position statements. SEE ORDER FOR DETAILS. Signed by District Judge M. Hannah Lauck on 6/24/2020. (smej,) (Entered: 06/24/2020)
06/26/2020	117	*Motion to Suppress GeoFence Search Warrant* WITNESS LIST by USA as to Okello T. Chatrie (Simon, Kenneth) (Entered: 06/26/2020)
06/26/2020	118	*Motion to Suppress GeoFence Search Warrant* EXHIBIT LIST by USA as to Okello T. Chatrie (Simon, Kenneth) (Entered: 06/26/2020)
06/26/2020	119	*Preliminary* EXHIBIT LIST by Okello T. Chatrie (Koenig, Laura) (Entered: 06/26/2020)
06/26/2020	120	*Preliminary* WITNESS LIST by Okello T. Chatrie (Koenig, Laura) (Entered: 06/26/2020)
07/02/2020	121	STATUS REPORT *(Joint) Regarding Rescheduling the Geofence Motion Hearing* by Okello T. Chatrie (Koenig, Laura) (Entered: 07/02/2020)
07/02/2020	123	MOTION for Issuance of Subpoenas *Duces Tecum and Memorandum in Support* by Okello T. Chatrie. (Attachments: # 1 Exhibit A)(Koenig, Laura) (Entered: 07/02/2020)
07/07/2020	126	Consent MOTION for Extension *of Supplemental Briefing Deadline On Magistrate Questions* by Okello T. Chatrie. (Attachments: # 1 Proposed Order)(Koenig, Laura) (Entered: 07/07/2020)

07/07/2020	127	ORDER as to Okello T. Chatrie. This matter comes before the Court on Defendant Okello T. Chatrie's Motion for Issuance of a Second Subpoena Duces Tecum Pursuant to Rule 17(c) (the "Second Motion for Subpoena"). The United States SHALL file a response to the Second Motion for Subpoena no later than July 13, 2020. It is SO ORDERED. Signed by District Judge M. Hannah Lauck on 7/7/2020. (sbea,) (Entered: 07/07/2020)
07/07/2020		Exhibit of DVD Received re 123 MOTION for Issuance of Subpoenas Duces Tecum and Memorandum in Support. Placed on shelf in Clerk's Office. (smej,) (Entered: 07/07/2020)
07/07/2020	128	ORDER – It is hereby ORDERED that the Defendant's Motion to Extend Supplemental Briefing on Magistrate Questions in this case is GRANTED. The parties must file any supplemental briefing on the issue by July 22, 2020. Signed by District Judge M. Hannah Lauck on 7/7/2020. (smej,) (Entered: 07/07/2020)
07/13/2020	129	RESPONSE by USA as to Okello T. Chatrie re 123 MOTION for Issuance of Subpoenas *Duces Tecum and Memorandum in Support*, 127 Order on Motion for Issuance of Subpoenas, (Attachments: # 1 Exhibit Subpoena Requests Updated to Include United States Additons)(Simon, Kenneth) (Entered: 07/13/2020)
07/16/2020	130	REPLY TO RESPONSE to by Okello T. Chatrie re 129 Response, 123 MOTION for Issuance of Subpoenas *Duces Tecum and Memorandum in Support* (Koenig, Laura) (Entered: 07/16/2020)
07/17/2020	131	ORDER that the Court GRANTS 123 Second Motion for Subpoena. See Order for details. Signed by District Judge M. Hannah Lauck on 7/17/2020. (jsmi,) (Main Document 131 replaced on 7/17/2020) (jsmi,). (Entered: 07/17/2020)
07/17/2020	132	ORDER re United States' standing argument raised in 129 response to Defendant Okello T. Chatrie's 123 Motion for Issuance of a Second Subpoena Duces Tecum. No later than July 31, 2020, Chatrie SHALL file a response to the United States' standing argument. This response SHALL NOT exceed 10 pages. If it so chooses, no later than August 7, 2020, the United States SHALL file a reply to Chatrie's response. This reply SHALL NOT exceed 10 pages. Signed by District Judge M. Hannah Lauck on 7/17/2020. (jsmi,) (Entered: 07/17/2020)
07/20/2020	133	Subpoena Issued as to Okello T. Chatrie. (Attachments: # 1 Exhibit A) (smej,) (Entered: 07/20/2020)
07/22/2020	134	RESPONSE by USA as to Okello T. Chatrie re 116 Order,, (Simon, Kenneth) (Entered: 07/22/2020)
07/22/2020	135	Supplemental Memorandum by Okello T. Chatrie re 29 MOTION to Suppress *Evidence Obtained from a "Geofence" General Warrant* (Attachments: # 1 Exhibit A, # 2 Exhibit B, # 3 Exhibit C)(Koenig, Laura) (Entered: 07/22/2020)
07/29/2020	139	RESPONSE by USA as to Okello T. Chatrie re 135 Supplemental Memorandum (Simon, Kenneth) (Additional attachment(s) added on 7/30/2020: # 1 Appointment Order, # 2 Certificate, # 3 Oath of Office) (smej,). (Entered: 07/29/2020)
07/31/2020	140	RESPONSE by Google, LLC as to Okello T. Chatrie re 133 Subpoena(s) Issued (Amadi, Brittany) (Entered: 07/31/2020)
07/31/2020	141	MOTION for Leave to File *Documents Responsive to Rule 17(C) Subpoena Under Seal* by Google, LLC as to Okello T. Chatrie. (Attachments: # 1 Proposed Order)(Amadi, Brittany) (Entered: 07/31/2020)
07/31/2020	142	ORDER as to Okello T. Chatrie. Having considered the motion of amicus curiae Google LLC for leave to file documents responsive to the July 22, 2020 subpoena under seal, and good cause appearing, it is hereby ORDERED that the motion is GRANTED. The clerk is DIRECTED to accept the documents lodged with the Court via e–mail for filing and to maintain them under seal. It is hereby ORDERED that Google will file a redacted version of the sealed documents on the public record within seven days of this Order.Signed by District Judge M. Hannah Lauck on 7/31/2020. (sbea,) (Entered: 07/31/2020)

07/31/2020	143	RESPONSE by Okello T. Chatrie re 129 Response, 132 Order,, (Koenig, Laura) (Entered: 07/31/2020)
08/07/2020	147	RESPONSE by Google, LLC as to Okello T. Chatrie re 133 Subpoena(s) Issued (Attachments: # 1 Exhibit A, # 2 Exhibit B)(Amadi, Brittany) (Entered: 08/07/2020)
08/19/2020	149	MOTION to Terminate Speedy Trial Hearing by Okello T. Chatrie. (Attachments: # 1 Envelope) (smej,) (Entered: 08/20/2020)
08/24/2020	151	ORDER – This matter comes before the Court on Defendant Okello T. Chatrie's pro se Motion to Terminate Speedy Trial Hearing, (the "Motion") 149 . The Court observes that Chatrie has legal representation through Laura Jill Koenig, Michael William Price, and Paul Geoffrey Gill. Despite having the benefit of Counsel, it appears that Chatrie filed this Motion without Counsels' legal assistance 149 . Because Chatrie remains represented by counsel, the Court DENIES WITHOUT PREJUDICE Chatrie's prose Motion to Terminate Speedy Trial Hearing 149 . Signed by District Judge M. Hannah Lauck on 8/24/2020. (smej,) (Entered: 08/24/2020)
09/28/2020	152	NOTICE OF ATTORNEY APPEARANCE Donald Eldridge Jeffrey, III appearing for USA. (Jeffrey, Donald) (Entered: 09/28/2020)
10/05/2020	153	ORDER – This matter comes before the Court on Defendant Okello T. Chatrie's Motion to Suppress Evidence Obtained from the Geo fence Warrant (the "Motion"). (ECF No. 29.) Upon review of the Parties' briefing on the Motion, the Court ORDERS the Parties to appear, in person, for a hearing on the Motion on Tuesday, November 17, 2020, at 10:00 a.m. Signed by District Judge M. Hannah Lauck on 10/05/2020. (tjoh,) (Entered: 10/05/2020)
10/05/2020		Set/Reset Deadlines re Motion or Report and Recommendation in case as to Okello T. Chatrie 29 MOTION to Suppress *Evidence Obtained from a "Geofence" General Warrant*, 21 MOTION to Suppress *Evidence Obtained from Buick Lacrosse Search*, 20 MOTION to Suppress *Evidence Obtained from Mr. Chatrie's Google Accounts Search*, 18 MOTION to Suppress *Evidence Obtained from Willis Street Search*, 19 MOTION to Suppress *Evidence Obtained from Mason Dale Drive Search*. Motion Hearing set for 11/17/2020 at 10:00 AM in Richmond Courtroom 6100 before District Judge M. Hannah Lauck. (khan,) (Entered: 10/05/2020)
10/08/2020		Set/Reset Hearings as to Okello T. Chatrie: Status Conference set for 10/22/2020 at 12:30 PM in Richmond Remote before District Judge M. Hannah Lauck. (khan,) (Entered: 10/08/2020)
10/16/2020	154	ORDER – The Parties clearly exchanged some information, such as Magistrate Bishop's educational history, either before or after the Subpoena was served. After reviewing the materials before it and in the interest of judicial efficiency, the Court DIRECTS the Parties to meet and confer about a potential stipulation of the below facts prior to the status conference with the Court scheduled for Thursday October 22, 2020. SEE ORDER FOR DETAILS. Signed by District Judge M. Hannah Lauck on 10/16/2020. (smej,) (Entered: 10/16/2020)
10/22/2020		Minute Entry for proceedings held before District Judge M. Hannah Lauck:Telephone Conference held via ZOOM as to Okello T. Chatrie held on 10/22/2020. (Court Reporter Diane Daffron, OCR.)(khan,) (Entered: 10/22/2020)
10/22/2020	156	STIPULATION by Okello T. Chatrie *of Partial Facts Relating to Magistrate Issue* (Koenig, Laura) (Entered: 10/22/2020)
10/26/2020	157	TRANSCRIPT of Status Conference held on October 22, 2020, before Judge M. Hannah Lauck. Court reporter Diane Daffron, Telephone number 804–916–2893. **NOTICE RE REDACTION OF TRANSCRIPTS:The parties have thirty(30) calendar days to file with the Court a Notice of Intent to Request Redaction of this transcript. If no such Notice is filed, the transcript will be made remotely electronically available to the public without redaction after 90 calendar days. The policy is located on our website at www.vaed.uscourts.gov Transcript may be viewed at the court public terminal or purchased through the court reporter before the deadline for Release of Transcript Restriction. After that date it may be obtained through PACER Redaction Request due 11/25/2020. Redacted Transcript Deadline set for 12/28/2020. Release of Transcript Restriction set for 1/25/2021.(daffron, diane) (Entered: 10/26/2020)**

10/26/2020	160	ORDER – This matter comes before the Court on Magistrate David M. Bishop's Motion to Quash (the "Motion"). (ECF No. 145.) On October 22, 2019, Defendant Okello T. Chatrie moved this Court to suppress evidence, (the "Motion to Suppress"), that law enforcement officers obtained pursuant to a warrant of Chatrie's Google accounts ("the June 14, 2019 Geofence Warrant"). (Mot. Suppress Evid. 1, ECF No. 20.). The Court GRANTS the Motion to Quash. (ECF No. 145.) SEE ORDER FOR DETAILS. Signed by District Judge M. Hannah Lauck on 10/26/2020. (smej,) (Entered: 10/26/2020)
11/09/2020	161	MOTION for Leave to Present Remote Testimony by Google, LLC as to Okello T. Chatrie. (Attachments: # 1 Proposed Order)(Amadi, Brittany) (Entered: 11/09/2020)
11/09/2020	162	*Motion to Suppress Hearing* WITNESS LIST by USA as to Okello T. Chatrie (Simon, Kenneth) (Entered: 11/09/2020)
11/09/2020	163	*Motion to Suppress Hearing* EXHIBIT LIST by USA as to Okello T. Chatrie (Simon, Kenneth) (Entered: 11/09/2020)
11/09/2020	164	*11–17–20 Hearing* WITNESS LIST by Okello T. Chatrie (Koenig, Laura) (Entered: 11/09/2020)
11/09/2020	165	*11–17–20 Hearing* EXHIBIT LIST by Okello T. Chatrie (Koenig, Laura) (Entered: 11/09/2020)
11/11/2020	166	RESPONSE in Opposition by Okello T. Chatrie re 161 MOTION for Leave to Present Remote Testimony (Koenig, Laura) (Entered: 11/11/2020)
11/12/2020	167	REPLY TO RESPONSE to Google, LLC as to Okello T. Chatrie re 161 MOTION for Leave to Present Remote Testimony (Amadi, Brittany) (Entered: 11/12/2020)
11/12/2020		Minute Entry for proceedings held before District Judge M. Hannah Lauck:Status Conference as to Okello T. Chatrie held on 11/12/2020 via ZOOM (Court Reporter Diane Daffron, OCR.)(khan,) (Entered: 11/16/2020)
11/16/2020	168	MOTION to Continue *November 17, 2020, Hearing* by Okello T. Chatrie. (Koenig, Laura) (Entered: 11/16/2020)
11/20/2020	169	STATUS REPORT *(Joint) on Potential Google Objections* by Okello T. Chatrie (Koenig, Laura) (Entered: 11/20/2020)
12/18/2020	170	ORDER – This matter comes before the Court on Defendant Okello T. Chatrie's Motion to Continue the November 17, 2020 Hearing (the "Motion"), (ECF No. 168.) Upon review of the Parties' briefing on Chatrie's Motion to Suppress Evidence Obtained from the Geofence Warrant, the Court GRANTS the Motion, (ECF No. 168), and ORDERS the Parties to appear, in person, for a hearing on the Motion to Suppress Evidence on **Thursday, March 4, 2021, at 9:30 a.m.** in Courtroom 6100 of the Spottswood W. Robinson III and Robert R. Merhige, Jr. United States Courthouse. Signed by District Judge M. Hannah Lauck on 12/18/2020. (smej,) (Entered: 12/18/2020)
12/18/2020		Set/Reset Deadlines re Motion or Report and Recommendation in case as to Okello T. Chatrie 29 MOTION to Suppress *Evidence Obtained from a "Geofence" General Warrant*. Motion Hearing set for 3/4/2021 at 09:30 AM in Richmond Courtroom 6100 before District Judge M. Hannah Lauck. (khan,) (Entered: 12/18/2020)
01/08/2021	171	**DISREGARD** – Letter from Brittany Amadi regarding the withdrawal of Alex Hemmer on behalf of Google LLC, (Amadi, Brittany) Modified on 1/12/2021 (smej,). (Entered: 01/08/2021)
01/11/2021		Notice of Correction re 171 Letter: The clerk has notified the filing attorney of the proper filing procedures for withdrawing from a case. The filing attorney has been instructed to file a motion to withdraw using the correct docket event. (smej,) (Entered: 01/11/2021)
01/14/2021	172	MOTION to Withdraw as Attorney by Alex Hemmer. by Google, LLC as to Okello T. Chatrie. (Attachments: # 1 Proposed Order)(Amadi, Brittany) (Entered: 01/14/2021)
01/14/2021	173	Letter from Brittany Amadi (Amadi, Brittany) (Entered: 01/14/2021)

01/19/2021	174	ORDER – ORDER GRANTING MOTION TO WITHDRAW AS COUNSEL – Having considered the motion for leave to withdraw Alex Hemmer as counsel, and good cause appearing, it is hereby ORDERED that the that the motion is GRANTED. Signed by District Judge M. Hannah Lauck on 1/19/2021. (smej,) (Entered: 01/19/2021)
01/25/2021	175	MOTION to Compel *Disclosure of Expert Report and Exhibit 12 on or before February 5, 2021* by USA as to Okello T. Chatrie. (Attachments: # 1 Proposed Order Proposed Order)(Simon, Kenneth) (Entered: 01/25/2021)
02/03/2021	176	ORDER that the Court ORDERED Chatrie to respond to the Motion no later that Thursday, February 4, 2021 at noon. The Parties shall be advised of their duties under the Eastern District of Virginia Local Rule 37(H). The parties shall appear via teleconference on Thursday, February 4, 2021 at 2:00 p.m. for a status conference in this matter. Signed by District Judge M. Hannah Lauck on 2/3/21. (khan,) (Entered: 02/03/2021)
02/03/2021		Set/Reset Hearings as to Okello T. Chatrie: Status Conference set for 2/4/2021 at 02:00 PM in Richmond Remote before District Judge M. Hannah Lauck. (khan,) (Entered: 02/03/2021)
02/03/2021	177	RESPONSE to Motion by Okello T. Chatrie re 175 MOTION to Compel *Disclosure of Expert Report and Exhibit 12 on or before February 5, 2021* (Koenig, Laura) (Entered: 02/03/2021)
02/04/2021	178	Letter from Brittany Amadi regarding Witness Availability, (Amadi, Brittany) (Entered: 02/04/2021)
02/04/2021	179	ORDER that the Court denies as moot 175 Motion to Compel. The Court ORDERS that the Parties submit expert reports no later than February 16, 2021. The Parties SHALL file any arguments as to an extension to the February 16, 2021, deadline no later than February 12, 2021. On February 25, 2021, the Parties SHALL file their updated witness and exhibit lists and provide the Court with two courtesy copies of the exhibits, should they conform to paper copies. Signed by District Judge M. Hannah Lauck on 2/4/2021. (jsmi,) (Entered: 02/04/2021)
02/05/2021	181	Minute Entry for proceedings held before District Judge M. Hannah Lauck:Status Conference as to Okello T. Chatrie held on 2/5/2021 (Court Reporter Diane Daffron, OCR.)(khan,) (Entered: 02/05/2021)
02/11/2021	184	Letter from Catherine Carroll (Carroll, Catherine) (Entered: 02/11/2021)
02/22/2021	185	ORDER as to Okello T. Chatrie. In light of the quickly approaching hearing on the pending Motion to Suppress Evidence Obtained from Chatrie's Google Accounts, (ECF No. 20), Counsel for Chatrie SHALL file on February 25, 2021, a status update regarding Chatries ability to personally appear at the hearing currently scheduled for March 45, 2021. On February 26, 2021, at 1:30 p.m., the Parties SHALL appear before the Court, via video teleconference, for a status conference. It is SO ORDERED. Signed by District Judge M. Hannah Lauck on 2/22/2021. (sbea,) (Entered: 02/22/2021)
02/22/2021		Set/Reset Hearings as to Okello T. Chatrie: Status Conference set for 2/26/2021 at 01:30 PM in Richmond Remote before District Judge M. Hannah Lauck. (khan,) (Entered: 02/22/2021)
02/22/2021		Set/Reset Hearings as to Okello T. Chatrie: Status Conference set for 2/25/2021 at 04:00 PM in Richmond Remote before District Judge M. Hannah Lauck. (khan,) (Entered: 02/22/2021)
02/25/2021	186	*Motion to Suppress 3–4–21 Hearing* WITNESS LIST by USA as to Okello T. Chatrie (Simon, Kenneth) (Entered: 02/25/2021)
02/25/2021	187	*Motion to Suppress Hearing* EXHIBIT LIST by USA as to Okello T. Chatrie (Simon, Kenneth) (Entered: 02/25/2021)
02/25/2021	188	RESPONSE by Okello T. Chatrie re 185 Order,, (Gill, Paul) (Entered: 02/25/2021)
02/25/2021	189	EXHIBIT LIST by Okello T. Chatrie (Koenig, Laura) (Entered: 02/25/2021)

02/25/2021	190	WITNESS LIST by Okello T. Chatrie (Koenig, Laura) (Entered: 02/25/2021)
02/25/2021		Minute Entry for proceedings held before District Judge M. Hannah Lauck:Status Conference as to Okello T. Chatrie held on 2/25/2021 (Court Reporter Diane Daffron, OCR.)(khan,) (Entered: 02/26/2021)
02/26/2021	191	ORDER – This matter comes before the Court sua sponte. On February 25, 2021, the Court held a status conference in this matter over Zoom. For the reasons stated from the Bench, the Court ORDERS the Parties to file no later than Friday, February 26, 2021, at 1:00 p.m., their positions on COVID–19 protocol and procedures required by applicable governmental and health agencies for an in–person hearing on March 4, 2021. The Parties SHALL appear before the Court via video teleconference for a status conference in this matter on Friday, February 26, 2021, at 4:30 p.m. Signed by District Judge M. Hannah Lauck on 02/26/2021. (tjoh,) (Entered: 02/26/2021)
02/26/2021		Set/Reset Hearings as to Okello T. Chatrie: Status Conference set for 2/26/2021 at 04:30 PM in Richmond Remote before District Judge M. Hannah Lauck. (khan,) (Entered: 02/26/2021)
02/26/2021	192	Letter from Catherine Carroll (Carroll, Catherine) (Entered: 02/26/2021)
02/26/2021	193	Position on *Defendant's Presence at Suppression Hearing Following COVID–19 Diagnosis* by USA as to Okello T. Chatrie *Defendant's Presence at Suppression Hearing Following COVID–19 Diagnosis* (Simon, Kenneth) (Entered: 02/26/2021)
02/26/2021	194	RESPONSE by Okello T. Chatrie re 191 Order,, *Position on COVID–19 protocol and procedures* (Gill, Paul) (Entered: 02/26/2021)
02/26/2021		Minute Entry for proceedings held before District Judge M. Hannah Lauck:Status Conference as to Okello T. Chatrie held on 2/26/2021 (Court Reporter Diane Daffron, OCR.)(khan,) (Entered: 03/01/2021)
03/04/2021		Set/Reset Deadlines re Motion or Report and Recommendation in case as to Okello T. Chatrie 20 MOTION to Suppress *Evidence Obtained from Mr. Chatrie's Google Accounts Search*. Motion Hearing set for 3/5/2021 at 09:00 AM in Richmond Courtroom 6100 before District Judge M. Hannah Lauck. (khan,) (Entered: 03/04/2021)
03/04/2021	198	Minute Entry for proceedings held before District Judge M. Hannah Lauck:Motion Hearing as to Okello T. Chatrie held on 3/4/2021 re 29 MOTION to Suppress *Evidence Obtained from a "Geofence" General Warrant* filed by Okello T. Chatrie. Dft adduced evidence. Motion hearing continued to March 6, 2021 at 9:00 a.m. Dft remanded to custody. (Court Reporter Diane Daffron, OCR.)(khan,) Modified on 3/8/2021 (khan,). (Entered: 03/08/2021)
03/05/2021	199	Minute Entry for proceedings held before District Judge M. Hannah Lauck:Motion Hearing as to Okello T. Chatrie held on 3/5/2021 re 29 MOTION to Suppress *Evidence Obtained from a "Geofence" General Warrant* filed by Okello T. Chatrie. Dft adduced evidence, rested. Govt adduced evidence, rested. Briefing schedule set. Govt. maintained a set of exhibits for chambers use. Parties to maintain official set for record. Dft remanded to custody. (Court Reporter Diane Daffron, OCR.)(khan,) (Entered: 03/08/2021)
03/09/2021	200	ORDER as to Okello T. Chatrie – For the reasons stated from the Bench, Defendant Okello T. Chatrie SHALL file supplemental briefing on the Geofence Motion to Suppress no later than April 30, 2021. On or before May 21, 2021, the United States SHALL file its response. On or before June 4, 2021, Chatrie SHALL file his reply. The Court ORDERS the Parties to appear for a hearing on all outstanding matters on **June 24, 2021, at 10:00 a.m.** The Court DENIES as moot Google's Motion for Leave to Present Remote Testimony. (ECF No. 161.) Signed by District Judge M. Hannah Lauck on 3/9/2021. (smej,) (Entered: 03/09/2021)
03/09/2021		Set Motion in case as to Okello T. Chatrie. Motion Hearing set for 6/24/2021 at 10:00 AM in Richmond Courtroom 6100 before District Judge M. Hannah Lauck. (khan,) (Entered: 03/09/2021)
03/29/2021	201	TRANSCRIPT of Motion to Suppress held on March 4, 2021, before Judge M. Hannah Lauck. Court reporter Diane Daffron, Telephone number 804–916–2893.

		NOTICE RE REDACTION OF TRANSCRIPTS:The parties have thirty(30) calendar days to file with the Court a Notice of Intent to Request Redaction of this transcript. If no such Notice is filed, the transcript will be made remotely electronically available to the public without redaction after 90 calendar days. The policy is located on our website at www.vaed.uscourts.gov Transcript may be viewed at the court public terminal or purchased through the court reporter before the deadline for Release of Transcript Restriction. After that date it may be obtained through PACER Redaction Request due 4/28/2021. Redacted Transcript Deadline set for 6/1/2021. Release of Transcript Restriction set for 6/28/2021.(daffron, diane) (Entered: 03/29/2021)
03/29/2021	202	TRANSCRIPT of Motion to Suppress (Day 2) held on March 5, 2021, before Judge M. Hannah Lauck. Court reporter Diane Daffron, Telephone number 804–916–2893. **NOTICE RE REDACTION OF TRANSCRIPTS:The parties have thirty(30) calendar days to file with the Court a Notice of Intent to Request Redaction of this transcript. If no such Notice is filed, the transcript will be made remotely electronically available to the public without redaction after 90 calendar days. The policy is located on our website at www.vaed.uscourts.gov Transcript may be viewed at the court public terminal or purchased through the court reporter before the deadline for Release of Transcript Restriction. After that date it may be obtained through PACER Redaction Request due 4/28/2021. Redacted Transcript Deadline set for 6/1/2021. Release of Transcript Restriction set for 6/28/2021.(daffron, diane) (Main Document 202 replaced on 4/29/2021) (tjoh,). (Entered: 03/29/2021)**
04/30/2021	203	MOTION for Leave to File *Brief Exceeding 30 Pages* by Okello T. Chatrie. (Attachments: # 1 Exhibit 1, # 2 Proposed Order)(Koenig, Laura) (Entered: 04/30/2021)
05/03/2021	204	ORDER – Upon motion of defense counsel, with good cause having been shown, it is hereby ORDERED that the Defendants Motion for Leave to File Brief Exceeding 30 Pages in this case is GRANTED. (ECF No. 203.) Mr. Chatries Post–Hearing Brief on Geofence General Warrant is deemed timely filed. Mr. Chatrie shall refile that brief as a separate docket entry within three business days of this Order. Signed by District Judge M. Hannah Lauck on 5/3/2021. (smej,) (Entered: 05/03/2021)
05/03/2021	205	Supplemental Memorandum by Okello T. Chatrie re 29 MOTION to Suppress *Evidence Obtained from a "Geofence" General Warrant* (Koenig, Laura) (Entered: 05/03/2021)
05/14/2021	206	MOTION for Bond by Okello T. Chatrie. (Gill, Paul) (Entered: 05/14/2021)
05/21/2021	207	MOTION for Leave to File *Post–Hearing Supplemental Response in Opposition* by USA as to Okello T. Chatrie. (Attachments: # 1 Proposed Order Proposed Order, # 2 Exhibit Response in Opposition Post–Hearing Supplemental Brief)(Simon, Kenneth) (Entered: 05/21/2021)
05/24/2021	208	ORDER – Upon Motion of the United States of America, by and through attorneys, Raj Parekh, Acting United States Attorney for the Eastern District of Virginia, Kenneth R. Simon, Jr., and Peter S. Duffey, Assistant United States Attorneys, for leave to file an omnibus responsive brief that is in excess of thirty pages pursuant to Local Criminal Rule 47(F)(3). For good cause shown, the Court GRANTS the United States motion. Accordingly, the United States may file its omnibus responsive brief that is in excess of thirty pages. Signed by District Judge M. Hannah Lauck on 5/24/2021. (smej,) (Entered: 05/24/2021)
05/30/2021	209	RESPONSE in Opposition by USA as to Okello T. Chatrie re 206 MOTION for Bond (Attachments: # 1 Exhibit Still Photos from Robbery Video)(Simon, Kenneth) (Entered: 05/30/2021)
06/02/2021		Set as to Okello T. Chatrie: Bond Reconsideration Hearing set for 6/3/2021 at 2:15 PM in Richmond Courtroom 5400 before Magistrate Judge Elizabeth W. Hanes. (mful) (Entered: 06/02/2021)
06/03/2021	210	Addendum to Pretrial Services Bond Report (Sealed Document) as to Okello T. Chatrie (taylor, sheree) (Entered: 06/03/2021)

06/03/2021	211	Minute Entry for proceedings held before Magistrate Judge Elizabeth W. Hanes: Bond Reconsideration Hearing as to Okello T. Chatrie held on 6/3/2021; Deft adduced evidence; Arguments heard; Findings stated from the bench; Motion denied; Order to follow; Deft remanded. (FTR)(mful) (Entered: 06/04/2021)
06/03/2021	212	ORDER denying 206 Motion for Bond as to Okello T. Chatrie. Signed by Magistrate Judge Elizabeth W. Hanes on 6/3/21. (mful) (Entered: 06/04/2021)
06/04/2021	213	REPLY TO RESPONSE to by Okello T. Chatrie re 209 Response in Opposition (Koenig, Laura) (Entered: 06/04/2021)
06/17/2021	214	RESPONSE by USA as to Okello T. Chatrie re 205 Supplemental Memorandum (Simon, Kenneth) (Entered: 06/17/2021)
06/24/2021	215	Minute Entry for proceedings held before District Judge M. Hannah Lauck (Daffron, OCR): Matter came on for hearing as to Okello T. Chatrie on 6/24/2021 re: supplemental briefing to 29 Motion to Suppress Evidence Obtained from a "Geofence" General Warrant filed by Okello T. Chatrie. Defense counsel heard. Government heard. Matter taken under advisement by the Court. Defendant remanded to custody (rpiz) (Entered: 06/25/2021)
06/30/2021	216	NOTICE *of Supplemental Authority* by USA as to Okello T. Chatrie (Simon, Kenneth) (Entered: 06/30/2021)
07/15/2021	217	TRANSCRIPT of argument on summary judgment motion Proceedings held on June 24, 2021, before Judge M. Hannah Lauck. Court reporter Diane Daffron, Telephone number 804–916–2893. **NOTICE RE REDACTION OF TRANSCRIPTS:The parties have thirty(30) calendar days to file with the Court a Notice of Intent to Request Redaction of this transcript. If no such Notice is filed, the transcript will be made remotely electronically available to the public without redaction after 90 calendar days. The policy is located on our website at www.vaed.uscourts.gov Transcript may be viewed at the court public terminal or purchased through the court reporter before the deadline for Release of Transcript Restriction. After that date it may be obtained through PACER Redaction Request due 8/16/2021. Redacted Transcript Deadline set for 9/14/2021. Release of Transcript Restriction set for 10/13/2021.(daffron, diane) (Entered: 07/15/2021)**
07/16/2021	218	RESPONSE by Okello T. Chatrie re 216 Notice (Other) (Koenig, Laura) (Entered: 07/16/2021)
12/16/2021	219	NOTICE *of Supplemental Authority* by Okello T. Chatrie re 104 Supplemental Memorandum, 205 Supplemental Memorandum, 29 MOTION to Suppress *Evidence Obtained from a "Geofence" General Warrant* (Attachments: # 1 Exhibit A)(Koenig, Laura) (Entered: 12/16/2021)
03/03/2022	220	MEMORANDUM OPINION as to Okello T. Chatrie. Signed by District Judge M. Hannah Lauck on 3/3/22. (khan,) (Entered: 03/03/2022)
03/03/2022	221	ORDER denying 29 Motion to Suppress as to Okello T. Chatrie (1). Signed by District Judge M. Hannah Lauck on 3/3/22. (khan,) (khan,). (Entered: 03/03/2022)
03/03/2022	222	Sealed Document signed by M. Hannah Lauck, U.S. District Judge on 3/3/22. (khan,) (Entered: 03/03/2022)
03/03/2022	223	ORDER denying 18 Motion to Suppress as to Okello T. Chatrie (1); denying 19 Motion to Suppress as to Okello T. Chatrie (1); denying 20 Motion to Suppress as to Okello T. Chatrie (1); denying 21 Motion to Suppress as to Okello T. Chatrie (1). Signed by District Judge M. Hannah Lauck on 3/3/22. (khan,) (Entered: 03/03/2022)
05/02/2022		Set/Reset Hearings as to Okello T. Chatrie: Plea Agreement Hearing set for 5/9/2022 at 02:30 PM in Richmond Courtroom 6100 before District Judge M. Hannah Lauck. (khan,) (Entered: 05/02/2022)
05/06/2022	224	CRIMINAL INFORMATION as to Okello T. Chatrie (1) count(s) 1s, 2s. (jpow,) (Entered: 05/06/2022)
05/09/2022	226	Minute Entry for proceedings held before District Judge M. Hannah Lauck (Court Reporter Daffron, OCR): Plea Agreement Hearing as to Okello T. Chatrie held on 5/9/2022. Waiver of Indictment, Plea Agreement, and Statement of Facts filed in open

		court. Plea entered by Okello T. Chatrie (1) Guilty as to Counts 1s and 2s of the Criminal Information; Court accepted plea. Judgment: Defendant guilty as charged in Counts 1s and 2s. Sentencing set for 8/2/2022 at 11:00 AM. Defendant remanded to custody (rpiz) (Entered: 05/09/2022)
05/09/2022	227	WAIVER OF INDICTMENT by Okello T. Chatrie (rpiz) (Entered: 05/09/2022)
05/09/2022	228	PLEA AGREEMENT as to Okello T. Chatrie (rpiz) (Entered: 05/09/2022)
05/09/2022	229	STATEMENT OF FACTS as to Okello T. Chatrie (rpiz) (Entered: 05/09/2022)
05/09/2022	230	Order for sentencing guidelines as to Okello T. Chatrie: Sentencing set for 8/2/2022 at 11:00 AM in Richmond Courtroom 6100 before District Judge M. Hannah Lauck (signed by District Judge M. Hannah Lauck on 5/9/2022) (rpiz) (Entered: 05/09/2022)
05/09/2022	231	CONSENT ORDER OF FORFEITURE as to Okello T. Chatrie (signed by District Judge M. Hannah Lauck on 5/9/2022) (rpiz) (Entered: 05/09/2022)
06/28/2022	232	PRESENTENCE INVESTIGATION REPORT (Disclosed Presentence Investigation Report) (SEALED – government and defense counsel) as to Okello T. Chatrie. Objections to PSI due 07/12/2022. (Harrison, Dorothy) (Entered: 06/28/2022)
07/08/2022		Set/Reset Hearings as to Okello T. Chatrie: Sentencing set for 8/10/2022 at 02:00 PM in Richmond Courtroom 6100 before District Judge M. Hannah Lauck. (khan,) (Entered: 07/08/2022)
07/27/2022	233	PRESENTENCE INVESTIGATION REPORT (Sentencing Presentence Investigation Report) (SEALED – government and defense counsel) as to Okello T. Chatrie. (Harrison, Dorothy)INCLUDES ADDENDUM (Entered: 07/27/2022)
07/27/2022	235	Position on Sentencing by Okello T. Chatrie (Attachments: # 1 Exhibit B, # 2 Exhibit C)(Koenig, Laura) (Additional attachment(s) added on 7/27/2022: # 3 Ex. A Under Seal) (khan,). (Entered: 07/27/2022)
07/27/2022	236	Position on Sentencing by USA as to Okello T. Chatrie (Attachments: # 1 Exhibit Still Images from Surveillance and Threatening Letter)(Simon, Kenneth) (Entered: 07/27/2022)
08/08/2022	237	PRESENTENCE INVESTIGATION REPORT WITH SECOND ADDENDUM AND VICTIM IMPACT STATEMENTS (Sentencing Presentence Investigation Report) (SEALED – government and defense counsel) as to Okello T. Chatrie. (Attachments: # 1 VICTIM IMPACT STATEMENT #1, # 2 VICTIM IMPACT STATEMENT #2)(smith, lisa) (Entered: 08/08/2022)
08/10/2022	238	Minute Entry for proceedings held before District Judge M. Hannah Lauck:Sentencing held on 8/10/2022 for Okello T. Chatrie (1), Count(s) 1, 2, DISMISSED ON MOTION OF GOVT.; Count(s) 1s, 57 MONTHS IMPRISONMENT, 3 YEARS SUPERVISED RELEASE, $100 S/A, $196,932.01 RESTITUTION; Count(s) 2s, 84 MONTHS IMPRISONMENT TO BE SERVED CONSECUTIVE TO CT. 1, 3 YEARS SUPERVISED RELEASE TO BE SERVED CONCURRENT TO CT. 1, $100 S/A. Dft remanded to custody. (Court Reporter Diane Daffron, OCR.)(khan,) (Entered: 08/10/2022)
08/19/2022	239	JUDGMENT as to Okello T. Chatrie (1), Count(s) 1, 2, DISMISSED ON MOTION OF GOVT.; Count(s) 1s, 57 MONTHS IMPRISONMENT, 3 YEARS SUPERVISED RELEASE, $100 S/A, $196,932.01 RESTITUTION; Count(s) 2s, 84 MONTHS IMPRISONMENT TO BE SERVED CONSECUTIVE TO CT. 1, 3 YEARS SUPERVISED RELEASE TO BE SERVED CONCURRENT TO CT. 1, $100 S/A. Signed by District Judge M. Hannah Lauck on 8/19/22. (khan,) (Entered: 08/19/2022)
08/19/2022	240	Sealed Statement of Reasons as to Okello T. Chatrie. Signed by District Judge M. Hannah Lauck on 8/19/22. (khan,) (Entered: 08/19/2022)
08/25/2022	241	NOTICE OF APPEAL by Okello T. Chatrie as to 239 Judgment, 220 Memorandum Opinion, 221 Order on Motion to Suppress (Koenig, Laura) (Entered: 08/25/2022)
08/26/2022	242	Transmission of Notice of Appeal to 4CCA as to Okello T. Chatrie to US Court of Appeals re 241 Notice of Appeal. (All case opening forms, plus the transcript guidelines, may be obtained from the Fourth Circuit's website at

		www.ca4.uscourts.gov) (jsmi,) (Main Document 242 replaced on 8/29/2022) (jpow,). (Entered: 08/26/2022)
08/29/2022		USCA Case Number 22–4489, Case Manager A. Walker, for 241 Notice of Appeal filed by Okello T. Chatrie. (smej,) (Entered: 08/29/2022)
08/29/2022	243	ORDER of USCA as to Okello T. Chatrie re 241 Notice of Appeal. The court appoints the Federal Defender for the Eastern District of Virginia to represent appellant in this case. (22–4489) (smej,) (Entered: 08/29/2022)
09/06/2022	244	NOTICE *of Publication and Finality of Consent Order of Forfeiture* by USA as to Okello T. Chatrie re 231 Consent Order for Forfeiture of Property (Attachments: # 1 Declaration of Publication)(Lee, Janet) (Entered: 09/06/2022)
09/12/2022	245	TRANSCRIPT REQUEST by Okello T. Chatrie for proceedings held on May 9, 2022 (change of plea hearing) before Judge Lauck, (Pratt, Frances) (Entered: 09/12/2022)
09/13/2022	246	Transcript Order Acknowledgment from USCA re 241 Notice of Appeal: Court Reporter/Transcriber Diane Daffron. (smej,) (Entered: 09/13/2022)
10/04/2022	247	TRANSCRIPT of proceedings as to Okello T. Chatrie for dates of May 9, 2022 before Judge M. Hannah Lauck, re 241 Notice of Appeal Court Reporter Diane Daffron, Telephone number 804–916–2893. **NOTICE RE REDACTION OF TRANSCRIPTS:The parties have thirty(30) calendar days to file with the Court a Notice of Intent to Request Redaction of this transcript. If no such Notice is filed, the transcript will be made remotely electronically available to the public without redaction after 90 calendar days. The policy is located on our website at www.vaed.uscourts.gov** ***Does this satisfy all appellate orders for this reporter? y*** **Transcript may be viewed at the court public terminal or purchased through the court reporter before the deadline for Release of Transcript Restriction. After that date it may be obtained through PACER Redaction Request due 11/3/2022. Redacted Transcript Deadline set for 12/5/2022. Release of Transcript Restriction set for 1/2/2023.(daffron, diane) (Main Document 247 replaced at request of Court Reporter on 10/5/2022) (jsmi,). (Entered: 10/04/2022)**

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

UNITED STATES OF AMERICA	)	No. 3:19CR130
	)	
v.	)	Count 1: 18 U.S.C. §§ 2113(a), (d), and (e)
	)	Forced Accompaniment During Armed
OKELLO T. CHATRIE,	)	Credit Union Robbery
	)	
Defendant.	)	Count 2: 18 U.S.C. § 924(c)(1)(A)
	)	Use, Carry, and Brandish a Firearm During
	)	and in Relation to a Crime of Violence
	)	
	)	Forfeiture Allegation

September 2019 Term – at Richmond, Virginia

INDICTMENT

THE GRAND JURY CHARGES THAT:

COUNT ONE
(Forced Accompaniment during an Armed Credit Union Robbery)

On or about May 20, 2019, in the Eastern District of Virginia, the defendant, OKELLO T. CHATRIE, by force and violence, and intimidation, did take from the person and presence of another, namely J.W. and K.C., employees of the Call Federal Credit Union located at 3640 Call Federal Drive, Midlothian, Virginia, 23112, approximately $195,000 in United States currency, belonging to, and in the care, custody, control, management and possession of the Call Federal Credit Union, the accounts of which were then insured by the National Credit Union Administration Board; and in committing such offense, the defendant did knowingly and unlawfully assault and put in jeopardy the life of other persons, namely Call Federal Credit Union employees and customers, by the use of a dangerous weapon, namely a firearm; and further, the

defendant, in committing this offense, did knowingly and unlawfully force another person to accompany him without the consent of such person.

(In violation of Title 18, United States Code, Sections 2113(a), 2113(d), and 2113(e)).

COUNT TWO

(Use, Carry, and Brandish a Firearm During and in Relation to a Crime of Violence)

On or about May 20, 2019, in the Eastern District of Virginia, the defendant, OKELLO T. CHATRIE, did knowingly and unlawfully use, carry, and brandish a firearm during and in relation to a crime of violence for which he may be prosecuted in a court of the United States, that is, forced accompaniment during an armed credit union robbery, as charged in Count One of this Indictment, which is re-alleged as if fully set forth here.

(In violation of Title 18, United States Code, Sections 924(c)(1)(A)(i) and (ii)).

FORFEITURE ALLEGATION

Pursuant to Federal Rule of Criminal Procedure 32.2, the defendant, OKELLO T. CHATRIE, is notified that if convicted of Count One of this Indictment, the defendant shall forfeit to the United States, any property, real or personal, which constitutes or is derived from proceeds traceable to such violation.

This property includes, but is not limited to:

A sum of money of at least $195,000, which represents the total proceeds of the offense charged, to be partially offset by $102,293 seized from 1317 Willis Street, Richmond, Virginia, 23224 on August 13, 2019.

If the property subject to forfeiture cannot be located, the United States will seek an order forfeiting substitute assets.

The defendant is further notified that upon conviction of the offenses alleged in Count One or Count Two of this Indictment, the defendant shall forfeit any firearms and ammunition involved in or used in any knowing violation of such offenses.

Property subject to forfeiture includes, but is not limited to:

A 9 mm Taurus G2C pistol, serial number TLW87541; and

all accompanying ammunition.

(In accordance with Title 18, United States Code, Sections 924(d) and 981(a)(1)(C) as incorporated by Title 28, United States Code, Section 2461(c)).

A TRUE BILL:

FOREPERSON

G. ZACHARY TERWILLIGER
United States Attorney

Pursuant to the E-Government Act, the original of this page has been filed under seal in the Clerk's Office

By:
Kenneth R. Simon, Jr.
Peter S. Duffey
Assistant United States Attorneys

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	)	

DEFENDANT OKELLO CHATRIE'S MOTION TO SUPPRESS EVIDENCE OBTAINED FROM A "GEOFENCE" GENERAL WARRANT

Okello Chatrie, through counsel, moves the Court to suppress evidence that law enforcement obtained pursuant to a warrant authorizing state police to obtain the cell phone location information of 19 Google users who happened to be in the vicinity of a bank robbery on a Monday afternoon in Richmond. This is a "geofence" warrant, and it is an unlawful and unconstitutional general warrant that is both overbroad and lacks the particularity required by the Fourth Amendment. The Court should therefore suppress all evidence obtained from the warrant and all fruit of the poisonous tree, including the identification of Mr. Chatrie.

INTRODUCTION

Law enforcement obtained Mr. Chatrie's cell phone location information from Google using a "geofence" warrant. A geofence warrant requires Google to produce data regarding all devices using Google services within a geographic area during a given window of time. But unlike a typical warrant for location data, this geofence warrant did not identify Mr. Chatrie in any way. In fact, it did not identify any of the 19 people whose personal information was searched by the Virginia state police as a result. Instead, the warrant operated in reverse: it required Google to identify a large cache of deeply private data—held in the "Sensorvault"—and then allowed police

the discretion to obtain private information from devices of interest. This is nothing less than the modern-day incarnation of a "general warrant," and it is prohibited by the Fourth Amendment.

Virginia police obtained a warrant for the Sensorvault data in this case, presumably because they recognized, correctly, that such information is intensely private and constitutionally protected. Like the cell site location information ("CSLI") in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), cell phone users constantly generate Sensorvault location information by either (1) using devices running Google's software ("Android" phones), or (2) interacting with Google services (Maps, Gmail, Search, YouTube, etc.). *See* Background, *infra*. And as in *Carpenter*, users have a reasonable expectation of privacy in their location data, which is sensitive and revealing of the "privacies of life." 138 S. Ct. at 2214. Not only can this data reveal private activities in daily life, but it can also show that someone is inside a constitutionally protected space, such as a home, church, or hotel—all of which are in the immediate vicinity of the bank that was robbed in Richmond. The ability to access data that can locate individuals quickly, cheaply, and retroactively is an unprecedented expansion of law enforcement power, and doing so constitutes a Fourth Amendment search, just as it did in *Carpenter*. *Id* at 2230; *see also Prince Jones v. United States*, 168 A.3d 703, 712 (D.C. 2017) (recognizing that access to cell phone location data permits the "police to locate a person whose whereabouts were previously completely unknown."). In fact, the location data available in Google's Sensorvault is even more precise than the data in *Carpenter*. Google can pinpoint an individual's location to approximately 20 meters compared to "a few thousand meters" for cell site location data. Google, *Find and Improve Your Location's Accuracy* (Oct. 24, 2019), https://support.google.com/maps/answer/2839911?co=GENIE.Platform%3DAndroid&oco=1. Therefore, the third-party doctrine should not apply, and a valid warrant should be required for law enforcement to access any user's Sensorvault data.

Nonetheless, the fact that law enforcement obtained a warrant in this case does not save the search from constitutional infirmity. This is no ordinary warrant. It is a general warrant purporting to authorize a classic dragnet search of every Google user who happened to be near a bank in suburban Richmond during rush hour on a Monday evening. This is the kind of investigatory tactic that the Fourth Amendment was designed to guard against. Geofence warrants like the one in this case are incapable of satisfying the probable cause and particularity requirements, making them unconstitutional general warrants.

In the alternative, should the Court find that geofence warrants are not wholly impermissible under the Fourth Amendment, the warrant in this case fails to satisfy the particularity requirement and fails to establish probable cause to search Mr. Chatrie's Sensorvault data. Despite the prevalence of Google phones and services, there are no facts to indicate that the bank robber used either, whether ever or at the time of the robbery. There is no evidence that the robber used an Android operating system or accessed any Google service in connection with the crime. Instead, based only on Google's popularity and the prevalence of cell phones generally, law enforcement searched a trove of private location information belonging to 19 unknown Google users who happened to be near a local bank on a Monday evening. The government's generalized assumptions about cell phone use, devoid of any specific factual nexus to the criminal activities alleged, are insufficient to establish probable cause for the sweeping and invasive search in this case. Additionally, the discretion afforded to police to determine which accounts to search is the essence of an unparticularized warrant. In short, the warrant both lacks particularity and is fatally overbroad.

Finally, the good faith exception to the exclusionary rule does not apply to evidence obtained from this warrant. Given the lack of particularity and absence of probable cause for any

and all individuals whose data would be searched, no objectively reasonable officer could rely on such a warrant. For these reasons, the Court must suppress all evidence obtained from the geofence warrant and all fruit of the poisonous tree.

BACKGROUND

Over the last few decades, the ability of law enforcement to cheaply and easily access highly sensitive digital data has progressed in leaps and bounds. Requests for user information from cellular service providers and other online service providers like Google have become a powerful investigative tool for law enforcement to locate and identify almost any individual, as 96% of Americans now own cell phones. Pew Research Center, *Mobile Fact Sheet* (Jun. 12, 2019), http://www.pewinternet.org/fact-sheet/mobile/. As a result, "[o]nly the few without cell phones could escape this tireless and absolute surveillance." *Carpenter*, 138 S. Ct. at 2218.

Law enforcement can locate cell phones using user location data, which is collected and maintained by cell phone companies as well as third-party service providers, such as Google. For example, Google regularly collects detailed location information from all phones running Google's "Android" operating system. Android phones routinely transmit their GPS location to Google, but Google can also identify a phone's location based on nearby Wi-Fi networks, mobile networks, and device sensors. Google, *How Google Uses Location Information* (Oct. 25, 2019), https://policies.google.com/technologies/location-data. While it is possible to turn off location history on an Android phone, opening Google Maps or running a Google search will still pinpoint a user's latitude and longitude and create a record with Google. Ryan Nakashima, *Google Tracks Your Movements, Like it or Not*, Associated Press (Aug. 13, 2018), https://www.apnews.com/828aefab64d4411bac257a07c1af0ecb (identifying Google services that register a user's application upon use, including "Location History, Web and App activity, and …

device-level Location Services."). Even non-Android devices, such as Apple iPhones, transmit location information to Google when individuals use a Google service or application, such as Gmail, Search, and Maps. *Id.* Consequently, although Google's Sensorvault does not collect data on every phone, it nevertheless contains an enormous trove of location information on most Android phones and many iPhones in use in the United States.

In recent years, law enforcement has begun requesting this data from Google using geofence warrants to identify devices present in a geographic area during a window of time. Jennifer Valentino-DeVires, *Tracking Phones, Google Is a Dragnet for the Police*, N.Y. Times (Apr. 13, 2019), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html. Since a geofence warrant identifies a geographic area, and not a suspect, these requests "ensnare anyone who uses Google services at specific times in the . . . areas [near a crime]," sweeping up innocent individuals in an unconstitutional dragnet search. Debra Cassens Weiss, *FBI Asks Google to Turn Over All Data on Users Who Were Close to Robbery Locations*, ABA Journal (Oct. 25, 2018), http://www.abajournal.com/news/article/fbi_asks_google_for_location_data_on_anyone_close_to_robbery_locations_in_t. Individuals may be caught up in this search by merely using an Android phone, conducting an internet search using Google, running a Google application such as Google Maps or YouTube, or even receiving an automatic weather update from an Android service. Nakashima, *supra*, *Google Tracks Your Movements, Like it or Not*.

FACTS

Geofence warrants compel Google to produce location information about devices interacting with Google technology within a geographic area during a given timeframe. In this case, the government requested data from Google regarding all Google devices that were within 150 meters of the Call Federal Credit Union in Richmond, Virginia, during a one-hour period at

the beginning of Monday evening rush hour. Specifically, the warrant sought information on all devices within 150 meters of 37° 26' 18.3" N, 77° 35' 16.4" W between 4:20 and 5:20 p.m. EST. *See* Ex. A State Warrant at 3[1]. In addition to a major thoroughfare (U.S. Route 360), the immediate area includes a Ruby Tuesday restaurant, a Hampton Inn hotel, a mini storage facility, an apartment complex for seniors, another residential apartment complex, and the Journey Christian Church, a very large[2] church located directly across from the Credit Union. The 150-meter radius encompasses both the bank and the church as well as their parking lots.

The warrant describes a three-step process. First, Google provided "anonymized information" about all Google users in the area between 4:20 and 5:20 p.m., including "a numerical identifier for the account, the type of account, time stamped location coordinates and the data source." *See* Ex. A (State Warrant) at 2. This initial search affected 19 unique Google users, yielding 209 location points over an hour. *See* Ex. B (Excel Sheet 1). Law enforcement then reviewed the data and attempted to "narrow down the list" based on other known information. *See* Ex. A (State Warrant) at 2. Next, in a private letter to Google without any additional judicial scrutiny, police requested additional "contextual data points with points of travel *outside* of the [geofence]" and for "30 minutes before AND 30 minutes after the initial search time periods" for a subset of 9 users. *Id*. (emphasis added). This produced 680 location points over a total of two hours. *See* Ex. C (Excel Sheet 2). Finally, police returned to Google once again to obtain

[1] The government has provided the defense with a sealed copy of this search warrant with no explanation as to why it remains sealed. Per the Chesterfield County Circuit Court Clerk's Office, this warrant and its supporting documents will remain sealed absent further intervention from the government until December 19, 2019. Because the document is and will remain sealed until further action by the government, Mr. Chatrie does not attach it here, but refers to it for when the Court is able to review a copy.

[2] In 2017, Outreach Magazine, which tracks church attendance and congregation growth rates, reported that Journey Christian Church had 1,743 people attend its church and ranked as one of the fastest-growing congregations in the country. Outreach Magazine, Journey Christian Church, https://outreach100.com/churches/journey-christian-church.

"identifying account information/CSI" for 3 users, including: usernames, subscriber information, as well as all email addresses, electronic devices, and phone numbers associated with the accounts.[3] *See* Ex. A (State Warrant) at 3.

ARGUMENT

The acquisition of Mr. Chatrie's data from Google was a Fourth Amendment search. In either event, the action intruded upon Mr. Chatrie's reasonable expectation of privacy in his location data. This is critical because the warrant obtained by Virginia police is invalid. It is a general warrant, irredeemably unreasonable and completely impermissible under the Fourth Amendment. Law enforcement simply cannot establish the requisite probable cause and particularity to search a trove of data belonging individuals suspected of no wrongdoing. As a result, the warrant is also fatally overbroad and lacking particularity. Such a 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.").

I. The Acquisition of Mr. Chatrie's Data from Google Was a Fourth Amendment Search.

In *Carpenter*, the Supreme Court held that individuals have a reasonable expectation of privacy in their cell phone location data, and that the government's acquisition of those records in that case was a Fourth Amendment search. 138 S. Ct. at 2217. This holding applies with equal force in the context of a location data request directed to Google, which involves information that is more precise than the data at issue in *Carpenter*. Regardless of whether the Court analyzes this

[3] The warrant does not define "CSI" at any point in the warrant or application.

claim under the reasonable expectation of privacy framework set forth in *Katz* or a property-based theory, it should reach the conclusion that acquisition of Defendant's location information constituted a Fourth Amendment search.

A. Cell Phone Users Have a Reasonable Expectation of Privacy in Their Location Information.

In considering whether individuals reasonably expect information to remain private, the Supreme Court has crafted "a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); *see also Carpenter*, 138 S. Ct. at 2219 (applying the *Katz* analysis in the context of historical cell site location information and concluding that users have a reasonable expectation of privacy in this information). Cell phone location information is highly sensitive, as shown by the watershed decision in *Carpenter*, and this classification applies to Google's Sensorvault location data based on the strong similarities between the two types of information. In the majority opinion, Justice Roberts emphasized the revealing nature of historical cell site location information and compared this quality to that of GPS location information. *Id.* at 2217. ("*As with GPS information*, the time-stamped data provides an intimate window into a person's life, revealing … his particular movements" (citation omitted) (emphasis added)). GPS is one of the primary methods that Google uses to compile Sensorvault location data. Google, *supra*, *How Google Uses Location Information*. Google also includes location data from mobile networks, *id.*, the same technology at issue in *Carpenter*.

The fact that Google, a third-party service provider, collects and maintains this location information does not diminish an individual's expectation of privacy in it. *Carpenter*, 138 S. Ct. at 2220. While the third-party doctrine stands for the general proposition that an individual has a

reduced expectation of privacy in information knowingly shared with another, the rule is not to be "mechanically" applied in the digital age. *Id.* at 2219. To do so would "[fail] to contend with the seismic shifts in digital technology that made possible the tracking of not only [Mr. Chatrie's] location but also everyone else's, not for a short period but for years and years." *Id.* Indeed, Google is no ordinary third party: "Unlike the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible." *Id*. The fact that Google is able to provide location data information for a given place and time in the past is possible only because of its exhaustive and constant collection of user data.

In *Carpenter*, the Court rejected the government's contention that the third-party doctrine applied to historical cell-site information, and this holding applies to cell phone location data acquired through Google. The Court provided two main rationales for its decision: cell-site location information is qualitatively different from types of business records to which the doctrine may apply based on its revealing nature, and users do not voluntarily share their cell-site location information with their service provider. 138 S. Ct. at 2219–20. These two rationales apply with equal force to the location information Google stores, and as such third-party doctrine is inapposite to data gleaned from Google under the warrant.

Google location records are qualitatively different from the business records to which the third-party doctrine traditionally applies. *See Smith v. Maryland*, 442 U.S. 735, 742 (numbers dialed on a landline); *United States v. Miller*, 425 U.S. 435, 440 (1976) (bank deposit slips). Instead, they reveal the same type of information as the cell-site location data considered private in *Carpenter*, and they do so in an even more precise manner. Google, *supra, Find and Improve Your Location's Accuracy*. As the Supreme Court determined, "[t]here is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and [an]

exhaustive chronicle of location information." *Carpenter,* 138 S. Ct. at 2219. Location data from Google is similarly "exhaustive." Google routinely collects detailed location data on every user, not just when criminal activity is suspected. And when police obtain this information with a geofence warrant, it is also comprehensive, revealing every Google user who happened to pass through a given area over a given timeframe. In short, Google location data is qualitatively different from third-party business records, and regardless of the fact that Google stores it, it is entitled to a reasonable expectation of privacy.

Individuals do not voluntarily share their location information with Google, further supporting the notion that the third-party doctrine is inapposite in this context. The third-party doctrine is justified by the assumption that an individual cannot reasonably expect "information he *voluntarily* turns over to third parties" to remain private. *Smith*, 442 U.S. at 44 (emphasis added). In *Carpenter*, the Court held that cell phone users' "sharing" of their location data with their service provider is not done on a truly voluntary basis since "carrying [a cell phone] is indispensable to participation in modern society." 138 S. Ct. at 2220 (quoting *Riley*, 134 S. Ct. at 2484)). Similarly, navigation apps are exceedingly popular, with 77% of smartphone owners using them regularly, and Google Maps is far and away the most popular navigation app. Riley Panko, *The Popularity of Google Maps: Trends in Navigation Apps in 2018*, The Manifest (July 10, 2018), https://themanifest.com/app-development/popularity-google-maps-trends-navigation-apps-2018. This shows that, like owning a smartphone, using navigation software is, for many, "indispensable to participation in modern society." *Carpenter*, 138 S. Ct. at 2210. Much the same could be said about Gmail or Google Search. Indeed, Google software is ubiquitous on smartphones, with Android operating systems running on 87% of devices sold in 2019. International Data Corporation, *Smartphone Market Share*, https://www.idc.com/promo/smartphone-market-

share/os, Oct. 25, 2019. Likewise, Google Maps is the most popular navigation app, used on 67% of smartphones, making it nearly six times more popular than its closest competitor Waze, which is now also owned by Google.[4] Panko, *supra*, The *Popularity of Google Maps*. And more than 90% of all internet searches use Google. Jeff Desjardins, *How Google retains more than 90% of market share*, Business Insider (Apr. 23, 2018), https://www.businessinsider.com/how-google-retains-more-than-90-of-market-share-2018-4. In short, it is not reasonable to expect ordinary phone users to avoid Google software. It cannot be that individuals must choose between their privacy and carrying a cell phone, running a Google search, or watching a YouTube video.

B. Geofence Warrants Provide the Government with Unprecedented Powers of Surveillance that Upset Traditional Expectations of Privacy.

In a series of cases addressing the power of sense-enhancing technologies "to encroach upon areas normally guarded from inquisitive eyes," the Supreme Court "has sought to 'assure [ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" *Carpenter*, 138 S. Ct. at 2214 (quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001)) (last alteration in original); *accord United States v. Jones*, 565 U.S. 400, 406 (2012). As Justice Alito explained in *Jones*, "[i]n the precomputer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken." 565 U.S. at 429 (Alito, J., concurring in judgment).

Technological innovations, like the ability to locate cell phones (and their users) seemingly out of thin air, remove many of these practical limitations on government surveillance capabilities. *See, e.g., Prince Jones*, 168 A.3d at 714 (describing a cell-site simulator as a "powerful person-locating capability" that the government previously lacked, which is "only superficially analogous

[4] It is unclear whether use of the Waze app also contributes location data to Google's Sensorvault.

to the visual tracking of a suspect"). Recognizing the potential for technologies like these to enable invasive surveillance on a mass scale, the Court has admonished lower courts to remain vigilant "to ensure that the 'progress of science' does not erode Fourth Amendment protections." *Carpenter*, 138 S. Ct. at 2223.

1. The data collected through a geofence warrant is extraordinarily detailed and deeply revealing.

The *Carpenter* Court noted that "like GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic, and effortlessly compiled." 138 S. Ct. at 2216. Google's Sensorvault includes GPS data, which is even more precise than the cell site location information at issue in *Carpenter*. Google, *supra, Find and Improve Your Location's Accuracy*. Google also locates users using "device sensors . . . or WiFi" to augment GPS's accuracy when these methods are available. Google Policies, Location Data (Nov. 20, 2018), https://policies.google.com/technologies/location-data?hl=en. As a result, Google can locate a device within approximately 20 meters, compared to "a few thousand meters" for cell site location information. Google, *supra, Find and Improve Your Location's Accuracy*. This level of precision can pinpoint a device to a single a building, which is significantly more detailed that the location information available from wireless carriers like AT&T or Verizon. Russell Brandom, *Police Are Filing Warrants for Android's Vast Store of Location Data*, The Verge (June 1, 2016), https://www.theverge.com/2016/6/1/11824118/google-android-location-data-police-warrants.

Indeed, Google location data can reveal information about a user's location inside constitutionally protected areas. Individuals tend to carry cell phones at all times, "into private residences, doctor's offices, political headquarters, and other potentially revealing locales," *Carpenter*, 138 S. Ct. at 2218. In this case, the 150-meter geofence fully encompasses the Journey Christian Church, which has over 3,600 followers on Facebook. Journey Christian Church,

Facebook (Oct. 25, 2019), https://www.facebook.com/JourneyRVA/. A church, like a home, is a constitutionally protected space, especially because of its obvious First Amendment significance. But when law enforcement obtained the list of Google users near the bank, it also obtained the data of Google users inside Journey Christian Church, intruding on this quintessentially protected space and violating churchgoers' reasonable expectation of privacy. Such intrusions are "presumptively unreasonable in the absence of a search warrant." *Katz,* 389 U.S. at 361; *Kyllo*, 533 U.S. at 31 ("'At the very core' of the Fourth Amendment 'stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'") (quoting *Silverman v. United States,* 365 U.S. 505 (1961)).

When Fourth Amendment searches implicate First Amendment concerns, courts should be careful to apply Fourth Amendment requirements with "the most scrupulous exactitude," *Stanford v. Texas*, 379 U.S. 476, 485 (1965). Additional safeguards may be constitutionally required to protect First Amendment freedoms, *Marcus v. Search Warrant of Property*, 367 U.S. 717, 729 (1961). But the warrant application in this case did not even mention[5] the proximity of the church or take into account the sensitive First Amendment associations and activities that the search may reveal. Instead, it unconstitutionally left "the protection of [First Amendment] freedoms to the whim of the officers charged with executing the warrant." *Stanford,* 379 U.S. at 485.

2. A Geofence Warrant Allows Law Enforcement to Retrospectively Locate Individuals in Time and Space.

In *Carpenter*, the Supreme Court distinguished cell site location information from traditional law enforcement surveillance due to "the retrospective quality of the data" which "gives police access to a category of information otherwise unknowable." *Id.* at 2218. As the Court

[5] In fact, the warrant appears to refer to the church as simply "an adjacent business." *See* Ex. A State Search Warrant at 5.

explained, it is akin to a time machine that allows law enforcement to look at a suspect's past movements, something that would be physically impossible without the aid of technology: "[i]n the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection." *Id*. Geofence warrants likewise represent an unprecedented expansion of law enforcement's ability to locate a person in time and space. They enable law enforcement to reconstruct an individual's historical movements, something that would have been impossible at the time of the adoption of the Fourth Amendment at this level of ubiquity, specificity, and cost. And as with cell cite location information, they now allow the government to "travel back in time to retrace a person's whereabouts, subject only to [Google's] retention polices." *Id.*

The Supreme Court has never blessed anything remotely like dragnet geofence warrants as a permissible means of surveillance. Like the surreptitious GPS tracking in *Jones*, 565 U.S. at 420 (Alito, J., concurring), or the acquisition of historical CSLI in *Carpenter*, 138 S. Ct. at 2217, this search could not have been conducted through visual surveillance alone. It therefore violates a reasonable expectation of privacy and is impermissible under the Fourth Amendment. *Cf. Kyllo v. United States*, 533 U.S. 27, 40 (2001) (use of a thermal imaging device is a search because the information gleaned "would previously have been unknowable without [a] physical intrusion."); *Prince Jones*, 168 A.3d 703, 714 (D.C. 2017) (use of a "cell site simulator" to locate a person through a cell phone is a search because the information is not readily available or in the public view, unlike visual surveillance or older generations of tracking devices).

C. The Acquisition of Defendant's GPS Data from Google Was a Search Under a Property-Based Approach to the Fourth Amendment.

Under a property-based theory of the Fourth Amendment, Mr. Chatrie's GPS data constitutes his "papers or effects," regardless of whether they are held by a third-party service

provider like Google. They therefore cannot be searched or seized without a *valid* warrant. *Carpenter*, 138 S. Ct. at 2268 (Gorsuch, J., dissenting).

In his dissenting opinion in *Carpenter*, Justice Gorsuch opined that under a "traditional approach" to the Fourth Amendment, the protection against unreasonable searches and seizures applied as long as "a house, paper or effect was yours under law." *Id.* Justice Gorsuch drew a strong analogy between cell phone location data and mailed letters, in which people have had an established Fourth Amendment property interests for over a century, whether or not these letters are held by the post office. *Id.* at 2269. (citing *Ex parte Jackson*, 96 U.S. 727, 733 (1877)). Just as Gmail messages belong to their senders and recipients (and not to Google), so too does Google location data belong to the Google users who generate it.

Here, Mr. Chatrie's location information belongs to Mr. Chatrie. Google may be responsible for collecting and maintaining it, but even Google understands that it is the user's private data. For example, Google's privacy policy consistently refers to user data as "your information," which can be managed, exported, and even deleted from Google's servers at "your" request. Google, Privacy Policy (Oct. 26, 2019), https://policies.google.com/privacy#infodelete. These are not "business records." Businesses do not let customers export or delete the company's records at will. These are customer records—Mr. Chatrie's records. Mr. Chatrie merely entrusted his information to Google, as so many people do. He did not forfeit his Fourth Amendment interests in it.

As Justice Gorsuch explained in *Carpenter*, "[e]ntrusting your stuff to others is a bailment. A bailment is the 'delivery of personal property by one person (the bailor) to another (the bailee) who holds the property for a certain purpose.'" 138 S. Ct. at 2268–69 (Gorsuch, J., dissenting). Here, Google is the bailee, and it owes a duty to the bailor, Mr. Chatrie, to keep his data safe. This

arrangement is apparent from Google's privacy policy. Google is not allowed to do whatever it wishes with Mr. Chatrie's data. While Google reserves the right to use it for advertising or development purposes, it also promises not to disclose it to "companies, organizations, or individuals outside of Google," subject to a short list of explicit exceptions.[6] In other words, Mr. Chatrie retains the right to exclude others from his location data, a quintessential feature of property ownership. *See* William Blackstone, 2 Commentaries on the Laws of England *2 (1771) (defining property as "that sole and despotic dominion … exercise[d] over the external things … in total exclusion of the right of any other."); *Loretto v. Teleprompter Manhattan CATV Corp.*, 458 U.S. 419, 435 (1982) (calling the right to exclude "one of the most treasured strands" of the property rights bundle); *Kaiser Aetna v. United States*, 444 U.S. 164, 176 (1979) (calling the right to exclude "one of the most essential sticks" in the property rights bundle).

Law enforcement eviscerated Mr. Chatrie's right to exclude others from his location data, which Google held in trust for him. This trespass constitutes a Fourth Amendment search and seizure, no less than a violation of one's "reasonable expectation of privacy."

II. A Geofence Warrant Is an Unconstitutional General Warrant.

A geofence warrant, like the warrant in this case, is a general warrant, repugnant to the Constitution. It is the epitome of the "dragnet" law enforcement practice that the Supreme Court feared in *Knotts*, 460 U.S. at 284, sweeping up the location data of untold innocent individuals in the hopes of finding one potential lead. It is inherently overbroad and lacking particularity by design. It cannot satisfy the Fourth Amendment with "scrupulous exactitude" because it is

[6] Google, Privacy Policy (Oct. 26, 2019), https://policies.google.com/privacy#infosharing. One of these exceptions is "For legal reasons," but this is not a free pass to hand over user data to law enforcement. It is implied that legal process must be valid, which includes establishing probable cause and following the strictures of the Fourth Amendment, not just submitting the proper form. *See* Jim Harper, *The Fourth Amendment and Data: Put Privacy Policies in the Trial Record*, The Champion, Jul. 2019, at 21.

inherently antithetical to the Fourth Amendment. The Court should find that geofence warrants like this one are categorically invalid and void *ab initio.*

A. The Fourth Amendment Forbids General Warrants.

As the Supreme Court has repeatedly recognized, opposition to general warrants "helped spark the Revolution itself," demonstrating the degree to which they offend the most basic principles of American liberty. *Carpenter*, 138 S. Ct. at 2213; *see also Riley*, 573 U.S. at 403; *Stanford*, 379 U.S. at 481; *Marcus*, 367 U.S. at 728. The Virginia Declaration of Rights, like other founding documents, also reflects this colonial hostility to general warrants by explicitly and categorically prohibiting them:

> That general warrants, whereby an officer or messenger may be commanded to search suspected places without evidence of a fact committed, *or to seize any person or persons not named*, or whose offense is not particularly described and supported by evidence, are grievous and oppressive, and ought not to be granted.

Va. Const. art. I, § 10 (emphasis added); *see also Zimmerman v. Town of Bedford*, 134 Va. 787, 800 (1922). They are likewise forbidden by Virginia Code § 19.2–54 ("no general warrant for the search of a house, place, compartment, vehicle or baggage shall be issued"); *see also Morke v. Commonwealth*, 14 Va. App. 496, 500 (1992) (stating general warrants are proscribed by both the Fourth Amendment and Code § 19.2–54).

At the time of the Revolution, a general warrant meant a warrant that failed to identify the people to be arrested or the homes to be searched. *See Steagald v. United States*, 451 U.S. 204, 220 (1981) ("The general warrant specified only an offense . . . and left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched."). For example, one of the specific cases that gave rise to the Fourth Amendment was *Wilkes v. Wood*, 98 Eng. Rep. 489, 490 (1763), which concerned a general warrant that ordered

the king's messengers to "apprehend and seize the printers and publishers" of an anonymous satirical pamphlet, the *North Briton* No. 45. The warrant did not specify which houses to search or whom to arrest, but officials ransacked five homes, broke down 20 doors, rummaged through thousands of books and manuscripts, and arrested 49 people. *See* Thomas K. Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment*, 86 Ind. L.J. 979, 1007 (2011). The *Wilkes* court condemned the warrant because of the "discretionary power" it gave officials to decide where to search and what to take. 98 Eng. Rep. at 498. The case became wildly famous in the American colonies, one of three influential English cases that led to the rejection of general warrants.[7]

One reason the Founders opposed general warrants was because of the discretion they gave to officials. They placed "'the liberty of every man in the hands of every petty officer'" and were therefore denounced as "'the worst instrument of arbitrary power." *Stanford*, 379 U.S. at 481 (quoting James Otis). The other reason was that general warrants allowed the government to target people without any evidence of criminal activity, turning the concept of innocent until proven guilty on its head. Donohue, 83 U. Chi. L. Rev. at 1317. Instead of having information that the person or place to be searched is engaged in illegal activity, general warrants presume guilt, establishing innocence only after a search. *Id.* Prohibiting such "promiscuous" searches therefore served to protect not only individual rights, but also a cornerstone of American liberty. *Id.*

Thus, for example, no valid search warrant would permit the police to search every house in a neighborhood or pat down everyone in sight. *See United States v. Glenn*, 2009 WL 2390353, at *5 (S.D. Ga. 2009) ("The officers' 'generalized' belief that some of the patrons whom they had

[7] *See generally*, Laura K. Donohue, *The Original Fourth Amendment*, 83 U. Chi. L. Rev. 1181, 1196 (2016). In addition to *Wilkes v. Wood*, the cases were *Entick v Carrington*, 19 How St Tr 1029 (CP 1765), and *Leach v Money*, 19 How St Tr 1001 (KB 1765).

targeted for a systematic patdown might possibly have a weapon was insufficient to justify a 'cursory' frisk of everyone present."); *Commonwealth v. Brown*, 68 Mass. App. Ct. 261, 262 (Mass. App. Ct. 2007) (holding that a warrant "authorizing a search of 'any person present' . . . resulted in an unlawful general search."); *Grumon v. Raymond*, 1 Conn. 40, 43 (1814) (holding that a "warrant to search all suspected places [for stolen goods]" was unlawful because "every citizen of the United States within the jurisdiction of the justice to try for theft, was liable to be arrested"). Yet, with a geofence warrant, law enforcement can do just that, searching inside every home, vehicle, purse, and pocket in a given area, without particularized suspicion to search any of them.

B. A Geofence Warrant Is A General Warrant.

A geofence warrant, like the one in this case, is a modern-day incarnation of the historically reviled general warrant. It is the digital equivalent of searching every home in the neighborhood of a reported burglary, or searching the bags of every person walking along Broadway because of a theft in Times Square. Without the name or number of a single suspect, and without ever demonstrating any likelihood that Google even has data connected to a crime, law enforcement invades the privacy of tens or hundreds or thousands of individuals, just because they were in the area. *Cf. Sibron v. New York*, 392 U.S. 40, 63–64 (1968) (holding that "[t]he suspect's mere act of talking with a number of known narcotics addicts over an eight-hour period" did not give rise to either reasonable suspicion or probable cause to search him).

The Supreme Court has always been "careful to distinguish between [] rudimentary tracking . . . and more sweeping modes of surveillance," in deciding whether a search is constitutional. *Carpenter*, 138 S. Ct. at 2215 (citing *Knotts*, 460 U.S. at 284). Geofence warrants fall on the "sweeping" end of this spectrum, as they potentially affect everyone. They represent

the kind of surveillance that the Supreme Court cautioned against in *Knotts*, noting that "if such dragnet type law enforcement practices . . . should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable." 460 U.S. at 283–84. That time is now.

A comparison to the "rudimentary tracking" in beeper cases such as *Knotts* and *Karo* illuminates the drastically different, indiscriminate-dragnet nature of a geofence warrant. In the beeper cases, the government only sought to track *one* individual. To do so, law enforcement first needed to identify the individual, and then to physically install a tracking device on an object that was in their possession. With a geofence warrant, however, the government no longer needs identify a suspect. Instead, "[w]ith just the click of a button, the government can access [Google's] deep repository of historical location information at practically no expense." *Carpenter*, 138 S. Ct. at 2218; *see also United States v. Garcia*, 474 F.3d 994, 998 (7th Cir. 2007) ("Technological progress poses a threat to privacy by enabling an extent of surveillance that in earlier times would have been prohibitively expensive"). Because of the ubiquity of Google software on cell phones, Sensorvault includes location data on many of the 400 million devices in the United States—"not just those belonging to persons who might happen to come under investigation," meaning that "this newfound tracking capacity runs against everyone" who uses Google. *Carpenter*, 138 S. Ct. at 2218.

Geofence warrants pose the same type of threat as colonial-era general warrants "which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity." *Riley*, 134 S. Ct. at 2494. As in this case, they are the product of unrestrained searches of constitutionally protected spaces, like the Journey Christian Church. And they result

in rummaging through the digital papers and effects of large numbers of unknown, unnamed people, all or almost all of whom are admittedly innocent.

C. A Geofence Warrant Cannot Satisfy the Probable Cause or Particularity Requirements.

By design, a geofence warrant does not specify the individuals or individual Google accounts to be searched. Rather, the purpose is to search across millions of unknown user accounts and then identify specific accounts that law enforcement would like to search further. As a result, however, geofence warrants are inherently incapable of meeting the probable cause and particularity requirements of the Fourth Amendment, and are therefore general warrants.

Geofence warrants are intentionally overbroad. In contrast to warrants authorizing the acquisition of location data about a single individual suspected of a criminal offense, geofence warrants identify all Google users merely due to their proximity to a crime scene. But as the Supreme Court has held on more than one occasion, "a person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person." *Ybarra v. Illinois,* 444 U.S. 85, 91 (1979) (citing *Sibron*, 392 U.S. at 62–63); *see also United States v. Di Re*, 332 U.S. 581, 587 (1948) (holding that a person, by mere presence in a suspected car, does not lose immunities from search of his person to which he would otherwise be entitled). Consequently, there is an abject absence of individualized suspicion for any, let alone all, of the individuals whose Google data were searched by the warrant. Of course, it would have been difficult to establish probable cause for the location information of every Google user near the bank, as the government acknowledges that most of the data belongs to innocent people. But the convenience of gathering location information on all of those individuals with a single warrant to Google does not obviate the requirements of the Fourth Amendment. *Riley,* 134 S. Ct. at 2493 (citing *Coolidge v. New Hampshire*, 403 U.S. 443, 481 (1971)); *Carroll v.*

United States, 267 U.S. 132, 153–54 (1925) ("It would be intolerable and unreasonable if a prohibition agent were authorized to stop every automobile on the chance of finding liquor, and thus subject all persons lawfully using the highways to the inconvenience and indignity of such a search."). The warrant is void for lack of probable cause.

Similarly, a geofence warrant is not remotely particularized. The purpose of the particularity requirement is to prevent general warrants, which it does by "limiting the authorization to search the specific areas and things for which there is probable cause to search." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). With respect to seizures, the Fourth Amendment demands that "nothing is left to the discretion of the officer executing the warrant." And where, as here, there are significant First Amendment concerns—especially due to the proximity of a church—the particularity requirement takes on heightened importance. *Stanford*, 379 U.S. at 485; *Marcus*, 367 U.S. at 729; *A Quantity of Copies of Books v. Kansas*, 378 U.S. 205, 212 (1964).

A geofence warrants leaves the question of whose data to search and seize almost entirely the discretion of the executing officers. It does not "particularly describe the 'things to be seized,' let alone identify the name of a single suspect Google user, phone number, or account. *Dalia v. United States*, 441 U.S. 238, 255 (1979) (citing *Stanford v. Texas*, 379 U.S. 476, 485 (1965)). Instead, it identifies Google headquarters as the place to be searched and requests location data from *all* Google users near a given location. Although the data is "anonymized" initially, it does not stay that way. Rather, the warrant leaves it up to the police to "narrow down the list" by some unknown or unstated method before the officers decide which accounts to deanonymize and search further. *See* Ex. A State Search Warrant at 2. Law enforcement engage in multiple rounds of back-and-forth with Google—not the independent magistrate envisioned by the Fourth Amendment—

to decide whose data they would review. Paired with the sweeping scope and absence of probable cause, the lack of particularity in geofence warrants make them unconstitutional general warrants.

D. This Geofence Warrant is Overbroad and Lacking Particularity

Even if geofence warrants are not categorically impermissible, the geofence warrant obtained in this case is unconstitutionally overbroad and lacks particularity.

First, Virginia police did not have probable cause to believe that the bank was robbed by a Google user. While the warrant application does state that the robber could be seen using a cell phone, there is no evidence to show that it was an Android phone or that he or she used a Google service within the initial one-hour window identified in the warrant. The application cites the general popularity of cell phones, but does not provide any facts to suggest that Google specifically would have data pertaining to the perpetrator of this crime. It did not allege that bank robbers frequently use Google or state that a teller had noticed the phone's make and model. If the robber had an iPhone and did not use Google services between 4:20 and 5:20 p.m., then Google would not have a record of the phone's location during that time.[8]

Second, the warrant does not specify which Google accounts it seeks to search, presumably due to the lack of probable cause to search any specific Google user. Even the 150-meter radius is not sufficiently particular. Rather than a requesting data for just the bank and parking lot, the warrant included the entirety of the church next door. Furthermore, a three-step, back-and-forth process with the recipient of a warrant is not a substitute for particularizing that warrant at the outset. Instead, it is an unconstitutional delegation of discretion to the executing officers. The

[8] Likely for this reason, the use of geofence warrants elsewhere has frequently failed to identify suspects. *See* Tyler Dukes, *To find suspects, police quietly turn to Google*, WLAR (Mar. 15, 2018), https://www.wral.com/Raleigh-police-search-google-location-history/17377435/ (finding that "only one person has been arrested for any of the crimes in which police approached Google for data on *thousands of users*" across the four investigations).

issuing court had no information on how many people were likely to be initially affected. And it had no role in deciding which of those people would be subject to further search, outside the geofence, wherever they happened to be. Indeed, the warrant permits police to obtain location data from *anywhere outside* the geofence for an unknown subset of users, identified solely by investigators, with no additional showing or judicial involvement. *See* Ex. A State Search Warrant at 2. Finally, the court had no role in deciding which or how many people would have their data deanonymized and searched further still. The warrant left everything up to the discretion of the executing officers, violating the Fourth Amendment's particularity requirement.

III. The Good Faith Exception Does Not Apply

Under the good-faith exception to the exclusionary rule, evidence derived from an unconstitutional search should not be suppressed when it is obtained in reliance on a facially valid warrant. *United States v. Leon*, 468 U.S. 897 (1984). The Supreme Court has emphasized, however, that "in some circumstances the officer will have no reasonable grounds for believing that the warrant was properly issued." *Id.* at 922-23. There, the good faith exception would not apply, and suppression would be appropriate "if the officers . . . could not have harbored an objectively reasonable belief in the existence of probable cause." *Id.* at 926. Suppression is also appropriate where "a warrant may be so facially deficient—i.e., in failing to particularize the place to be searched or the things to be searched—that the executing officers cannot reasonably presume it to be valid." *Id.*

Here, a reasonable law enforcement officer could not have presumed that such an overbroad, unparticularized warrant would be valid. The police knew they did not have a suspect, let alone probable cause to search any specific person or place. Instead, they sought every Google user's location data near a bank at rush hour—with no evidence that the robber had ever used

Google. They then exercised complete discretion in deciding which accounts to search further, deanonymize, and obtain additional information about. The deficiencies of this geofence warrant—its absence of probable cause and particularity—are readily apparent, casting it within the circumstances described in *Leon* and making the good faith exception to the exclusionary rule inapplicable.

CONCLUSION

This is a case of first impression, but the Court should treat the geofence warrant here as any other general warrant: repugnant to the Constitution. Geofence warrants represent an unprecedented expansion of the government's surveillance capabilities. *Carpenter*'s emphasis on the degree to which location data obtained by law enforcement is sensitive or "deeply revealing" shows that courts are recognizing the need to treat cell phone data differently from physical records. Based on the sensitivity of these records and the scope of the search, geofence warrants are Fourth Amendment searches of the unreasonable variety. The warrant obtained in this case implicates First Amendment concerns, and as such must withstand "scrupulous exactitude" under the Fourth Amendment. Yet this geofence warrant cannot even survive the probable cause and particularity under the Fourth Amendment. Instead, the warrant functions as a general warrant, thus not meeting the higher First Amendment standard. Finally, because the good faith exception cannot apply to a warrant no reasonable law enforcement officer would in good faith rely on, this geofence warrant is an unconstitutional search, and we therefor request that its fruits be suppressed.

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

CERTIFICATE OF SERVICE

I hereby certify that on October 29, 2019, I filed the foregoing with the Clerk of Court using the CM/ECF system, which will send a notification of such filing (NEF) to all counsel of record.

_____/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

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 OF EVIDENCE OBTAINED PURSUANT TO GOOGLE GEOFENCE WARRANT

The United States of America, by its undersigned attorneys, moves this Court to deny Defendant Okello T. Chatrie's motion to suppress evidence obtained from Google, LLC ("Google") pursuant to a search warrant for GeoFence location information (the "GeoFence warrant"). (ECF No. 29.)

The warrant authorized disclosure from Google of two hours of location information associated with electronic devices that were, within a one-hour interval, within 150 meters of the site of a bank robbery. This Court should deny the defendant's motion for three reasons. First, investigators did not conduct a search under the Fourth Amendment when they obtained this information from Google. Second, the GeoFence warrant complied with the Fourth Amendment, as it was issued based on probable cause and specified its object with particularity. Third, suppression is inappropriate because investigators relied on the warrant in good faith.

I. BACKGROUND

At approximately 4:50 p.m. eastern standard standard time, on May 20, 2019, a then-unknown male entered the Call Federal Credit Union in Midlothian, Virginia with a firearm. While the man stood in line, victim-teller J.B. asked another teller, J.W., to assist this customer

when he reached the counter. When he reached J.W.'s station, the man presented a handwritten note. That note 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." After J.W. told him that she did not have access to that amount of money, the armed robber pulled out a silver and black handgun. Waving the firearm around, he then directed J.W., other Call Federal Credit Union employees, and customers to move to the center of the lobby and get on the floor. Once there, the armed robber led victims behind the teller counter and into a back room where the Credit Union's safe was located.

Once in the back room, he ordered everyone to their knees at gunpoint and demanded that the bank manager open the safe. The Credit Union manager, fearing for his life, obliged by opening the safe and handing over $195,000 in United States currency.

After the armed robbery, victims dialed 911 to request assistance. When law enforcement arrived, they reviewed surveillance video from the credit union and determined that the armed robber entered the credit union from an area behind a nearby church, held a cellular telephone to his ear when entering the credit union, and ran back towards the church after the robbery. An employee of that church explained to law enforcement that he saw a suspicious individual in a newer model, blue Buick sedan prior to the time of the robbery.

Investigators knew that Google stored location information that could help them apprehend and convict the robber. Google obtains and stores its customers' location information for a wide variety of purposes. Google explains: "From driving directions, to making sure your search results include things near you, to showing you when a restaurant is typically busy, location can make your experiences across Google more relevant and helpful. Location information also helps with some core product functionality, like providing a website in the right language or helping to

keep Google's services secure." How Google Uses Location Information (available at https://policies.google.com/technologies/location-data).

In particular, Federal Bureau of Investigation Task Force Officer Josh Hylton knew that in response to a "GeoFence" warrant, Google could produce location and identity information from accounts associated with electronic devices present in a specified area at a specified time. In one of his previous robbery investigations, an Assistant United States Attorney had reviewed his application for a federal GeoFence search warrant, and he subsequently applied for and obtained a GeoFence warrant in that investigation from a United States Magistrate Judge. In addition, he had previously discussed GeoFence warrants with a Virginia state prosecutor, who had expressed no concerns about their constitutionality.

On June 14, 2019, Task Force Officer Hylton sought and obtained a GeoFence warrant from the Chesterfield Circuit Court of Virginia. 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 and appeared to be speaking with someone. *See* State GeoFence Warrant at 4.[1] The statement then explained why there was reason to believe that Google would have evidence pertaining to the robbery. 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." *Id.* at 5. Magistrate David Bishop issued the GeoFence warrant upon a finding of

[1] The United States will provide a copy of the entire GeoFence search warrant application to the Court in conjunction with this motion.

probable cause. *Id.*

The GeoFence warrant specified a target geographical area, identified as a circle of radius 150 meters around a specific latitude and longitude point near the bank. *See id.* at 3. 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). *See id.* at 2-3. The warrant also authorized disclosure of specified customer identity information associated with these accounts, including user name and email address. *See id.* at 3.

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. *Id.* at 2-3. The warrant directed that in the first step, Google was to disclose location information for devices present in the target area during the hour of the robbery, but not the identity information associated with the devices. *See id.* at 2. 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 identity information. *See id.* at 2-3. In the third step, law enforcement was to identify accounts that remained of interest, and Google was to disclose subscriber identity information for those accounts. *See id.* at 3.

Investigators followed this three-step process when they executed the warrant. In step one, Google produced one hour of location information within the target area for 19 anonymized accounts. In step two, investigators identified nine of those accounts for further disclosure, and Google produced two hours of anonymized location information for those nine accounts. The

anonymized information showed one account of particular interest (hereinafter, the "Chatrie Account"), as it was associated with a device that: (1) was near the church prior to the robbery at the same time that the church witness recalled seeing the suspicious individual; (2) inside the credit union during the robbery; and (3) immediately left the area following the robbery via the area near the church. In step three, law enforcement requested and obtained subscriber information for three accounts, including the Chatrie Account, which belonged to the defendant. This information included the defendant's email address and that he used an Android phone and Google Location History.

As the owner of an Android phone, the defendant had affirmatively opted-in to Google's use and storage of his location information. *See* Google Privacy Policy (available at https://policies.google.com/privacy/archive/20190122) ("You can also turn on Location History if you want to create a private map of where you go with your signed-in devices.").[2] He also had the ability to delete his location history. *See id.* In addition, he agreed to disclose his location information to Google for multiple purposes, including for Google to provide "personalized" services to him (including "content and ads" or "driving directions") and for Google to develop new services. *See id.*

Subsequent investigation provided further evidence that the defendant was the robber. On September 17, 2019, the grand jury returned a two-count Indictment for Forced Accompaniment during an Armed Credit Union Robbery, in violation of 18 U.S.C. § 2113(e), and Brandishing a Firearm During and in Relation to a Crime of Violence, in violation of 18 U.S.C. § 924(c)(1)(A)(i).

[2] Google archives changes over time to its Privacy Policy. *See* https://policies.google.com/privacy/archive. Here, the United States references the Privacy Policy that was in effect from January 22 to October 14, 2019, a period which includes the bank robbery.

The defendant pleaded not guilty on October 1, 2019, and trial was scheduled for December 3, 2019, through December 5, 2019, at 9:00 a.m. before the Honorable M. Hannah Lauck.

On October 29, 2019, the defendant filed the Motion to Suppress that is subject of this response.

II. ARGUMENT

A. The Defendant Had No Reasonable Expectation of Privacy in Two Hours of Google Location Information

As set forth below, the defendant had no reasonable expectation of privacy in any of the information disclosed by Google pursuant to the GeoFence warrant. The defendant argues that he had a reasonable expectation of privacy in his location information under *Carpenter v. United States*, 138 S. Ct. 2206 (2018), but *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*, 138 S. Ct. at 2217 n.3. Here, the United States' acquisition of two hours of the defendant's location information is governed by the long-standing principle that a person has no reasonable expectation of privacy in information disclosed to a third party and then conveyed by the third party to the government.[3]

1. Obtaining Two Hours of the Defendant's Location Information Was Not a Search Under *Carpenter*

The defendant claims based on *Carpenter* that he had a reasonable expectation of privacy in the two hours of location information disclosed by Google, but *Carpenter* does not bear the weight he places on it. In *Carpenter*, the Supreme Court determined that individuals have a

[3] Google also disclosed to the government the defendant's basic subscriber information, including email address, Google Account ID, and Google services used. In *United States v. Bynum*, 604 F.3d 161, 164 (4th Cir. 2010), the Fourth Circuit held that a subscriber has no reasonable expectation of privacy in such information. The defendant does not claim any protected privacy interest in this information.

"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." *Carpenter*, 138 S. Ct. at 2217 & n.3.

The Court emphasized that its decision was "a narrow one." *Carpenter*, 138 S. Ct. at 2220. It 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. *Id.* at 2217 n.3. It also explicitly refused to decide whether obtaining a cell tower dump constituted a Fourth Amendment search. *See id.* at 2220. This limitation is relevant here because tower dump information is similar to the information disclosed pursuant to the GeoFence warrant. A tower dump includes "information on all the devices that connected to a particular cell site during a particular interval." *Id.* Here, the GeoFence warrant sought information on all devices that were within a particular area during a particular interval.

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 defendant's location information pursuant to the GeoFence warrant.

Two hours of location data is only 1/84th of the period that *Carpenter* held constituted a search, and it does not provide the sort of "all-encompassing record of the holder's whereabouts" and "intimate window into a person's life" that concerned the Court. *Carpenter*, 138 S. Ct. at 2217. 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.

The United States is not aware of any judicial opinions addressing whether a GeoFence warrant infringes a reasonable expectation of privacy under *Carpenter*. The Seventh Circuit, however, held that *Carpenter* "does not help" a robber identified via tower dumps. *United States v. Adkinson*, 916 F.3d 605, 611 (7th Cir. 2019). The court explained that *Carpenter* "did not invalidate warrantless tower dumps (which identified phones near one location (the victim stores) at one time (during the robberies))." *Id.* at 611.

The defendant's additional *Carpenter*-related arguments do not establish that the government infringed his reasonable expectation of privacy. He argues that Google's information about its users' location is "more precise than the cell site location information at issue in *Carpenter*," ECF No. 29 at 12, but the Supreme Court in *Carpenter* stated that cell-site information "is rapidly approaching GPS-level precision," and *Carpenter*'s holding "t[ook] account of more sophisticated systems that are already in use or in development." *Carpenter*, 138 S. Ct. at 2218-19. Thus, because the Supreme Court grounded *Carpenter*'s holding in an assumption that cell-site information would approach the precision of GPS, any distinction in precision between them

cannot create enhanced Fourth Amendment protections for GPS information.

The defendant also argues that GeoFence information "Allows Law Enforcement to Retrospectively Locate Individuals in Time and Space," ECF No. 29 at 13, but that fact does not distinguish GeoFence information from a wide variety of other business records, or even from witness testimony. For example, credit card records, landline telephone records, employee time sheets, and IP address records may enable law enforcement to retrospectively locate individuals at particular points in time. However, like the GeoFence information, none of these records provide a comprehensive inventory of the whole of a person's movements, and the government does not infringe the privacy interest protected by *Carpenter* when it obtains them. *See, e.g.*, *United States v. Wellbeloved-Stone*, 777 F. App'x 605, 607 (4th Cir. June 13, 2019) (unpublished) (holding that defendant had no reasonable expectation of privacy in IP address information, even after *Carpenter*).

2. The Defendant Has No Reasonable Expectation of Privacy in Location Information He Disclosed to Google

Because *Carpenter* does not create a reasonable expectation of privacy in two hours of location information, Google's disclosure of that information to the United States is subject to the long-standing principle that an individual retains no reasonable expectation of privacy in information revealed to a third party and then disclosed by the third party to the United States. For decades, the Supreme Court has repeatedly invoked this third-party doctrine in cases ranging from private communications to business records, and this principle applies here to the defendant's location information.

For example, in *Hoffa v. United States*, 385 U.S. 293 (1966), the Court applied the third-party doctrine to incriminating statements made in the presence of an informant. The Court held that the Fourth Amendment did not protect "a wrongdoer's misplaced belief that a person to whom

he voluntarily confides his wrongdoing will not reveal it." *Id.* at 302. A decade later the Supreme Court rejected a Fourth Amendment challenge to a subpoena for bank records in *United States v. Miller*, 425 U.S. 435 (1976). The Court held "that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, 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." *Id.* at 443. *See also SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984) (applying the third-party doctrine to financial records in the hands of a third-party).

The Supreme Court also relied on this principle in *Smith v. Maryland*, 442 U.S. 735 (1979), when it held that a telephone user had no reasonable expectation of privacy in dialed telephone number information. First, the Court stated that "we doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed." *Id.* at 742. In addition, the Supreme Court further held that even if the defendant had a subjective expectation of privacy in his dialed telephone numbers, "this expectation is not one that society is prepared to recognize as reasonable." *Id.* at 743 (internal quotation marks omitted). The Court explained that the user "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business." *Id.* at 743-44.

The defendant therefore had no reasonable expectation of privacy in Google's records of his location because he voluntarily conveyed his location to Google in exchange for receiving the benefits of Google services. Because Google location service is an opt-in service, the defendant had previously taken an affirmative step to disclose his location information to Google. Moreover,

he agreed that Google would have access to his location information for purposes ranging from providing him with targeted advertising or assistance with driving directions to Google's development of new services. *See* Google Privacy Policy (available at https://policies.google.com/privacy/archive/20190122). These facts demonstrate that the defendant voluntarily disclosed his location information to Google, and the United States did not infringe his reasonable expectation of privacy when it obtained from Google information about his device's location during a two-hour interval.

Finally, the fact that the defendant voluntarily disclosed his location information to Google is confirmed by the reasoning of *Carpenter*. *Carpenter* concluded that cell-site information was not voluntarily disclosed to the phone company for two reasons, neither applicable here. First, the Court held that carrying a cell phone "is indispensable to participation in modern society." *Carpenter*, 138 S. Ct. at 2220. In contrast, although Google services are frequently helpful and convenient, most may be used without turning on Google location services, and using Google services with location enabled is not essential to participation in modern society. Google location services are no more indispensable than having a bank account or making a phone call, and bank records and dialed telephone number information remain unprotected by the Fourth Amendment under *Miller* and *Smith*. Second, *Carpenter* held that cell-site information is collected "without any affirmative act on the part of the user beyond powering up" and that "there is no way to avoid leaving behind a trail of location data." *Id.* In contrast, in order for Google to have his location information, the defendant had to affirmatively opt in, and he also retained the ability to delete his information. Finally, a cell phone user's disclosure of location information to the phone company is merely incidental to receiving communication service from the company, but a device owner's disclosure of location information to Google is the central prerequisite to obtaining Google

location services. The defendant thus voluntarily disclosed his location information to Google, and Google's disclosure of that information to the government did not infringe upon his reasonable expectation of privacy.

The defendant also asserts that the GeoFence warrant intruded on the reasonable expectation of privacy of others, ECF No. 29 at 13, but this argument fails for two separate reasons. First, 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)). The defendant therefore lacks standing to challenge the government's acquisition of others' location information. *See, e.g.*, *United States v. Patrick*, 842 F.3d 540, 545 (7th Cir. 2016) (rejecting defendant's argument that investigator's use of a cell-site simulator violated the privacy rights of third parties, because the defendant was "not entitled to invoke the rights of anyone else; suppression is proper only if the defendant's own rights have been violated"). Second, these other individuals also voluntarily disclosed their location information to Google. Google's disclosure of their location information therefore did not infringe their Fourth Amendment rights either.

Finally, the defendant claims that obtaining his information from Google constitutes a search under "a property-based theory of the Fourth Amendment." ECF No. 29 at 14. This argument is rooted in Justice Gorsuch's solo dissent in *Carpenter*, where he discussed a transformation of the Fourth Amendment that would jettison not only *Smith* and *Miller*, but also the reasonable expectation of privacy test of *Katz v. United States*, 389 U.S. 347 (1967). *See Carpenter*, 138 S. Ct. at 2262-72 (Gorsuch, J., dissenting). Ultimately, Justice Gorsuch concluded that *Carpenter* forfeited this new argument because he did not raise it below. *See id.* at 2272. Regardless, a solo dissent is not the law, and *Smith*, *Miller*, and *Katz* remain binding on this Court.

Under existing law, Google's disclosure of location information to the government did not infringe upon any reasonable expectation of privacy.

B. The GeoFence Warrant Satisfied the Fourth Amendment

The GeoFence warrant did not remotely resemble a general warrant. A general warrant "specified only an offense—typically seditious libel—and left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched." *Steagald v. United States*, 451 U.S. 204, 220 (1981). In contrast, the GeoFence warrant authorized the government to obtain from Google limited and specified information directly tied to a particular robbery at a particular place and time. As set forth below, because the warrant was supported by probable cause and specified its object with particularity, the defendant's argument that the warrant was a general warrant is without merit. *See* ECF No. 29 at 16-24.

More broadly, the facts of this case illustrate why a warrant that requires disclosure of information about devices in a particular place at a particular time is neither a general warrant nor, as the defendant asserts, "repugnant to the Constitution." ECF No. 29 at 16. When law enforcement officers sought the warrant, they were investigating a serious violent crime, and they had reason to believe that the perpetrator was reasonably likely to commit other similar offenses if not identified and apprehended. The GeoFence warrant allowed them to solve the crime and protect the public by examining a remarkably 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. Rather than being "repugnant to the Constitution," this investigative technique involved no unreasonable search or seizure and should be encouraged, not condemned.

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 warrant established an ample basis for the issuing magistrate's finding of probable cause. First, it established that an unknown subject committed an armed bank robbery at a particular place and time. *See* State GeoFence Warrant at 4. Second, it established that at the bank prior to the robbery, the robber held the cell phone to his ear and appeared to be speaking with someone. *See id.* Third, the affidavit established that even as of 2013, the majority of cell phones were smartphones. *See id.* at 5. Fourth, it established a connection between smartphones and Google location information. It explained 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. *Id.* It also explained 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." *Id.* From this information, there was a substantial basis for the magistrate to find probable cause to believe that Google possessed evidence related to the robbery.

The defendant objects that there was no probable cause to believe that the bank was robbed by a Google user, *see* ECF No. 29 at 23, but his argument ignores that the probable cause standard requires only a fair probability that evidence will be found at the place searched. The defendant posits a situation in which Google would not have had the robber's location information—"[i]f the robber had an iPhone and did not use Google services"—but he does not dispute that it was likely that Google would have information regarding Android users or that it would have information regarding some non-Android users. ECF No. 29 at 23. The magistrate therefore had a substantial basis for his finding of probable cause.

The United States is unaware of any decisions addressing Fourth Amendment challenges to GeoFence warrants, but one district court recently rejected a similar challenge to cell tower dump warrants. In *United States v. James*, No. 18-cr-216, 2019 WL 325231 (D. Minn. Jan. 25, 2019), 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.* Here, where the robber used his phone just before the robbery, the basis for the magistrate's finding of probable cause was at least as strong as in *James*.

Furthermore, the probable cause established by the affidavit supported obtaining Google information for evidentiary purposes other than identifying the robber directly. As the affidavit explained, location information from Google could also "identify potential witnesses" and "assist investigators in forming a fuller geospatial understanding and timeline" of the robbery. State GeoFence Warrant at 5. The warrant appropriately sought such information, as a search warrant

may be issued to obtain evidence to "aid in a particular apprehension or conviction." *Warden v. Hayden*, 387 U.S. 294, 307 (1967).

Messerschmidt v. Millender, 565 U.S. 535 (2012), demonstrates that the Supreme Court does not narrowly construe 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.

Similarly, the issuing magistrate here had multiple reasons to believe that the location information for those present at the robbery would constitute 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 the robber and 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 defendant is correct that proximity to criminals does not alone give rise to probable cause that he committed a crime, *see* ECF No. 29 at 21, here probable cause existed for the location information sought by the warrant. The issuing magistrate had a substantial basis for finding

probable cause to believe that Google possessed location information regarding the scene of the robbery, and this Court should therefore deny the defendant's motion to suppress.

Finally, the defendant repeatedly emphasizes that the GeoFence warrant collected information about persons not suspected of criminal activity, but this fact does not aid his Fourth Amendment argument. The Supreme Court has held that "it is untenable to conclude that property may not be searched unless its occupant is reasonably suspected of crime." *Zurcher v. Stanford Daily*, 436 U.S. 547, 559 (1978). Instead, a search warrant "may be issued when it is satisfactorily demonstrated to the magistrate that fruits, instrumentalities, or evidence of crime is located on the premises." *Id.*[4]

2. The GeoFence Warrant 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). The particularity requirement constrains a warrant so that it is "no broader than the probable cause on which it is based." *United States v. Hurwitz*, 459 F.3d 463, 473 (4th Cir. 2006). It protects against "exploratory rummaging in a person's belongings." *United States v. Williams*, 592 F.3d 511, 519 (4th Cir. 2010) (quoting *Andresen v. Maryland*, 427 U.S. 463, 480 (1976)). Moreover, the test for particularity "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

[4] *Zurcher*, which approved a warrant to search an innocent newspaper for evidence of crime, also demonstrates that the Fourth Amendment standards of probable cause and particularity govern warrants that raise significant First Amendment concerns. *See id.* at 565 ("courts apply the warrant requirements with particular exactitude when First Amendment interests would be endangered by the search"). Here, the defendant cannot demand any exacting scrutiny of the GeoFence warrant merely because he robbed a bank near a church, because Fourth Amendment rights may not be vicariously asserted. *See Rakas*, 439 U.S. at 133-34. In any event, the GeoFence warrant satisfied the Fourth Amendment under the standards of *Zurcher* because it was issued based on probable cause and specified its objects with particularity.

743, 745 (8th Cir. 1976)).

Here, the GeoFence warrant 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 interval. 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 robber.

The cell tower dump opinion *United States v. James* provides persuasive authority that the warrant here was sufficiently particular. In *James*, the defendant argued that the tower dump warrants used to identify him as a robber were insufficiently particular 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 were sufficiently particular 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, rather than hundreds or thousands.

The defendant also challenges the warrant because it included the three-step process for executing the warrant that allowed investigators to obtain less than the maximum quantity of location and identity information that the warrant authorized. *See* ECF No. 29 at 24 ("The warrant left everything up to the discretion of the executing officers."). 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 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. Rather than violating the Fourth Amendment, the three-step process allowed investigators to further protect privacy.

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

[5] 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 III 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).

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. The GeoFence warrant was not a general warrant, and this Court should deny the defendant's motion to suppress.

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. 19, 2014) (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.[6] Importantly, first-step information alone was sufficient for investigators to recognize that the Chatrie Account likely belonged to the robber: the defendant's electronic device was near the church prior to the robbery, inside the credit union during the robbery, and left immediately following the robbery via the area near the church. 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.

C. Evidence from the GeoFence Warrant Should Not Be Suppressed Because Investigators Relied upon 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 are no judicial opinions analyzing them under the Fourth Amendment. In *McLamb*, the Fourth Circuit rejected suppression in this circumstance. The court

[6] 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.

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, Task Force Officer Hylton followed the approach endorsed by *McLamb*. He had consulted with prosecutors—both state and federal—about GeoFence warrants, and he had previously obtained a similar warrant for Google location information issued by a United States Magistrate Judge. In this investigation, he then sought and obtained a search warrant from a state magistrate. Task Force Officer Hylton thus did "precisely" what *McLamb* expects, and the good-faith exception precludes suppression here.

Alternatively, the traditional good-faith analysis of *United States v. Leon*, 468 U.S. 897 (1984), leads to the same result: no suppression. 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, and the defendant does not claim that the affiant misled the magistrate or that the magistrate abandoned his judicial role.

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* ECF No. 29 at 24-25, 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*, 565 U.S. at 547). The defendant asserts that there was "no evidence that the robber had ever used Google," ECF No. 29 at 24-25, but he ignores that the affidavit established that the armed 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. 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* ECF No. 29 at 24. But as discussed in Section II.B above, the warrant was quite specific in scope: it was limited to anonymized location information over a two-hour interval, as well as accompanying identity information for a smaller subset, for individuals present at the site of the robbery during a one-hour interval.

In addition, the defendant argues that the warrant was facially deficient because it allowed officers to choose to obtain less information about those present at the robbery, *see* ECF No. 29 at 25, but this argument is foreclosed by *McLamb*. 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. The warrant thus was not facially deficient, and this Court should deny the defendant's motion to suppress.

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,

G. ZACHARY TERWILLIGER
United States Attorney

By: /s/

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

Nathan Judish
Senior Counsel, Computer Crime and
Intellectual Property Section
Criminal Division
United States Department of Justice

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 19th day of November, 2019, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send an electronic notification of such filing to the following:

Laura Koenig
Office of the Federal Public Defender (Richmond)
701 E Broad Street
Suite 3600
Richmond, VA 23219
Email: Laura_Koenig@fd.org

Paul Geoffrey Gill
Office of the Federal Public Defender (Richmond)
701 E Broad Street
Suite 3600
Richmond, VA 23219
Email: paul_gill@fd.org

Michael William Price
National Association of Criminal Defense Lawyers
1660 L Street NW
12th Floor
Washington, DC 20036
(202) 465-7615
Email: mprice@nacdl.org
PRO HAC VICE

_____/s/_____
Kenneth R. Simon, Jr.
Assistant United States Attorney
Office of the United States Attorney
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	)	

DEFENDANT'S REPLY TO GOVERNMENT'S RESPONSE MOTION TO SUPPRESS EVIDENCE OBTAINED FROM A "GEOFENCE" GENERAL WARRANT

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. 29.

I. Obtaining Mr. Chatrie's Google location information was a search.

Mr. Chatrie presents two arguments as to why the government's acquisition of his Google location data was a search. The government responds to only one of them on the merits. First, Mr. Chatrie argues that the government's conduct was a search under the *Katz* reasonable expectation of privacy test. The government contends that he had no privacy interest in two hours of his location information, failing to appreciate the significance of the Supreme Court's landmark decision in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), and seeking to create a *de minimis* exception to the Fourth Amendment. Second, Mr. Chatrie argues that it was a search under a property rights theory of the Fourth Amendment. 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); *Kyllo v. United States*, 533 U.S. 27, 37 (2001); *Soldal v. Cook County*, 506 U.S. 56, 62 (1992). The government, however, brushes it aside as if it were a recent invention of Justice

Gorsuch, offering no response on the merits. ECF No. 41 at 12. Under both theories, however, the acquisition of Mr. Chatrie's Google location data was a search.

A. Obtaining Mr. Chatrie's Google location information infringed on his reasonable expectation of privacy.

The government contends that Mr. Chatrie had "no reasonable expectation of privacy in any of the information disclosed by Google" because the location data covered two hours instead of seven days. ECF No. 41 at 6. But *Carpenter* did not gift the government a free pass from the Fourth Amendment for any such "limited period." 138 S. Ct. at 2220. On the contrary, the Court made it clear that it would not "grant the state unrestricted access to a wireless carrier's database of physical location information," describing such information as "deeply revealing," "comprehensive," and "inescapable" *Id.* at 2223. Mr. Chatrie had a reasonable expectation of privacy in his Google location information, which was at least as private as the records in *Carpenter*.

Carpenter involved two orders for historical cell site location information ("CSLI"): one seeking 152 days, and a second for seven days. 138 S. Ct. at 2212. In holding that a warrant is required for seven days or more of CSLI, the Court merely decided *Carpenter* on the facts before it. There is no higher constitutional significance to seven days, and *Carpenter* does not suggest that the Fourth Amendment would condone warrantless searches for a shorter period of time. In fact, the second CSLI order only produced only two days of records, not seven. *Id.* at 2212. Likewise, the Court did not express a view on real-time CSLI or "tower dumps" because those facts were not present in the record. *Id.* at 2220. But it would require misreading the rest of the Court's opinion to view this judicial restraint as an invitation to engage in warrantless surveillance. It is not enough to suppose, as the government does, that it might be possible to replicate this

location information given enough time and resources.[1] ECF No. 41 at 8. While some physical searches may be permissible without a warrant, the Court has been clear that "any extension of that reasoning to digital data has to rest on its own bottom." *Riley v. California*, 134 S. Ct. 2473, 2489 (2014).

Applying the *Carpenter* framework, it is clear that obtaining Google location data was a search that infringed on Mr. Chatrie's reasonable expectation of privacy. Like the CSLI in *Carpenter*, Google location information is deeply revealing, comprehensive, and inescapable. 138 S. Ct. at 2223. It its revealing because it can expose the location of devices inside constitutionally protected areas, including "private residences, doctor's offices, political headquarters, and other potentially revealing locales." *Id.* at 2218. Indeed, Google uses it for that very purpose when serving advertisements. Google Policies, Location Data (Nov. 20, 2018), https://policies.google.com/technologies/location-data?hl=en. And in this case, it located 11 users inside the Journey Christian Church, a quintessentially protected space that raises additional First Amendment concerns. *See Stanford v. Texas*, 379 U.S. 476, 485 (1965) (requiring courts to apply Fourth Amendment requirements with "the most scrupulous exactitude" when searches implicate First Amendment concerns).[2] In sum, two hours of Google location information is capable of revealing the same type of sensitive, private information as CLSI.

[1] Mr. Chatrie maintains that the data obtained through this warrant could not have been obtained through visual surveillance alone. In addition to subscriber information and account details, which are not observable, it would have been impossible to reconstruct all of the location data obtained from Google. Even if the government had unlimited time and resources, they would not be free to enter constitutionally protected spaces to log the devices located inside. Mr. Chatrie does not concede his privacy interest in the non-location data obtained through the geofence warrant.

[2] The government fails to adequately address these First Amendment concerns, just as it failed to recognize or address them when seeking a geofence warrant that fully encompassed a large church. The affiant simply described the church as "an adjacent business" without telling the Court that the "business" was actually a church.

The fact that the government obtained a smaller quantity of this location data than in *Carpenter* does not diminish its potentially revealing nature. *Carpenter* emphasized the long-term privacy implications of cell phone location tracking only because those were the facts before the Court. Elsewhere, the Justices have expressed concern with even short-term monitoring. In *United States v. Karo*, for example, the use of a beeper to track a drum of ether inside a private residence was sufficient to trigger Fourth Amendment scrutiny. 468 U.S. 705, 716 (1984) ("We cannot accept the Government's contention that it should be completely free from the constraints of the Fourth Amendment to determine by means of an electronic device . . . whether a particular article—or a person, for that matter—is in an individual's home *at a particular time*.") (emphasis added). Just a small window of GPS monitoring still creates a "precise, comprehensive record of a person's movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring). Indeed, it takes little imagination to conjure the privacy implications of even a single trip to "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." *Id.* (quoting *People v. Weaver*, 12 N.Y.3d 433, 441-442 (2009)).

Far more troubling is the breadth of the search in this case. Whereas *Carpenter* concerned the search of just one person's location data, the geofence warrant authorized the search of an unlimited number of people's location data. Neither the government nor the magistrate knew in advance how many devices would be swept up as a result of the search. Indeed, the fact that it would yield information about 19 different devices was unknowable at the time of the government's application. This was not a problem the *Carpenter* Court had occasion to consider,

but it is one that has repeatedly troubled the Court.[3] Indeed, "dragnet" searches are a perennial Fourth Amendment fear. That is why the Constitution prohibits general warrants and requires both probable cause and sufficient particularity. Even if obtaining two hours of location data for a single person would not trouble the Court, obtaining two hours of data for every person in an area is a very different story. In this sense, it arouses the same fears of "too permeating police surveillance" and exercise of "arbitrary power" that motivated the *Carpenter* Court. 138 S. Ct. at 2214. Although the concerns in *Carpenter* are not identical, the potentially unlimited breadth of a geofence search makes up for the comparatively shorter duration of a geofence search. Consequently, the data obtained are highly revealing and deserving of Fourth Amendment protection, as much if not more so than the CSLI in *Carpenter*.

Similarly, Google location data has a comprehensive reach that is comparable to CSLI. In fact, CSLI *is* one of the data sources that Google collects and uses to determine users' locations. But Google also includes GPS location data as well as "additional information from nearby Wi-Fi, mobile networks, and device sensors." Google Policies, *supra*. As a result, Google location information is significantly more precise than CSLI alone. The government puts no stock in this distinction because the *Carpenter* Court "t[ook] account of more sophisticated systems" and recognized that CSLI "is rapidly approaching GPS-level precision." [G. at 8-9 (quoting *Carpenter*, 138 S. C.t at 2218-19).] But because Google uses multiple sources of location data, it locates devices even in places where GPS is unavailable or unreliable, such as indoors. If GPS data is not

[3] *See, e.g.*, *United States v. Knotts*, 460 U.S. 276, 284 (1983) (reserving the question of whether "different constitutional principles may be applicable" to "dragnet-type law enforcement practices"); *see also Jones*, 565 U.S. at 408 n.6 (quoting *Knotts*); *Karo*, 468 U.S. at 716 ("Indiscriminate 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."); *United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div.*, 407 U.S. 297, 327 (1972) (Douglas, J., concurring) ("[T]he recurring desire of reigning officials to employ dragnet techniques … lies at the core of [the Fourth Amendment]."); *Davis v. Mississippi*, 394 U.S. 721, 726 (1969) ("Nothing is more clear than that the Fourth Amendment was meant to prevent wholesale intrusions upon the personal security of our citizenry").

available, Google will then approximate location information based on the signal strength of known nearby Wi-Fi networks, which have a short range. Google is capable of doing this by referencing the billions of data points it gathers each day from other Android phones that report on the availability of Wi-Fi networks in range. *See* Tr. at 29, *Commonwealth v. Anderson*, No. CR17-4909-00F (Va. Cir. Ct., Jan. 4, 2019) (Ex. D). Only when Wi-Fi and GPS are unavailable does Google fall back to using CSLI, the least precise method. Consequently, Google location data is likely to be *more* comprehensive than GPS, locating devices where GPS is unavailable.

And finally, Google location data is "automatic and inescapable." For Android users like Mr. Chatrie, there is no practical way to avoid transmitting location information to Google, even if "Location History" is turned off. Location History only controls whether location data gets added to a user's "Timeline" feature, not whether Google sees or stores the data. Likewise, disabling Google Location Services does not actually stop a device from determining its location and creating a record. As Google explains, "Your device's location will continue to work even if GLS [Google Location Services] is turned off, but the device will rely only on GPS to estimate device location for apps with the necessary permission." Google Policies, *supra*. Those apps include basic, built-in Google services like Search and Maps. Thus, because "Google Location Services is distinct from your device's location setting," some location information still flows to Google even when it is off. *See* Ryan Nakashima, *Google Tracks Your Movements, Like it or Not*, Associated Press (Aug. 13, 2018), https://www.apnews.com/828aefab64d4411bac257a07c1af0ecb. And while Google notes that there are separate controls for "Web & App Activity," this setting is isolated and unaffected by the restriction of other location information. Furthermore, the government is incorrect that Mr. Chatrie "had to affirmatively opt in" to sharing his location information with Google. As the user of an Android phone, Google Location Services is enabled

by default. *See* Verizon, Samsung Galaxy S9 / S9+ - Activate / Set Up Device, https://www.verizonwireless.com/support/knowledge-base-216675/ (showing Google location services on by default at step eight). Location History, by contrast, is an opt-in feature, but one that has no effect on the GPS, Wi-Fi, and other location data transmitted to Google through Location Services or Web & App Activity.[4] While it is technically possible to disable the phone's location functions altogether by activating "airplane mode" or powering off the device completely, such drastic steps are not required by *Carpenter*. 138 S. Ct. at 2220 ("Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily 'assume[] the risk' of turning over a comprehensive dossier of his physical movements."). Rather, collection of Google location data is "inescapable" because, as in *Carpenter*, it relates to services one needs to be a functioning member of today's society. *Id*. In addition the ubiquity of Google services such as Search, Maps, and Mail, all Android phones—such as the one Mr. Chatrie had—run on Google's operating system and regularly transmit location data back to Google without any affirmative user action at all. The collection is therefore just as automatic and inescapable as CSLI.

In sum, Google location data is at least as revealing, comprehensive, and inescapable as CSLI. Thus, as in *Carpenter*, the fact that "such records are generated for commercial purposes . . . does not negate [Mr. Chatrie's] anticipation of privacy in his physical location." 138 S. Ct. at 2217. Mr. Chatrie had a reasonable expectation of privacy in his Google location data and obtaining those records was therefore a Fourth Amendment search. This is especially true because

[4] The government also draws a confusing and unsupported distinction between "incidental" disclosure of location information and disclosure as a "central prerequisite" to obtaining services. CSLI, however, is in fact essential to the use of a cell phone – required to route information to the correct tower and device. It is both central to the way cell phones function and a prerequisite to using their features.

of the "dragnet-style" search used to get them, a longstanding fear of the Court even when long-term surveillance is not at issue.

B. Obtaining Mr. Chatrie's Google location information infringed on his property rights in that data.

The *Katz* reasonable-expectation-of-privacy test has been in place since 1967, but the Supreme Court's Fourth Amendment jurisprudence is not so young. Throughout the late-19th and early-20th centuries, the Court hued closely to a literal reading of the constitutional text, focusing on the property rights attached to "persons, houses, papers, and effects." U.S. Const. amnd. IV; *see, e.g., Agnello v. United States*, 269 U.S. 20, 32 (1925) ("The search of a private dwelling without a warrant is in itself unreasonable and abhorrent to our laws."); *Weeks v. United States*, 232 U.S. 383, 391 (1914) (recognizing that the essence of a Fourth Amendment violation is "the invasion of his indefeasible right of personal security, personal liberty, and private property."); *Ex parte Jackson*, 96 U.S. 727, 732-33 (1878) (holding that postal mail is just as protected under the Fourth Amendment as those papers and effects kept in the safety of one's home). Indeed, the invasion of property rights was at the heart of Lord Camden's judgment in *Entick v. Carrington*, one of the pillars of English liberty and a catalyst for the Fourth Amendment. 19 How. St. Tr. 1029 (K.B. 1765) ("Papers are the owner's goods and chattels. They are his dearest property; and are so far from enduring a seizure, that they will hardly bear an inspection"); *see also Boyd v. United States*, 116 U.S. 616, 626 (1886) (describing *Entick* as a "monument of English freedom" and "the true and ultimate expression of constitutional law"). On this side of the Atlantic, the founding fathers specifically designed the Fourth Amendment to assure security "in person *and property*" against unlawful searches. *Adams v. New York*, 192 U.S. 585, 598 (1904) (emphasis added). In short, the "traditional," property-based theory of the Fourth Amendment has a pedigree that long predates *Katz* and, given the Court's recent jurisprudence, is as valid as ever.

When the Court decided *Katz*, there was a palpable worry that property rights alone would not be sufficient to implement the Fourth Amendment in an age when communications could occur without an in-person meeting, but through electronic whispers miles apart. Justice Harlan embodied this concern in his famous concurrence, declaring that the Fourth Amendment protects "people, not places." 389 U.S. at 351. This understanding of the Fourth Amendment has served the Court well for decades, but it "did not repudiate [the] understanding" held for "most of our history" that the Fourth Amendment embodies "a particular concern for government trespass" on one's "papers" and "effects." *Jones*, 565 U.S. at 406-07.

Thus, for example, the Court in *Soldal* unanimously held that removal of a tenant's mobile home was a Fourth Amendment seizure even though the owner's "privacy" was not invaded. 506 U.S. at 62 ("[O]ur cases unmistakably hold that the Amendment protects property as well as privacy."). Likewise, in *Kyllo*, Justice Scalia avoided the *Katz* doctrine in finding that the use of a thermal imager on a home was a search. 533 U.S. at 37 ("The Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained."). Indeed, the *Kyllo* Court noted that "well into the 20th century, our Fourth Amendment jurisprudence was tied to common-law trespass." *Id.* at 40. And finally, in *Jones*, the opinion of the Court rested on trespass grounds. 565 U.S. at 404-05. The *Jones* Court found that placement of a GPS tracker on a car was a "physical intrusion" that "would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted." *Id*. Reaffirming *Soldal*, the *Jones* Court unequivocally stated that "the *Katz* reasonable-expectation-of-privacy test had been *added to*, not *substituted for*, the common-law trespassory test." *Id.* at 409; *see also Jones*, 565 U.S. at 414 (Sotomayor, J., concurring) ("*Katz*'s reasonable-expectation-of-privacy test augmented, but did not displace or diminish, the common-law trespassory test that preceded it.").

Justice Gorsuch's dissent in *Carpenter* was a clarion call for courts and counsel to reassert the central role that property rights have played in the history of Fourth Amendment jurisprudence. 138 S. Ct. at 2272 ("Carpenter pursued only a *Katz* 'reasonable expectations' argument. He did not invoke the law of property or any analogies to the common law, … [and therefore] forfeited perhaps his most promising line of argument."). Mr. Chatrie does not ask this Court to adopt a novel theory, but to apply a deep-rooted one. *See id.* at 406-07. Mr. Chatrie takes Justice Gorsuch's warning seriously and seeks to fully assert his Fourth Amendment rights. The government, however, simply does not engage with the merits of Mr. Chatrie's property-based argument. ECF No. 41 at 12-13. Instead, the government chooses to ignore over a century of Fourth Amendment jurisprudence and merely quip that "a solo dissent is not the law." *Id.* at 12.

II. The warrant lacked probable cause and was even more unparticularized than previously thought.

The government responds that the geofence warrant was supported by sufficient probable cause and particularity. *Id.* at 13-21. But their arguments are even less persuasive in light of additional discovery showing that they twice requested additional location data on all 19 devices initially identified by Google, in contravention of the warrant itself. *See* Ex. A (First Step 2 Request) at 1; Ex. B (Second Step 2 Request) at 1. Indeed, Google twice rebuffed this request, ultimately sending additional information on nine devices. This development underscores why such an ad hoc, back-and-forth negotiation with the recipient of a warrant is no substitute for judicial oversight and a particularized warrant supported by probable cause.

More fundamentally, the government's response appears to misunderstand the significance of the Fourth Amendment's particularity requirement. Particularity is not just about how clearly a warrant identifies the object of a search for which there is probable cause to seize, but whether it adequately constrains law enforcement's discretion in the execution of that search and seizure. Its

basic purpose is to prevent general warrants by ensuring that "nothing is left to the discretion of the officer executing the warrant." *Marron v. United States*, 275 U.S. 192, 196 (1927). The government contends that the information it sought was "constrained" based on location, date, and time to the robbery under investigation. ECF No. 41 at 18. But it is not enough to simply name the crime and identify the general area where it occurred. Rather, such a warrant is more akin to the general warrant in *Wilkes v. Wood* that identified the crime of seditious libel but did not specify the places to be searched, the papers to be seized, or the persons to arrest. 98 Eng. Rep. 489, 490 (1763). Drawing a circle around the neighborhood to be ransacked does not change the analysis.

The government contends that the initial search ("Step One") satisfied the particularity and probable cause requirements because it specified information "directly tied" to a particular robbery, which of course occurred "at a particular place and time." ECF No. 41 at 13. But it failed to individualize its suspicion and tie that robbery to a particular account or accounts to be searched. That is like permitting the police to search for stolen goods in any place near a theft, to pat down every person in a bar where a crime had been committed, or to search every person in an apartment where illegal drugs may be present--all of which courts have found to be unconstitutional. *See Grumon v. Raymond,* 1 Conn. 40, 43 (1814); *United States v. Glenn, 2009 WL 2390353*, at *5 (S.D. Ga. 2009); *Commonwealth v. Brown*, 68 Mass. App. Ct. 261, 262 (Mass. App. Ct. 2007). It is also strongly reminiscent of the facts in *United States v. Curry*, in which this Court held that police did not have reasonable suspicion to stop Mr. Curry or any of the other men in a group after shots were fired in the general vicinity of where he was walking. No. 3:17CR130, 2018 WL 1384298, at *11 (E.D. Va. Mar. 19, 2018), *rev'd and remanded*, 937 F.3d 363 (4th Cir. 2019), *reh'g en banc granted,* No. 18-4233, 2019 WL 6133704 (4th Cir. Nov. 18, 2019) ("[G]eneralized suspicion and fear cannot substitute for specific and articulable facts . . . that support a

particularized and objective basis for suspecting *the particular person stopped* of criminal activity.") (internal quotations omitted). The government scoffs at the fact that "19 individuals, rather than hundreds or thousands" were affected by Step One of the warrant, ECF No. 41 at 18, but it gives no indication of how many bystanders would have to be searched before the collateral damage becomes too much for the Fourth Amendment to bear. Indeed, the government did not and could not have known how many devices would be affected by such a high-tech fishing expedition. The only thing certain at Step One was that law enforcement intended to search the Google data of many people who were *not* involved in the robbery.

It is not sufficient to respond, as the government does, that the location records of admittedly innocent people are the proper target of a search warrant on the off-chance that they might be useful in reconstructing the scene, identifying potential witnesses, or rebutting potential defenses raised by the robber. ECF No. 41 at 16. This argument proves too much. The issue is not whether there is some evidence to be had, but where the line is between a general warrant and a particularized one. The boilerplate speculation offered by the government would seemingly justify a search of anyone near any crime.

Moreover, the underlying reason the warrant lacks particularity is because the government does not have probable cause to search an unlimited number of unknown people who were near a crime. Probable cause is what makes particularity possible. Without it, there should be no surprise when a warrant also lacks particularity. As the government notes, the "information specified by a warrant must be 'no broader than the probable cause on which it is based.'" ECF No. 41 at 19 (citing *United States v. Hurwitz*, 459 F.3d 463, 473 (4th Cir. 2006)). But here, the distinguishing feature of the warrant application is the absence of any identifiable suspects. Without some

individualized suspicion, it is trying to imagine how the resulting warrant would be anything other than unparticularized.

Contrary to the government's assertion, the warrant application established no probable cause for any of the Google data it obtained. Mere proximity to crime is not probable cause of criminal activity. The government points to the so-called "Playpen warrant" as precedent for its actions here, *Id.* at 20, but unlike the Playpen cases, there was no honeypot in this case—only a dragnet. The Playpen warrant was "based on probable cause to search any computer logging into [a child pornography website]." *Id.* at 20 (quoting *United States v. Matish*, 193 F. Supp. 3d 585, 609 (E.D. Va. 2016)). The suspicion generated as a result of logging in to such a website has been a critical element in decisions upholding that warrant's constitutionality. See, e.g., *Matish*, 193 F. Supp. 3d at 603 (finding that the "chances of someone innocently discovering, registering for, and entering Playpen were slim" because of the "numerous affirmative steps that one must take to even find Playpen on the Tor network" that make it "extremely unlikely for someone to stumble innocently upon Playpen"); *see also United States v. McLamb*, 880 F.3d 685, 688 (4th Cir. 2018) (noting that to access Playpen, a user must download Tor and enter a 16-character URL consisting of random letters and numbers, as well as enter a username and password to proceed past a welcome page that "was suggestive enough that Playpen's content would be apparent" to any visitor). In this case, however, there is no argument that using Google services or being near the Call Federal Credit Union is somehow inherently suspicious. Instead, a crime was committed, law enforcement had no suspects, and the government simply cast a dragnet. The prevalence of Android phones is not probable cause to search any Google users that happen to be nearby. And

the absence of any individualized suspicion, let alone probable cause, at Step One renders the entire warrant unconstitutional.[5]

The second phase of the warrant ("Step Two") fares even worse. The government asserts that the warrant was "remarkably limited" because it obtained the location information for nine individuals over a two-hour interval, regardless of whether they were inside or outside the 150-meter radius. ECF No. 41 at 13. Indeed, the government commends itself for seizing "less than the maximum quantity of location and identity information that the warrant authorized." ECF No. 41 at 18. But this argument only gives lie to the entire three-step process. According to the government, the warrant authorized the government to seize "identity information and two hours of location data for *all individuals* present at the site of the robbery during the hour of the robbery." *Id.* at 19 (emphasis added). The warrant, however, is not so clear on this point.

The impression one gets from reading the warrant application is that the three-step process matters—that it is a means of protecting the privacy of bystanders by using "anonymized"[6] data to "narrow down the list" before obtaining additional records in Step Two, and then de-anonymized identity information in the third phase ("Step Three"). But the government, in its requests to Google and in a careful reading of Attachment II, said that they were actually entitled to Step 2 and Step 3 data on *everyone* snared in Step 1, no narrowing required. The warrant only says that law enforcement will "attempt" to narrow the list in Steps 2 and 3. *See* Warrant

[5] The government invites this Court to "sever the second step of the warrant and to suppress second-step information" only, ECF No. 41 at 20, but to do so would condone the digital equivalent of a general warrant that lacked particularity from the outset. *See, e.g., United States v. Sells*, 463 F.3d 1148, 1158 (10th Cir. 2006) (noting that "every court to adopt the severance doctrine has further limited its application to prohibit severance from saving a warrant that has been rendered a general warrant by nature of its invalid portions despite containing some valid portion").
[6] Mr. Chatrie does not concede that this data is not personally identifiable.

Attachment I at 1-2; Warrant Attachment II at 2-3. The verb "attempt" appears six times, doing quite a lot of work.

The government did in fact request the "maximum" amount of data—twice. In two emails to Google following the production of Stage One records, the government asked for "additional location data and subscriber info" for all 19 devices identified in step one. *See* Ex. A at 1; Ex. B at 1. Google did not respond to either of these requests. It was not until the government sent a third email requesting additional data on just nine devices that Google produced more records. *See* Ex. C (Third Step 2 Request) at 1. This is not to suggest that the government did not "attempt" to narrow down the list. Indeed, the government twice tells Google, "If this request seems unreasonable, please keep in mind that device numbers 1-9 may fit the more likely profile of parties involved," but then requested additional information on all 19 anyway. *See* Ex. A at 1; Ex. B at 1.

It is unclear whether the practical realties of the three-step process were apparent to the issuing magistrate. It was certainly not clear to Mr. Chatrie prior to reviewing the negotiations between Google and law enforcement over the data to be produced in Step Two. The critical point, however, is that it was up to Google to decide whether the additional search was "reasonable." *Id.* That is a question that the Constitution makes clear is for a neutral and detached magistrate, not Google. *See Groh v. Ramirez*, 540 U.S. 551, 561 (2004) ("Even though [law enforcement] acted with restraint in conducting the search, 'the inescapable fact is that this restraint was imposed by the agents themselves, not by a judicial officer.'") (quoting *Katz*, 389 U.S. at 356). In reality, the government would have obtained the "maximum" amount of data authorized had Google not enforced the warrant's strong suggestion that law enforcement should be required to first "narrow down the list." *See* Ex. A at 1; Ex. B at 1. Google, not the government, deserves commendation

for somewhat limiting the scope of this dragnet search—but it is not and should not be their job to do so.

Put simply, the government lacked probable cause to search any individual's location data, so law enforcement sought to search a broad swath of everyone's data in the area of the robbery. Without sufficient probable cause, the warrant was doomed from the start, as further evinced by its equal lack of particularity. The government's "attempt" to "narrow down the list" was merely cosmetic, masking its multiple grabs for the "maximum" amount of data that it believed investigators was entitled to. Law enforcement's emails to Google clearly demonstrate how the government viewed the three-step process as no more than window dressing. Instead, the government put Google in the role of magistrate, deferring to Silicon Valley to determine what was "reasonable." *See* Ex. A at 1; Ex. B at 1. Such a delegation of constitutional authority is contrary to the Fourth Amendment, demonstrating the profound absence of probable cause or particularity in this case.

III. The warrant was *void ab initio*.

The government seeks to sidestep the unlimited breadth of the warrant by arguing that Mr. Chatrie "lacks standing to challenge the government's acquisition of others' location information." ECF No. 41 at 12. But Mr. Chatrie is not asserting the Fourth Amendment rights of others; he is asserting his own. The unlimited breadth of the warrant bears directly on its absence of particularity, rendering it an unconstitutional general warrant that was *void ab initio*—invalid from the beginning. *See Groh*, 540 U.S. at 558 (finding a warrant "so obviously deficient" in particularity that "we must regard the search as 'warrantless' within the meaning of our case law.").

The history of the Fourth Amendment and the framers of the Constitution make this very clear. For example, "[w]hen James Otis, Jr., delivered his courtroom oration against writs of

assistance in 1761," he argued that "the writs … were void as a form of general warrant." *Payton v. New York*, 445 U.S. 573, 608 (1980) (White, J., dissenting). Lord Camden's judgment in *Entick*, one of the pillars of English liberty and a catalyst for the Fourth Amendment, similarly held a general warrant to be "illegal and void." 19 How. St. Tr. 1029; *see Boyd*, 116 U.S. at 616 (citing this holding and noting that "the principles laid down in [*Entick*] affect the very essence of constitutional liberty and security."); *State Tax Comm'n v. Tenn. Coal, Iron & R. Co.*, 89 So. 179, 182 (Ala. 1921) (noting *Entick*'s holding that "the general warrants issued by the Secretary of State were, under such circumstances there outlined, declared illegal and void."). And when a warrant is void, "potential questions of 'harmlessness'" do not matter. *United States v. Krueger*, 809 F.3d 1109, 1123 (10th Cir. 2015) (Gorsuch, J., concurring). The geofence warrant violated Mr. Chatrie's Fourth Amendment rights, not just the rights of bystanders.

IV. The good faith doctrine does not apply.

The *Leon* good faith exception to the exclusionary rule does not apply to evidence discovered as a result of an arrest premised upon a warrant that was *void ab initio*. As the *Leon* Court explained, "in so limiting the suppression remedy, we leave untouched the probable-cause standard and the various requirements for a valid warrant." 468 U.S. 897, 923-24 (1984). Thus, the good-faith exception is inapplicable to warrants that do not meet the probable cause and particularity requirements. While the Fourth Circuit has applied the good faith exception to warrants authorized by magistrates lacking jurisdiction, *McLamb*, 880 F.3d at 691, the Circuit did so because suppression would not have appreciably deterred police misconduct. *See United States v. Seerden*, 916 F.3d 360, 367 (4th Cir. 2019). By contrast, the Fourth Circuit has never applied the good faith doctrine to a general warrant, as suppression serves the goal of deterring police from seeking such intentionally overbroad and unparticularized warrants in the future. *Leon* may excuse

a deficiency in the language of a warrant that is subsequently invalidated, but it cannot excuse a general warrant that is void at its inception. To hold otherwise would incentivize the kind of "systemic error" and "reckless disregard of constitutional requirements" that the Supreme Court has cautioned against. *Herring v. United States*, 555 U.S. 135, 144 (2009).

Even if *Leon* were to apply in this case, evidence from an unconstitutional search should still be suppressed in at least four circumstances, three of which are relevant here. *See United States v. Leon*, 468 U.S. 897, 923 (1984).

First, magistrate issuing the geofence warrant "abandoned his judicial role" by granting immense discretion to the executing officers to decide what Google data to search, and so "no reasonably well trained officer should [have] rel[ied] on the warrant." *See id.* (citing *Lo-Ji Sales, Inc. v. New York*, 442 U.S. 319 (1979)). *Lo-Ji Sales* determined that a "Town Justice" abandoned his judicial role when he accompanied the police to execute a warrant for obscene material at a store and granted the police immense discretion in seizing materials. 442 U.S. at 326-27. "When he ordered an item seized because he believed it was obscene, he instructed the police officers to seize all 'similar' items as well, leaving determination of what was 'similar' to the officer's [sic] discretion." *Id.* at 327. "The Fourth Amendment does not permit such action," nor such "open-ended warrants." *Id.* at 325. Among other problems, this grant of discretion prevents the magistrate from "verify[ing] that the inventory prepared by the police . . . accurately reflected what he had ordered seized." *Id.* at 327. Here, the warrant left it up to law enforcement and Google to decide which devices would be subject to further search in Steps 2 and 3. "The Fourth Amendment does not permit such action," reserving this function for the judiciary. *See id.* at 325. Here, the court would have no way of determining whether the data obtained in Steps 2 and 3 "accurately reflected" what the magistrate had ordered seized because there were no separate court orders

authorizing them. Instead, it was effectively an "open-ended warrant," *id.*, in which the magistrate abandoned his judicial role.

Second, the good faith exception should not apply because the government's generalized assumptions about cell phone use rendered the geofence warrant "so lacking in indicia of probable cause" to search Mr. Chatrie's data that "official belief in its existence [was] entirely unreasonable." *See Leon*, 468 U.S. at 923 (internal citations and quotations omitted). In *United States v. Doyle*, for example, the Fourth Circuit Court of Appeals held that good faith did not apply when the police searched a house for child pornography with a warrant that contained "remarkably scant evidence … to support a belief that [the defendant] *in fact* possessed child pornography." 650 F.3d 460, 472 (2011) (emphasis added). The district court incorrectly "opined that '[t]he magistrate could reasonably infer'" this possession from the affidavit's recitation of allegations of sexual assault by children and second-hand allegations of possession of child pornography. *Id*. at 471-72. In *Seerden*, by contrast, good faith did apply where the affidavit contained allegations and admissions of the actual crime for which evidence was sought (sexual assault). 916 F.3d 360, 367-68 (4th Cir. 2019). Here, the police presented no evidence that the robber "in fact" had a smartphone, used Android or Google services, and opted-in to location services, and thus that his data was "in fact" in Google's Sensorvault. *See Doyle*, 650 F.3d at 472; ECF No. 41 at 14. Per *Doyle*, this Court cannot "reasonably infer" this fact from the government's generalized assumptions about cell phone use and should instead hold that any "belief in [the] existence [of probable cause for the warrant was] entirely unreasonable." *See Doyle*, 650 F.3d at 471; *see Leon*, 468 U.S. at 923.

Third, good faith should not apply because the geofence warrant was "facially deficient." *See Leon*, 468 U.S. at 923. It sought unfettered discretion to search deeply private data of an

unlimited number of people, and was so lacking in probable cause and particularity that "the executing officers [could not have] reasonably presume[d] it to be valid." *See id*. The government's attempt to evade this problem with *McLamb* is unpersuasive. In *McLamb*, the court found that "the boundaries of a magistrate judge's jurisdiction in the context of remote access warrant" was not clear at the time the agent applied for the warrant. 880 F.3d at 691. In those very limited circumstances, the court looked to the agent's consultation with attorneys from a specialized section within DOJ as evidence of good faith. Here, the watershed decision in *Carpenter* provided significant guidance for officers in this case. This Court cannot allow a reference to consulting with a government attorney to subsume the Fourth Amendment's requirement that a neutral and detached magistrate decide whether to issue the warrant.

As the Supreme Court recognized many decades ago, the Fourth Amendment requires a "neutral and detached" judge to find probable cause because the investigating officers are engaged in "the often competitive enterprise of ferreting out crime." *Coolidge v. New Hampshire*, 403 U.S. 443, 449 (1971). "[T]he whole point of the basic rule . . . is that prosecutors and policemen simply cannot be asked to maintain the requisite neutrality with regard to their own investigations—the 'competitive enterprise' that must rightly engage their single-minded attention." *Id.* at 450. Thus, it is the role of only the courts to enforce the constitutional requirement of particularity. To adopt the government's position here that consulting with members of the prosecution team is sufficient to establish good faith would completely eviscerate a clear protection that the Fourth Amendment in its own words requires.

CONCLUSION

The geofence warrant in this case was a general warrant, devoid of the probable cause and particularity required by the Fourth Amendment, the unconstitutionality of which should have been

readily apparent. For the foregoing reasons, Mr. Chatrie requests that this Court find the warrant void and suppress all of 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

CERTIFICATE OF SERVICE

I hereby certify that on December 9, 2019, I filed the foregoing with the Clerk of Court using the CM/ECF system, which will send a notification of such filing (NEF) to all counsel of record.

_____/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

From: Hylton, Joshua
To: USLawEnforcement@google.com
Subject: 2590472

Google Legal Team,

I appreciate your team's quick response and professionalism. After reviewing the return data and associated Google Device ID(s), Assistant United States Attorney, Kenneth Simon, and I, request additional location data and subscriber info for the following device ID(s):

1. 1716665659
2. -1662305683
3. -1305167611
4. -1844271119
5. -965610516
6. 2021066118
7. 702354289
8. 907512662
9. 1207269668

10. -1144423700
11. -162381959
12. -1637158857
13. -2058726931
14. -41133693
15. 1135979718
16. 138503045
17. 1485182252
18. 319756533
19. 449021346

As the sought Google devices are fairly low in number, I am requesting the above data in an effort to rule out possible co-conspirators. If this request seems unreasonable, please keep in mind that Google device numbers 1-9 may fit the more likely profile of parties involved.

I appreciate any help and consideration in the above matter. If you have any questions or concerns, please don't hesitate to call, [redacted]

Respectfully,

Master Detective J.P. Hylton Unit: 936
Criminal Investigations Division: Persons Unit
[redacted]

"If you only do what you can do, you will never be better than what you are now."

Respectfully,

Master Detective J.P. Hylton Unit: 936
Criminal Investigations Division: Persons Unit
[redacted]
[redacted]

"If you only do what you can do, you will never be better than what you are now."

From: Hylton, Joshua
To: USLawEnforcement@google.com
Subject: 2590472
Importance: High

Google Legal Team,

I'm writing to inquire about my correspondence with your office on 07/01 and 07/02. Please keep in mind that expedition is requested based on armed and dangerous subject(s) still being at large. Subject was on cell phone just prior to violent act; therefore, Google may have captured pertinent information to identify and arrest parties involved. See below:

I appreciate your team's quick response and professionalism. After reviewing the return data and associated Google Device ID(s), Assistant United States Attorney, Kenneth Simon, and I, request additional location data and subscriber info for the following device ID(s):

1. 1716665659
2. -1662305683
3. -1305167611
4. -1844271119
5. -965610516
6. 2021066118
7. 702354289
8. 907512662
9. 1207269668

10. -1144423700
11. -162381959
12. -1637158857
13. -2058726931
14. -41133693
15. 1135979718
16. 138503045
17. 1485182252
18. 319756533
19. 449021346

As the sought Google devices are fairly low in number, I am requesting the above data in an effort to rule out possible co-conspirators. If this request seems unreasonable, please keep in mind that Google device numbers 1-9 may fit the more likely profile of parties involved.

I appreciate any help and consideration in the above matter. If you have any questions or concerns, please don't hesitate to call, [redacted]

Respectfully,

Master Detective J.P. Hylton Unit: 936
Criminal Investigations Division: Persons Unit
[redacted]

"If you only do what you can do, you will never be better than what you are now."

From: Hylton, Joshua
To: USLawEnforcement@google.com
Subject: 2590472

Google Legal Team,

As discussed yesterday over the phone, I appreciate your quick response and willingness to provide GPS data for the below device ID(s). Please expedite this request where possible due to this suspect's continued threat to our community. If it would speed up the process, please provide data as it becomes accessible/available, starting with device ID(s) 1 – 9. It was mentioned that the larger the request, the more time it will take to get data back. With this in mind, I will still have to rule out device ID(s) 1-9; however, I may be able to do so more quickly if I can begin reviewing data. The faster I can review the data, the faster I can get this guy/guys off the street.

Thanks again for your professionalism and understanding. I realize that I'm asking for a lot and you and your team are likely tasked-out already, but any and all assistance and expedited process is MUCH appreciated.

1. 1716665659
2. -1662305683
3. -1305167611
4. -1844271119
5. -965610516
6. 2021066118
7. 702354289
8. 907512662
9. 1207269668

If you have any questions or concerns, please don't hesitate to call, [redacted]

Respectfully,

Master Detective J.P. Hylton Unit: 936
Criminal Investigations Division: Persons Unit
[redacted]

"If you only do what you can do, you will never be better than what you are now."

Respectfully,

Master Detective J.P. Hylton Unit: 936
Criminal Investigations Division: Persons Unit
[redacted]

[redacted]

"If you only do what you can do, you will never be better than what you are now."

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 NOTICE REGARDING ATTACHMENT OF GOOGLE GEOFENCE STATE SEARCH WARRANT TO RESPONSE IN OPPOSITION TO MOTION TO SUPPRESS

The United States of America, by its undersigned attorneys, hereby provides notice that the State Search Warrant attached to this Notice is the underlying search warrant relevant to the Defendant's Motion to Suppress Evidence Obtained from the Google "Geofence" Search Warrant, the United States' Response in Opposition, and the Defendant's Reply. ECF Nos. 29, 41, 48. Accordingly, the United States seeks to have the attached search warrant docketed as an exhibit to its Response in Opposition to the Defendant's Motion. *See* ECF No. 41.

Respectfully submitted,

G. ZACHARY TERWILLIGER
United States Attorney

By: /s/

Kenneth R. Simon, Jr.
Peter S. Duffey
Assistant United States Attorneys
United States Attorney's Office
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

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 18th day of December, 2019, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send an electronic notification of such filing to the following:

Laura Koenig
Office of the Federal Public Defender (Richmond)
701 E Broad Street
Suite 3600
Richmond, VA 23219
Email: Laura_Koenig@fd.org

Paul Geoffrey Gill
Office of the Federal Public Defender (Richmond)
701 E Broad Street
Suite 3600
Richmond, VA 23219
Email: paul_gill@fd.org

Michael William Price
National Association of Criminal Defense Lawyers
1660 L Street NW
12th Floor
Washington, DC 20036
(202) 465-7615
Email: mprice@nacdl.org
PRO HAC VICE

_____/s/_____
Kenneth R. Simon, Jr.
Assistant United States Attorney
United States Attorney's Office
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

ALL INFORMATION SEALED

J.A. 107

AFFIDAVIT FOR SEARCH WARRANT

Commonwealth of Virginia VA. CODE § 19.2-54

The undersigned Applicant states under oath:

1. A search is requested in relation to [X] an offense substantially described as follows:
   [ ] a person to be arrested for whom a warrant or process for arrest has been issued identified as follows:

   Code of Virginia 18.2-58: Robbery
   Code of Virginia 18.2-53.1: Use of a Firearm in Commission of a Felony

[ ] CONTINUED ON ATTACHED SHEET

2. The place, person or thing to be searched is described as follows:

   Google LLC, which is headquartered at 1600 Google Amphitheater Parkway, Mountain View, California 94043, and applies to Target Location: Geographical area pertaining to a radius of 150 meters around a latitude/longitude coordinate, Latitude: 37.438420, Longitude: -77.587900. It is your affiant's belief that the records requested are actually possessed by Google LLC, and that Google LLC provides electronic communication service or remote computing service within the Commonwealth of VA. (See Attachment I. for Additional Information)

[ ] CONTINUED ON ATTACHED SHEET

3. The things or persons to be searched for are described as follows:

   See Attachment II.

2019 JUN 14 AM 10:30

[ ] CONTINUED ON ATTACHED SHEET

(OVER)

FORM DC-338 (MASTER, PAGE ONE OF TWO) 07/17

FILE NO. 744

AFFIDAVIT FOR SEARCH WARRANT

APPLICANT:

J.P. Hylton
NAME

Master Detective
TITLE (IF ANY)

P.O. Box 148
ADDRESS

Chesterfield, VA 23832

Certified to Clerk of Chesterfield Circuit Court
CITY OR COUNTY

on 6/14/19
DATE

Magistrate
TITLE

[signature]
SIGNATURE

Original Delivered [X] in person [ ] by certified mail
[X] by electronically transmitted facsimile
[ ] by use of filing/security procedures defined in the Uniform Electronic Transactions Act

to Clerk of Chesterfield Circuit Court
CITY OR COUNTY WHERE EXECUTED

on 6/14/19
DATE

Magistrate
TITLE

[signature]
SIGNATURE

4. The material facts constituting probable cause that the search should be made are: ALL INFORMATION SEALED

See Attachment III.

5. The object, thing or person searched for [X] constitutes evidence of the commission of such offense [ ] is the person to be arrested for whom a warrant or process for arrest has been issued.

6. [X] I have personal knowledge of the facts set forth in this affidavit AND/OR

[ ] I was advised of the facts set forth in this affidavit, in whole or in part, by one or more other person(s). The credibility of the person(s) providing this information to me and/or the reliability of the information provided may be determined from the following facts:

Your affiant has over seven years of law enforcement experience stemming from employment as a police officer with the Chesterfield County Police Department. The undersigned is a duly appointed Task Force Officer with the Federal Bureau of Investigation (FBI). Your affiant is assigned to the Richmond FBI's Central Virginia Violent Crimes Task Force, where his duties include investigating extraterritorial offenses, commercial and bank robberies, murder, kidnappings, serial offenses, armed carjackings, and theft of government property. The undersigned has investigated numerous criminal violations and obtained multiple arrest and search warrants, culminating in the successful prosecution of their respective offenders. Your affiant is familiar with the methods violent offenders use to conduct their illegal activities, to include their communication techniques, utilization of electronic devices for planning/execution, use of additional co-conspirators, and reoccurring method of operation (MO).

The statements above are true and accurate to the best of my knowledge and belief.

Master Detective
TITLE OF APPLICANT

APPLICANT

Subscribed and sworn to before me this day.

6/14/19
DATE AND TIME

[ ] CLERK [✓] MAGISTRATE [ ] JUDGE

FORM DC-338 (MASTER, PAGE TWO OF TWO) 07/17

ALL INFORMATION SEALED

ATTACHMENT I.
PERSON, PLACE, OR THING TO BE SEARCHED:

This data is maintained on computer servers that are stored at premises controlled by Google Inc., a company that accepts service of legal process at 1600 Amphitheater Parkway, Mountain View, California 94043.

Your affiant knows that Google Inc. maintains certain records during the normal course of business and when properly served with a legal request, Google Inc. will provide Law Enforcement with the said records. Your affiant also knows that these electronic records will further support the ongoing criminal investigation. Your affiant believes that the records requested are actually or constructively possessed by a foreign corporation, Google Inc. that provides electronic communication service or remote computing service within the Commonwealth of Virginia.

Your affiant knows that section 19.2-70.3 of the Code of Virginia states that a provider of electronic communication service or remote computing service, which includes a foreign corporation that provides such services, shall disclose certain business records pertaining to their customers, excluding the contents of electronic communications and real-time location data, to an investigative or law-enforcement officer if the investigative or law-enforcement officer shows that there is reason to believe the records or other information sought are relevant and material to an ongoing criminal investigation. This warrant shall be properly served on the entity named above in accordance with 19.2-70.3 of the code of Virginia.

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider, Google Inc. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in ATTACHMENT II.

RECEIVED & FILED
CHESTERFIELD CIRCUIT COURT
2019 JUN 14 AM 10: 31
[illegible] HUGHES
CLERK OF COURT
[illegible]
D. CLERK

ALL INFORMATION SEALED

ATTACHMENT II.
THE PLACE, PERSON OR THING TO BE SEARCHED:

The facts and circumstances outlined in this affidavit brought on by your Affiant suggest that there is probable cause to believe evidence of the commission of the crime of **Robbery**, a violation of **Virginia Code 18.2-58** and **Use of a Firearm in Commission of a Felony,** a violation of **Virginia Code 18.2-53.1**, may be found within computer servers maintained or controlled by Google, Inc. or Google Payment Corp. Such accounts are described further in ATTACHMENT II. (hereinafter "the Accounts") stored at premises controlled by Google, Inc., a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California 94043. The following material is sought for the time period listed below:

- **Date/Time: 05/20/2019 at 1620 hours (EST) – 05/20/2019 at 1720 hours (EST)**

- For each type of Google account that is associated with a device that was inside the geographical area described further in ATTACHMENT II., **during the time frame listed above,** Google will provide **"anonymized information"** regarding the Accounts that are associated with a device that was inside the described geographical area during the time frame described above. This **"anonymized information"** will include a numerical identifier for the account, the type of account, time stamped location coordinates and the data source that this information came from if available. The information initially provided by Google will not contain any further content or information identifying the user of a particular device or account.

- Law enforcement officers will review this **"anonymized information"** provided by Google, Inc. in an effort to narrow down the list of accounts associated with devices identified in the **"anonymized information."** Law enforcement officers will attempt to narrow down the list by reviewing the time stamped location coordinates for each account and comparing that against the known time and location information that is specific to this crime.

- Law enforcement officers will return a list that they have attempted to narrow down. This list will still be identified by the "**anonymized information**" described above. After this review by Law Enforcement and upon request, Google, Inc. shall produce "contextual data points with points of travel outside of the geographical area" described further in ATTACHMENT II. of this Application for Search Warrant. The time frame will be expanded for this production of "contextual data points with points of travel outside of the geographical area" for 30 minutes before AND 30 minutes after the initial search time periods. This expanded time frame will be as listed below (Google Inc. shall provide this additional information to Law Enforcement for review):

ALL INFORMATION SEALED

- **Date/Time: 05/20/2019 at 1620 hours (EST) – 05/20/2019 at 1720 hours (EST) (+/- 30 Minutes) Eastern Standard Time (EST)**

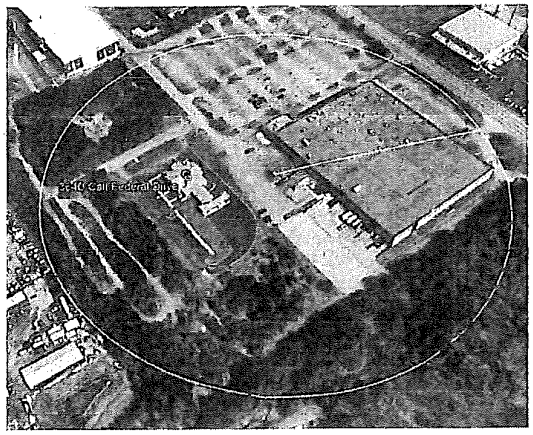
- Law Enforcement officers will review this additional information along with the **"anonymized information"** and will attempt to narrow down the list by comparing this additional information regarding travel and time against the known time and location information that is specific to this crime.

- After review and upon request by Law Enforcement, Google Inc. shall provide identifying account information/CSI for the accounts requested by Law Enforcement. This identifying account information/CSI shall include all of the following that are available: user name and subscriber information to include date of birth if available, account type and account number, email addresses associated with the account, electronic devices associated with the account and their identifying make, model and other identifying numbers, telephone numbers associated with the account including telephone numbers used to set up the account, verify the account or to receive assistance with the account, and Google Voice phone numbers associated with the account.

This search warrant applies to the Google Accounts associated with devices that were located inside the geographical regions bounded by the following latitudinal and longitudinal coordinates, dates, and times:

Date/Time: 05/20/2019 at 1620 hours (EST) – 05/20/2019 at 1720 hours (EST)

Geographical Area: Radius of 150 meters around a latitude/longitude coordinate, **Latitude: 37.438420, Longitude: -77.587900.** **An area encompassing the Call Federal Credit Union and an adjacent business the UNSUB fled towards following the robbery**



ALL INFORMATION SEALED

ATTACHMENT III.

MATERIAL FACTS CONSTITUTING PROBABLE CAUSE:

The Affiant swears to the following facts to establish probable cause for the issuance of a search warrant:

On 05/20/2019 at approximately 1650 hours, an unknown subject (UNSUB) entered the Call Federal Credit Union, [redacted] Call Federal Drive, Chesterfield, VA 23235. After entering the bank, the UNSUB approached a teller line and presented a demand note stating the following:

"I've been watching you for sometime now. 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 got my boys on the lookout out side. The first cop car they see am going start hurting everyone in sight, hand over all the cash, I need at least 100k and nobody will get hurt and your family will be set free. Think smartly everyone safety is depending and you and your coworkers action so I hope they don't try nothing stupid."

After reading the note, the victim-teller advised she did not have access to that amount of money; subsequently, the UNSUB produced a silver and black firearm from his waste and began forcing the customers and employees to the center of the room. After forcing several patrons to the floor at gunpoint, the UNSUB moved the manager and other parties present to the back of the business where the vault was located. The UNSUB forced the manager to open the vault and place $195,000.00 of United States currency into a bag he brought with him. After acquiring said funds, the UNSUB fled the area on foot towards an adjacent business, west of the bank.

Upon investigative response, law enforcement officials reviewed the bank's surveillance video prior to the robbery and noted the UNSUB had a cell phone in his right hand and appeared to be speaking with someone on the device. Subsequently, your affiant finds it necessary and prudent to request that Google provide Geo Fencing data in order to assist with the investigation. In the undersigned's training and experience, when people act in concert with one another to commit a crime, they frequently utilize cellular telephones and other such electronic devices, to communicate with each other through WiFi, Bluetooth, GPS, voice calls, text messages, social media accounts, applications, emails, and/or cell towers in the area of the victim-business, located at [redacted] Call Federal Drive, Chesterfield, Virginia 23235. Furthermore, the requested data/information would have been captured by Google during the requested time.

This applicant knows a cellular telephone or mobile telephone is a handheld wireless device primarily used for voice, text, and data communication through radio signals.

ALL INFORMATION SEALED

Cellular telephones send signals through networks of transmitter/receivers called "cells" or "cell sites," enabling communication with other cellular telephones or traditional "landline" telephones. Cellular telephones rely on cellular towers, the location of which may provide information on the location of the subject telephone. Cellular telephones may also include global positioning system ("GPS") or other technology for determining a more precise location of the device.

This applicant also knows that Google is a company, which, among other things, provides electronic communication services to subscribers, including email services. Google allows subscribers to obtain email accounts at the domain name gmail.com and/or google.com. Subscribers obtain an account by registering with Google. A subscriber using the Provider's services can access his or her email account from any computer/device connected to the Internet.

This applicant knows that Google has also developed a proprietary operating system for mobile devices, including cellular phones, known as Android. Nearly every cellular phone using the Android operating system has an associated Google account, and users are prompted to add a Google account when they first turn on a new Android device.

Based on this applicant's training and experience, this applicant knows that Google collects and retains location data from Android-enabled mobile devices when a Google account user has enabled Google location services. Google can also collect location data from non-Android devices if the device is registered to a Google account and the user has location services enabled. The company uses this information for location-based advertising and location-based search results and stored such data in perpetuity unless it is manually deleted by the user. This location information is derived from GPS data, cell site/cell tower information, Bluetooth connections, and Wi-Fi access points.

This applicant knows that location data can assist investigators in forming a fuller geospatial understanding and timeline related to a specific criminal investigation; and may tend to identify potential witnesses and/or suspects. Such information can also aid investigators in possibly inculpating or exculpating persons of interest.

Additionally, location information can be digitally integrated into image, video, or other computer files associated with a Google account and can indicate the geographic location of the account's user at a particular date and time (e.g., digital cameras, including on cellular telephones, frequently store GPS coordinates indicating where a photo was taken in the "metadata" of an image file).

Your affiant knows that in the September 2013 Pew Research Center study, it was determined that 91% of American adults own a cellular phone with 56% being smartphones. Pew Research Center is located at 1615 L St. NW, Suite 800 Washington, DC 20036 and conduct public opinion polling, demographic research, content analysis and other data-driven social science research. Because of this, your Affiant believes that there is probable cause to believe that the offender(s) in the robbery would have had a mobile device on their person or within close proximity to them.

ALL INFORMATION SEALED

SEARCH WARRANT

Commonwealth of Virginia VA. CODE §§ 19.2-56, 19.2-57

TO ANY AUTHORIZED OFFICER:

You are hereby commanded in the name of the Commonwealth to forthwith search the following place, person or thing either in day or night

Google, LLC. which is headquartered at 1600 Google Amphitheater Parkway, Mountain View, California 94043 - Probable cause that the records are possessed by a foreign corporation that provides electronic communication service orremote computing service within Virginia.

for the following property, objects and/or persons:
See Attached

You are further commanded to seize said property, persons, and/or objects if they be found and to produce before the Chesterfield Circuit Court an inventory of all property, persons, and/or objects seized.

This SEARCH WARRANT is issued in relation to [X] an offense substantially described as follows:
[ ] a person to be arrested for whom a warrant or process for arrest has been issued identified as follows:
Code of Virginia 18.2-58 Robbery
Code of Virginia 18.2-53.1 Use of a Firearm in the Commission of a Felony

I, the undersigned, have found probable cause to believe that the property or person constitutes evidence of the crime identified herein or tends to show that the person(s) named or described herein has committed or is committing a crime, or that the person to be arrested for whom a warrant or process for arrest has been issued is located at the place to be searched, and further that the search should be made, based on the statements in the attached affidavit sworn to by

Hylton, J.P. CPD[redacted]
NAME OF AFFIANT

06/14/2019 10:06 AM
DATE AND TIME

[ ] CLERK [X] MAGISTRATE [ ] JUDGE

David Bishop

FORM DC-339 (MASTER, PAGE ONE OF TWO) 07/17

FILE NO. 744

SEARCH WARRANT

COMMONWEALTH OF VIRGINIA

v./*In re*

Google LLC

Return to Circuit Court

ORIGINAL

SWN: 041CM1900017880

ALL INFORMATION SEALED

SEARCH INVENTORY AND RETURN

The following items, and no others, were seized under authority of this WARRANT:

1. Data
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.

RECEIVED & FILED
CHESTERFIELD CIRCUIT COURT
WENDY S. HUGHES, CLERK
JUN 19 2019
TESTE:
CLERK DEPUTY CLERK

The statement above is true and accurate to the best of my knowledge and belief.

6/19/2019
DATE

EXECUTING OFFICER

Subscribed and sworn before me this day

6.19.19
DATE

[ ] CLERK [ ] MAGISTRATE [ ] JUDGE

FOR NOTARY PUBLIC'S USE ONLY:

State of ..... [ ] City [ ] County of .....

Acknowledged, subscribed and sworn to before me this ..... day of ....., 20 .....

NOTARY REGISTRATION NUMBER

NOTARY PUBLIC
(My commission expires: .....)

FORM DC-339 (MASTER, PAGE TWO OF TWO) 01/09

EXECUTION

Executed by searching the within described place, person or thing.

6/14/2019 at 1030 Hrs
DATE AND TIME EXECUTED

Hylton
EXECUTING OFFICER

Certified to Chesterfield County Circuit Court on 6/19/2019
DATE

EXECUTING OFFICER

Received [X] in person [ ] by certified mail
[ ] by electronically transmitted facsimile

on 6.19.19
DATE

by:
CLERK OF CIRCUIT COURT

ALL INFORMATION SEALED

ATTACHMENT I.
THE PLACE, PERSON OR THING TO BE SEARCHED:

The facts and circumstances outlined in this affidavit brought on by your Affiant suggest that there is probable cause to believe evidence of the commission of the crime of **Robbery**, a violation of **Virginia Code 18.2-58** and **Use of a Firearm in Commission of a Felony,** a violation of **Virginia Code 18.2-53.1**, may be found within computer servers maintained or controlled by Google, Inc. or Google Payment Corp. Such accounts are described further in ATTACHMENT II. (hereinafter "the Accounts") stored at premises controlled by Google, Inc., a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California 94043. The following material is sought for the time period listed below:

- **Date/Time: 05/20/2019 at 1620 hours (EST) – 05/20/2019 at 1720 hours (EST)**

- For each type of Google account that is associated with a device that was inside the geographical area described further in ATTACHMENT II., **during the time frame listed above,** Google will provide **"anonymized information"** regarding the Accounts that are associated with a device that was inside the described geographical area during the time frame described above. This **"anonymized information"** will include a numerical identifier for the account, the type of account, time stamped location coordinates and the data source that this information came from if available. The information initially provided by Google will not contain any further content or information identifying the user of a particular device or account.

- Law enforcement officers will review this **"anonymized information"** provided by Google, Inc. in an effort to narrow down the list of accounts associated with devices identified in the **"anonymized information."** Law enforcement officers will attempt to narrow down the list by reviewing the time stamped location coordinates for each account and comparing that against the known time and location information that is specific to this crime.

- Law enforcement officers will return a list that they have attempted to narrow down. This list will still be identified by the "**anonymized information**" described above. After this review by Law Enforcement and upon request, Google, Inc. shall produce "contextual data points with points of travel outside of the geographical area" described further in ATTACHMENT II. of this Application for Search Warrant. The time frame will be expanded for this production of "contextual data points with points of travel outside of the geographical area" for 30 minutes before AND 30 minutes after the initial search time periods. This expanded time frame will be as listed below (Google Inc. shall provide this additional information to Law Enforcement for review):

ALL INFORMATION SEALED

- **Date/Time: 05/20/2019 at 1620 hours (EST) – 05/20/2019 at 1720 hours (EST) (+/- 30 Minutes) Eastern Standard Time (EST)**

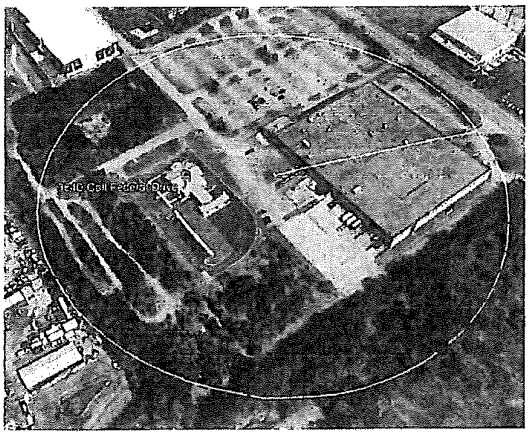
- Law Enforcement officers will review this additional information along with the **"anonymized information"** and will attempt to narrow down the list by comparing this additional information regarding travel and time against the known time and location information that is specific to this crime.

- After review and upon request by Law Enforcement, Google Inc. shall provide identifying account information/CSI for the accounts requested by Law Enforcement. This identifying account information/CSI shall include all of the following that are available: user name and subscriber information to include date of birth if available, account type and account number, email addresses associated with the account, electronic devices associated with the account and their identifying make, model and other identifying numbers, telephone numbers associated with the account including telephone numbers used to set up the account, verify the account or to receive assistance with the account, and Google Voice phone numbers associated with the account.

This search warrant applies to the Google Accounts associated with devices that were located inside the geographical regions bounded by the following latitudinal and longitudinal coordinates, dates, and times:

Date/Time: 05/20/2019 at 1620 hours (EST) – 05/20/2019 at 1720 hours (EST)

Geographical Area: Radius of 150 meters around a latitude/longitude coordinate, **Latitude: 37.438420, Longitude: -77.587900.** **An area encompassing the Call Federal Credit Union and an adjacent business the UNSUB fled towards following the robbery**



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

UNITED STATES OF AMERICA v. OKELLO T. CHATRIE, *Defendant*.	Case No. 3:19-cr-00130-MHL

BRIEF OF AMICUS CURIAE GOOGLE LLC IN SUPPORT OF NEITHER PARTY CONCERNING DEFENDANT'S MOTION TO SUPPRESS EVIDENCE FROM A "GEOFENCE" GENERAL WARRANT (ECF NO. 29)

DISCLOSURE STATEMENT

Pursuant to Local Criminal Rule 12.4, Google hereby discloses that it is an indirect subsidiary of Alphabet Inc., a publicly traded company. No publicly traded company holds more than 10% of Alphabet Inc.'s stock.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES AND RULES

OTHER AUTHORITIES

INTEREST OF AMICUS CURIAE[1]

Google LLC ("Google") is a diversified technology company whose mission is to organize the world's information and make it universally accessible and useful. Google offers a variety of products and services, including the Android and Chrome operating systems, as well as Google Search, Maps, Drive, and Gmail. Among those products and services is Google Location History ("LH"), which allows individual users who have chosen to use the LH service to create, edit, and save records of their whereabouts over time—akin to journal entries of journeys taken and places visited. The warrant at issue in this motion compelled Google to produce data associated with Chatrie and other Google users—specifically, data from Google's LH service.

When using LH and other services, Google users routinely entrust private, personal data, including location-related information, to Google for processing and storage. Google recognizes and respects the privacy of this information and is transparent with users about when and how their information is stored. For example, Google's Privacy Policy informs users about their data, how to keep it safe, and how to take control. And Google regularly publishes transparency reports that reflect the volume of requests for disclosure of user data that Google receives from government entities.

Google respectfully submits this amicus brief in support of neither party to provide contextual information to the Court about the data at issue in Defendant Chatrie's motion to suppress evidence obtained from a so-called "geofence" warrant. *See* Mot. to Suppress Evidence

[1] The undersigned certifies that no party or party's counsel authored this brief in whole or in part; no party or party's counsel contributed money that was used to fund the preparation or submission of this brief; and no persons other than amicus curiae or its counsel contributed money that was intended to fund the preparation or submission of this brief.

Obtained From a "Geofence" General Warrant (ECF No. 29) ("Mot."); Govt. Response in Opp. to Def.'s Motion for Suppression of Evidence Obtained Pursuant to Google Geofence Warrant (ECF No. 41) ("Opp."). That warrant compelled Google to produce users' LH information, so an understanding of that information—including what it is, how users can create and save it, and what Google must do to comply with a warrant to produce it—is needed to resolve the parties' legal arguments on the motion to suppress. While the parties' briefs reveal some uncertainty about certain aspects of LH that are relevant to the questions presented by the motion, Google is well situated to explain the nature of the data and the steps Google takes in response to geofence warrants like the one at issue here. Moreover, because law-enforcement requests for this type of data have become increasingly common in recent years, Google also has a significant interest in the constitutional and statutory requirements and limitations that govern law enforcement efforts to obtain LH information. While Google takes no position on the validity of the warrant at issue in this case or whether the evidence it yielded should be suppressed, it respectfully urges the Court to take into account the full factual context surrounding the warrant and hold that both the Stored Communications Act, 18 U.S.C. § 2703, and the Fourth Amendment require the government to obtain a warrant supported by probable cause to obtain LH information stored by Google users.[2]

INTRODUCTION AND SUMMARY OF ARGUMENT

Pursuant to the Stored Communications Act, 18 U.S.C. §§ 2701 *et seq.*, law enforcement can and frequently does obtain legal process compelling Google to disclose the contents or

[2] By submitting this brief as amicus curiae, Google does not become a party to the case and does not waive any objections it might have to any efforts by the parties to obtain discovery or testimony from Google. *See, e.g.*, Fed. R. Crim. P. 17(c)(2); *In re Grand Jury, John Doe No. G.J.2005-2*, 478 F.3d 581, 585 (4th Cir. 2007) ("Courts have recognized various ways in which a subpoena may be unreasonable or oppressive under Rule 17(c).").

records of particular users' stored electronic communications, including data that reveals those persons' locations and movements at particular times of interest. Such requests typically seek to compel disclosure of information pertaining to specifically identified persons of interest in a criminal investigation.

This case, in contrast, concerns a novel but rapidly growing technique in which law enforcement seeks to require to search across LH data, using legal requests sometimes called "geofence" requests. Rather than seeking information relating to a known suspect or person of interest, these requests broadly seek to identify all Google LH users whose LH data suggests that they were in a given area in a given timeframe—even though law enforcement has no particularized basis to suspect that all of those users played a role in, or possess any information relevant to, the crime being investigated. State and federal law-enforcement authorities have made increasing use of this technique in recent months and years. Year over year, Google has observed over a 1,500% increase in the number of geofence requests it received in 2018 compared to 2017; and to date, the rate has increased over 500% from 2018 to 2019.

As set forth below, the LH information at issue in geofence requests such as the one in this case differs in significant respects from the cell site location information ("CSLI") at issue in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), and other types of data that courts have considered in Fourth Amendment cases. For example, rather than a record created and stored by Google as an automatic result of using a Google service, Google LH information is created, edited, and stored by and for the benefit of Google users who opt into the service and choose to communicate their location information to Google for storage and processing. Moreover, LH information can often reveal a user's location and movements with a much higher degree of precision than CSLI and other types of data. And rather than targeting the electronic

communications of only a specific user or users of interest, the steps Google must take to respond to a geofence request entail the government's broad and intrusive search across Google users' LH information to determine which users' devices may have been present in the area of interest within the requested timeframe.

Given the characteristics of geofence requests, the law requires the government to obtain a warrant to require Google to search LH information. First, although the parties have not addressed the statutory context, the Stored Communications Act ("SCA")—quite apart from the Constitution—requires the government to obtain a search warrant because a geofence request seeks the "contents" of Google users' electronic communications within the meaning of the SCA. *See* 18 U.S.C. § 2703(a), (b). Therefore, regardless of whether a geofence request amounts to a "search" for Fourth Amendment purposes, the government must obtain a warrant from a neutral magistrate that satisfies the requirements of probable cause and particularity. *See id.* (incorporating requirements of Fed. R. Crim. P. 41).

In any event, it is also clear that a geofence request constitutes a "search" within the meaning of the Fourth Amendment and that, absent an applicable exception, the Constitution independently requires the government to obtain a warrant to obtain LH information. Users have a reasonable expectation of privacy in their LH information, which the government can use to retrospectively reconstruct a person's movements in granular detail. Under *Carpenter*, the "third-party doctrine" does not defeat that reasonable expectation of privacy merely because users choose to store and process the information on Google' servers.

Whether under the SCA or under the Fourth Amendment—and absent an applicable exception—the government is therefore obligated to obtain a warrant to search LH information. That requirement is entirely appropriate in light of the sensitivity of LH information, the intimate

details it can reveal about a user's life, and the breadth of the government's intrusion on users' private LH information that occurs whenever a geofence search is executed. Google's users expect their LH information to be kept private, and the Court should ensure that it receives the greatest available protection. Google takes no position on Defendant Chatrie's arguments that the warrant at issue here failed to satisfy the requirements of probable cause and particularity or, if so, whether suppression is the appropriate remedy. But the Court should hold—taking account of the full factual context—that a warrant is indeed required.

ARGUMENT

I. GOOGLE "LOCATION HISTORY" INFORMATION DIFFERS SIGNIFICANTLY FROM CELL SITE LOCATION INFORMATION AND OTHER TYPES OF LOCATION DATA COURTS HAVE CONSIDERED IN OTHER FOURTH AMENDMENT CASES

While many of Google's products and services can be used without a Google account, millions of people choose to create Google accounts and log into them from their mobile devices or while using Google applications to take full advantage of account-specific products such as Gmail and to obtain a more personalized experience on applications such as Maps and Search. Holders of Google accounts can control various account-level and service-level settings and preferences. "Location History" (or "LH") is an optional account-level Google service. It does not function automatically for Google users. But when users opt into LH on their Google accounts, it allows those users to keep track of locations they have visited while in possession of their mobile devices.

In the briefing, the parties analogize the LH information at issue in this case to CSLI, "tower dumps," GPS data, and other types of location information that courts have considered in other cases. Mot. 2, 14; Opp. 7-8, 11-12, 18. In fact, while Google LH information bears some similarities to those types of data in some respects, it differs in important ways that are highly

relevant to the question whether a warrant is required. In determining the legal framework governing law enforcement requests for Google LH information, the court should therefore proceed with an understanding of the nature and precision of that information, how it is recorded and stored, how users control it, and how it is collected in response to legal process.

A. Google "Location History" Is Not A Business Record, But A Journal Of A User's Location And Travels That Is Created, Edited, And Stored By And For The Benefit Of Google Users Who Have Opted Into The Service

Google "Location History" information is essentially a history or journal that Google users can choose to create, edit, and store to record their movements and travels. Google's users activate and use LH for many reasons. By enabling and using LH, a Google user can keep a virtual journal of her whereabouts over a period of time. For most Google users, this journal is captured in the "Timeline" feature of the Google Maps app. *See* Fig. 1. The Timeline feature allows the user to visualize where she has traveled with her phone and when over a given period—in essence, a journal. The Timeline might reflect, for instance, that the user left her home on Elm Street in the morning and walked to the bus stop, took the bus to her office on Main Street, walked to a nearby coffee shop and back to the office in the afternoon, and then went to a nearby restaurant in the evening before returning home by car.

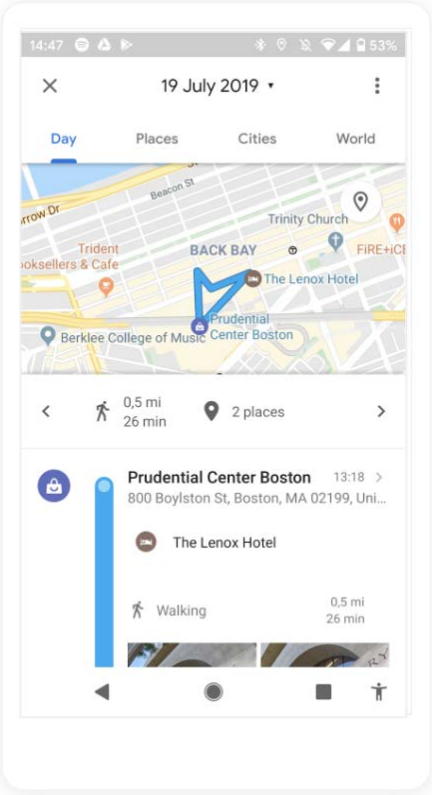


Figure 1. Sample Google Timeline.

By using Google LH, the user can access other benefits on her Google device or applications as well. For example, she can obtain personalized maps or recommendations based

on places she has visited, get help finding her phone, and receive real-time traffic updates about her commute.[3]

For Google LH to function and save information about a user's location, the user must take several steps—some tied to her mobile device, some tied to her Google account. First, the user must ensure that the device-location setting on her mobile device is turned on. When the device-location setting is activated, the mobile device automatically detects its own location, which the device ascertains based on GPS and Bluetooth signals, Wi-Fi connections, and cellular networks.[4] Second, the user must configure her mobile device to share location information with applications capable of using that information. Not all mobile applications can use location information, and those that can, such as Google Maps, will do so only if the user configures her device to allow the app to use the mobile device's location information.

Critically, merely taking the steps described above that are tied to the mobile device does not on its own generate a saved LH record of a Google user's locations. Google does not save information about where a particular mobile device has been to a user's account—even when the device-location feature is turned on and applications on the device are using location data—unless the user has also taken additional specific steps tied to her Google account. Specifically, the user must opt into LH in her account settings and enable "Location Reporting"—a subsetting

[3] *See* Google, *Manage Your Location History*, https://support.google.com/accounts/answer/3118687 (visited Dec. 20, 2019).

[4] Android users can tailor their devices' location-reporting settings, controlling which sources of information (*e.g.*, GPS, cellular, or Wi-Fi) are detectable from the device, and which applications can access location data. *See, e.g.*, Google, *Manage Your Android Device's Location Settings*, https://support.google.com/accounts/answer/3467281 (visited Dec. 20, 2019); Google, *Choose Which Apps Use Your Android Phone's Location*, https://support.google.com/android/answer/6179507 (visited Dec. 20, 2019).

within LH—for the particular device.[5] And to actually record and save LH data, the user must then sign into her Google account on her device and travel with that device. In sum, LH functions and saves a record of the user's travels only when the user opts into LH 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, permits that device to share location data with Google, powers on and signs into her Google account on that device, and then travels with it.

When a user takes those steps, the resulting data is communicated to Google for processing and storage on Google's cloud-based servers, and to enable Google to make it available to the user in various ways. But it is the user who controls the LH information. The user can review, edit, or delete her Timeline and LH information from Google's servers at will. For example, the user could decide to keep LH information only for dates when she was traveling abroad and manually delete the rest; she could delete all Timeline entries except those associated with visits to memorable restaurants; she could instruct Google to automatically delete all LH information after a set period (say, every three months); or she could keep all LH information for future reference.

The user thus controls her Google LH data—unlike, for instance, the CSLI at issue in *Carpenter* or cellular data obtained via a "tower dump." As the Supreme Court explained in *Carpenter*, CSLI consists of time-stamped records that are automatically generated by and for the wireless carrier whenever a mobile device connects to a cell site (*i.e.*, the physical radio

[5] A Google account may be associated with multiple devices. The "Location Reporting" feature within LH allows users to select specific devices on which to enable LH. *See* Google, *Manage Your Location History*, https://support.google.com/accounts/answer/3118687 (visited Dec. 20, 2019).

antennas that make up the cellular network). 138 S. Ct. at 2211-2212. Wireless carriers collect and maintain CSLI records "for their own business purposes," such as identifying weak spots in the network or determining when to apply roaming charges. *Id.* at 2212. When law enforcement seeks access to CSLI, it is thus asking the wireless carrier to produce its own business records showing when a particular device connected to a cell site within a particular period of time. A request for a "tower dump" likewise seeks the wireless carrier's own business records—in that case, identifying every phone that connected to a particular cell site (or "tower") in a particular period.

Mobile device users cannot opt out of the collection of CSLI or similar records, nor can they retrieve, edit, or delete CSLI data. Google LH information, by contrast, is stored with Google primarily for the user's own use and benefit—just as a user may choose to store her emails on Google's Gmail service and her documents on Google Drive. Google LH information is controlled by the user, and Google stores that information in accordance with the user's decisions (*e.g.*, to opt in or out, or to save, edit, or delete the information), including to enhance the user's experience when using other Google products and services. *Supra* pp. 6-8.

Defendant thus errs in asserting that "[i]ndividuals do not voluntarily share their location information with Google," Mot. 10, and that the acquisition of user location records by Google is "automatic and inescapable," Reply 6. As discussed, Google does not save LH information unless the user opts into the LH service in her account settings (and logs into her Google account while using a properly configured mobile device), and the user can choose at any time to delete some or all of her saved LH information or to disable the LH service completely. And LH information was the only location information produced to the government in response to this geofence warrant.

B. Google LH Can Reflect A User's Location and Movements More Precisely Than CSLI And Other Types Of Data

Google LH information can be considerably more precise than other kinds of location data, including the CSLI considered in *Carpenter*. That is because, as a technological matter, a mobile device's location-reporting feature can use multiple inputs in estimating the device's location. Those inputs include not only information related to the locations of nearby cell sites, but also GPS signals (*i.e.*, radio waves detected by a receiver in the mobile device from orbiting geolocation satellites) or signals from nearby Wi-Fi networks or Bluetooth devices. Combined, these inputs (when the user enables them) can be capable of estimating a device's location to a high degree of precision. For example, when a strong GPS signal is available, a device's location can be estimated within approximately twenty meters.[6]

CSLI, by contrast, shows a less-detailed picture of a mobile device's movements. Although its precision has increased as wireless carriers have introduced more and more cell towers that cover smaller and smaller areas, it typically reflects location on the order of dozens to hundreds of city blocks in urban areas rather than a matter of meters, and up to forty times more imprecise in rural areas. *See Carpenter*, 138 S. Ct. at 2225 (Kennedy, J. dissenting); *see also United States v. Beverly*, 943 F.3d 225, 230 n.2 (5th Cir. 2019) ("CSLI should not be confused with GPS data, which is far more precise location information derived by triangulation between the phone and various satellites.").[7]

---

[6] *See* Google, *Find And Improve Your Location's Accuracy*, https://support.google.com/maps/answer/2839911 (visited Dec. 20, 2019).

[7] No estimate is perfect, and the estimated locations reflected in Google LH are no exception. Like any probabilistic estimate based on multiple inputs, the estimated locations reflected in Google LH have a margin of error, so a user's actual location will not always align with any one estimated location data point in LH. 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

C. Collecting And Producing Google LH Information To Law Enforcement In Response To A Geofence Request Requires A Uniquely Broad Search Of All Google Users' Timelines

The Stored Communications Act ("SCA") governs how service providers such as Google handle the contents and records of their users' stored electronic communications, including Google LH. In general, the SCA prohibits unauthorized access to those stored communications, restricts the service provider's ability to disclose them to the government, and delineates the procedures law enforcement must follow—and the substantive standards it must meet—to compel a service provider to produce them. *See* 18 U.S.C. §§ 2701 *et seq.*

Typically, U.S. law-enforcement authorities use legal process (whether in the form of a search warrant, court order, or subpoena) to compel Google to disclose content or records of electronic communications associated with specifically identified Google users or accounts. For example, the government might obtain a warrant for the contents of emails associated with a particular Gmail account. Google often receives warrants for LH information that take the same form—*i.e.*, demands for a specifically identified Google user's LH information from a specifically identified time range. When producing data in response to such a demand, Google must search for and retrieve only the responsive data that is associated with the particular users or accounts identified in the warrant.

So-called "geofence" requests operate quite differently. Geofence requests represent a new and increasingly common form of legal process that is not tied to any known person, user, or account. Instead, law enforcement uses geofence requests in an attempt to identify all Google users who might have stored LH data in their accounts suggesting that they were near a given

---

during a given time period. An LH user's Timeline, however, combines and contextualizes numerous individual location data points, so that the resulting picture of the user's location and movements is sufficiently precise and reliable for the purposes for which it was designed.

area in a given timeframe—and to do so at a level of precision not available through CSLI or similar data.

Such requests typically identify a geographic area surrounding a point of interest. That point of interest is typically a suspected crime scene. As Defendant observes (at Mot. 12-13), however, the geographic area can also include private homes, government buildings, places of worship, and other sensitive locations. A geofence request seeks to compel Google to produce LH information for all Google users whose LH records indicate that they may have been present in the defined area within a certain window of time, which might span a few minutes or a few hours. (In practice, although the legal requests do not necessarily reflect this limitation, such requests can cover only Google users who had LH enabled and were using it at the time in question.)

Many of the earliest "geofence" legal requests attempted to mimic "tower dump" requests, seeking LH data that would identify all Google users who were in a geographical area in a given time frame. In light of the significant differences between CSLI and Google LH data described above, however, Google developed a multi-step anonymization and narrowing protocol to ensure privacy protections for its users. That protocol typically entails a three-step process:

First, law enforcement obtains legal process compelling Google to disclose an anonymized list of all Google user accounts for which there is saved LH information indicating that their mobile devices were present in a defined geographic area during a defined timeframe. Google, however, has no way to know ex ante which users may have LH data indicating their potential presence in particular areas at particular times. In order to comply with the first step of the geofence protocol, therefore, Google must search across all LH journal entries to identify

users with potentially responsive LH data, and then run a computation against every set of coordinates to determine which LH records match the time and space parameters in the warrant.

After Google has completed that search, it assembles the LH information that is responsive to the request without any account-identifying information. This anonymized "production version" of the data includes an anonymized device number, the latitude/longitude coordinates and timestamp of the reported location information, the map's display radius,[8] and the source of the reported location information (that is, whether the location was generated via Wi-Fi, GPS, or a cell tower). The volume of data produced at this stage depends on the size and nature of the geographic area and length of time covered by the geofence request, which vary considerably from one request to another.[9]

Second, the government reviews the anonymized production version to identify the anonymized device numbers of interest. If additional anonymized location information for a specific device is necessary to eliminate false positives or otherwise determine whether that device is actually relevant to the investigation, law enforcement can compel Google to provide additional contextual location coordinates beyond the time and geographic scope of the original request. Here, for example, the government requested a second round of anonymized LH information showing where certain users moved during an extended period of time 30 minutes

[8] Each set of coordinates saved to a user's LH includes a value, measured in meters, that reflects Google's confidence in the reported coordinates. A value of 100 meters, for example, reflects Google's estimation that the user is likely located within a 100-meter radius of the reported coordinates.

[9] *See, e.g.*, Jennifer Valentino-DeVries, N.Y. Times, *Tracking Phones, Google Is a Dragnet for the Police* (Apr. 13, 2019), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html (discussing examples); Tony Webster, Minnesota Public Radio, *How Did The Police Know You Were Near A Crime Scene? Google Told Them* (Feb. 7, 2019), https://www.mprnews.org/story/2019/02/07/google-location-police-search-warrants (same).

before and 30 minutes after the original timeframe. This additional contextual LH information can assist law enforcement in eliminating devices that were not in the target location for enough time to be of interest, were moving through the target location in a manner inconsistent with other evidence, or otherwise are not relevant to the investigation. The government then reviews users' movements, as reflected in the anonymized data, and selects the anonymized device numbers for which it will require Google to produce identifying user account information.

Third, the government can compel Google to provide account-identifying information for the anonymized device numbers that it determines are relevant to the investigation. Typically, the legal request requires Google to provide account subscriber information such as the Gmail address associated with the account and the first and last name entered by the user on the account.

The steps necessary to respond to a geofence request are thus quite different from and far more intrusive than responses to requests for CSLI or "tower dumps." To produce a particular user's CSLI, a cellular provider must search its records only for information concerning that particular user's mobile device. A tower dump is similarly limited: It requires a provider to produce only records of the mobile devices that connected to a particular cell tower at a particular time. But because Google LH information on a user's account is distinct from a mobile device's location-reporting feature, Google has no way to identify which of its users were present in the area of interest without searching the LH information stored by every Google user who has chosen to store that information with Google.

II. THE STORED COMMUNICATIONS ACT REQUIRES THE GOVERNMENT TO OBTAIN A WARRANT TO COMPEL PRODUCTION OF "LOCATION HISTORY" INFORMATION

Although the parties' briefing has focused on the Fourth Amendment, the Court's resolution of the important questions presented here should reflect the entire legal landscape.

Google's storage and disclosure of user data, including LH information, is subject to the SCA, which governs law-enforcement efforts to compel service providers such as Google to disclose data relating to a user's stored electronic communications. *See* 18 U.S.C. § 2703. The SCA generally requires the government to obtain a warrant supported by probable cause to require a provider to disclose the "contents" of electronic communications (such as the contents of an email). *Id.* § 2703(a), (b)(1)(A); *United States v. Graham*, 824 F.3d 421, 437 (4th Cir. 2016) (en banc), *overruled on other grounds*, 138 S. Ct. 2206.[10] By contrast, if the government uses legal process requiring a less demanding showing than probable cause—such as a court order or subpoena—it can generally only compel the production by a provider of basic subscriber information (using a subpoena) and other "records" of electronic communications, such as data indicating when an email was sent or to whom, but without the content of the email (using a court order). *See* 18 U.S.C. § 2703(c), (d).

[10] The SCA draws a distinction between government access to the contents of electronic communications in "electronic storage in an electronic communications system for one hundred and eighty days or less"—for which a warrant is invariably required—and access to the contents of electronic communications in "electronic storage in an electronic communications system for more than one hundred and eighty days" or contents of electronic communications "in a remote computing service," for which a warrant is required unless the government complies with certain notice procedures. 18 U.S.C. § 2703(a), (b). That distinction, which reflected the technical landscape prevailing at the time of the SCA's enactment in 1986, has largely fallen into disuse. The statutory provisions purporting to allow warrantless access to "contents" of communications under certain conditions without a warrant have been held unconstitutional, *see United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010), and the Department of Justice has followed that holding as a matter of policy since 2013 by always using warrants to obtain stored content, *see* H.R. Rep. No. 114-528, at 9 (2016). In any event, Google acts as a provider of both an "electronic communication service" and a "remote computing service" in regard to LH information, and the information sought in this case was in storage for less than 180 days at the time of the warrant, rendering these statutory distinctions irrelevant in this case. *See In re Application of the United States of America for a Search Warrant for Contents of Elec. Mail and for an Order Directing a Provider of Elec. Comm'cn Servs. to not Disclose the Existence of the Search Warrant*, 665 F. Supp. 2d 1210, 1213 (D. Or. 2009) ("Today, most ISPs provide both ECS and RCS; thus, the distinction serves to define the service that is being provided at a particular time … , rather than to define the service provider itself.").

Google LH information is subject to the SCA's warrant requirement because that information qualifies as "contents" of "electronic communications." The SCA defines an "electronic communication" as a "transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part" by an electronic system. 18 U.S.C. § 2510(12). And it defines the "contents" of such a communication as "any information concerning the substance, purport, or meaning of that communication." *Id.* § 2510(8). A user's LH information qualifies as "contents" within that statutory definition. Google's users employ LH to record where they have been and when. In doing so, they "transfer" signals and data to Google, *id.* § 2510(12)—data that Google processes to fill users' Timelines and compile an accurate record of users' whereabouts, among other things. The user's location itself is the "substance" and "meaning" of the data the user transfers to Google, *id.* § 2510(8). The user's locations and movements are the "substance, purport, [and] meaning" of the data transmitted and they fill the digital journal that the Timeline feature provides. Although the contents of that journal are reflected on a map in one's Google account rather than in a written document, the locations and travels recorded therein are fundamentally the contents of the journal, capable of being reviewed, edited, and deleted by the user. Such information is plainly "contents" under the Act.

To be sure, location-reporting data in other contexts is sometimes considered to be "records" of electronic communications (sometimes called "metadata") because it is transmitted incidentally to a user's interaction with his or her mobile device. Sending such location data to a third party, in other words, is sometimes an ancillary byproduct of using a mobile device for other purposes (*e.g.*, to make a call or to find the best route home). That is certainly true of CSLI. As the Supreme Court explained in *Carpenter*, CSLI is generated "[e]ach time the phone

connects to a cell site," which can occur "several times a minute" in order to maintain the phone's function. 138 S. Ct. at 2211; *see also Graham*, 824 F.3d at 433 ("CSLI is non-content information because 'cell-site data—like mailing addresses, phone numbers, and IP addresses—are information that facilitate personal communications, rather than part of the content of those communications themselves.'"). As the Third Circuit has explained, however, location data need not be ancillary to an electronic communication; often, location data "serves no routing function, but instead comprises part of a communication's substance" itself. *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 136 (3d Cir. 2015). The question is whether the location information serves as "dialing, routing, addressing, or signaling information," or whether, as here, such information is "part of the substantive information conveyed to the recipient"—in which case "by definition it is 'content.'" *Id.*; *see also id.* at 137; *In re Certified Question of Law*, 858 F.3d 591, 594 (Foreign Int. Surv. Ct. Rev. 2016) (holding that digits an individual enters on a dial pad after dialing a telephone number, such as a PIN or a bank account number, qualify as content information because they transmit substantive information).[11] When users convey their locations to Google to save and store using the LH service, the data is not performing a "routing" or "addressing" role; it is itself the "substantive information" of the user's communications, 806 F.3d at 137, and thus "contents" for the purpose of the SCA.

Because LH information is "contents" under the SCA, the government must generally obtain a warrant to compel Google to disclose it—just as it would have to do to compel Google to produce the contents of a user's written journals stored on Google Drive. *See* 18 U.S.C.

[11] *See also* Orin Kerr, Volokh Conspiracy, Wash. Post, *Websurfing and the Wiretap Act* (June 4, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/06/04/websurfing-and-the-wiretap-act/ ("the line between contents and metadata is not abstract but contextual with respect to each communication").

§ 2703(a), (b)(1)(A); *Warshak*, 631 F.3d at 288. Thus, regardless of the Fourth Amendment analysis, the government was required to obtain a warrant in this case and to satisfy all the substantive and procedural obligations attending the issuance of a warrant.

III. ABSENT AN APPLICABLE EXCEPTION, THE FOURTH AMENDMENT REQUIRES THE GOVERNMENT TO OBTAIN A WARRANT TO COMPEL PRODUCTION OF "LOCATION HISTORY" INFORMATION

The Constitution also required a warrant in this case. The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const., amend. IV. The Amendment's purpose "is to safeguard the privacy and security of individuals against arbitrary invasions by government officials." *Camara v. Municipal Court*, 387 U.S. 523, 528 (1967). The Fourth Amendment protects people against unreasonable "searches," and governmental action that intrudes upon an "expectation of privacy" that "society is prepared to recognize as 'reasonable'" constitutes a search. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). Because the government's acquisition of Google LH information via a geofence request intrudes upon just such a reasonable expectation of privacy, it constitutes a search for which a warrant is generally required.

Under the traditional *Katz* analysis, Google's users have a reasonable expectation of privacy in their LH information. Google LH information "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'"—what the Supreme Court described in *Carpenter* as "the privacies of life." 138 S. Ct. at 2217 (quotation marks omitted). The Court in *Carpenter* held that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured" through the government's acquisition of cell-site location information. *Id.* The same is true of Google LH information.

The question in *Carpenter* was "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." 138 S. Ct. at 2211. As the Supreme Court explained, access to such records implicates two lines of precedent: one addressing "a person's expectation of privacy in his physical location and movements" and the other "draw[ing] a line between what a person keeps to himself and what he shares with others." *Id.* at 2215-2216. The government's ability to obtain CSLI plainly implicated a person's "reasonable expectation of privacy in the whole of [his] physical movements." *Id.* at 2217. By obtaining historical location data generated by a person's cell phone, the Court explained, the government could obtain "an all-encompassing record of the holder's whereabouts," thus "revealing not only his particular movements" but the most intimate details of his or her life, *id.* at 2217-2218; *see also Riley v. California*, 573 U.S. 373, 403 (2014) ("With all [modern cell phones] contain and all they may reveal, they hold for many Americans 'the privacies of life.'"). And while it was true that cell-phone-generated location information was shared with a third party (the cellular provider), the Court reasoned, that did not diminish users' reasonable expectation of privacy in that information, given that it constituted—in essence—"a detailed chronicle of a person's physical presence compiled every day [and] every moment." *Carpenter*, 138 S. Ct. at 2220; *see also United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) ("GPS monitoring generates a precise, comprehensive record of a person's public movements…."); *United States v. Aigbekaen*, 943 F.3d 713, 723 (4th Cir. 2019) (referring to location history as "unusually sensitive").

The same factors that led the Court in *Carpenter* to find a reasonable expectation of privacy in historical CSLI apply just as forcefully to Google LH information. Google LH information, like the CSLI at issue in *Carpenter* and the GPS data in *Jones*, permits the

government to ascertain where a person has been and when—contravening the person's "legitimate expectation of privacy in the record of his physical movements." 138 S. Ct. at 2217. As was true of the CSLI at issue in *Carpenter*, by compelling Google to disclose LH information, the government can, "[w]ith just the click of a button," access a "deep repository of historical location information at practically no expense." *Id.* at 2218. Such data is remarkably revealing. Like CSLI, Google LH information lets the government "travel back in time to retrace a person's whereabouts." *Id.* In fact, the LH information at issue here is significantly more granular than the data at issue in *Carpenter*. The CSLI at issue there allowed the government to trace a suspect to an area that could have been as wide as four square miles. *Id.*; *see also id.* at 2232 (Kennedy, J., dissenting). By contrast, the information recorded in a Google user's LH information potentially records a person's whereabouts to within a matter of meters. *See supra* p. 10. The privacy interests implicated by Google LH information are thus even greater than in *Carpenter*.[12]

Here, the government argues—just as it did in *Carpenter*—that users have no reasonable expectation of privacy in their Google LH information because such records consist only of data that users have "revealed to a third party." Opp. 9. But the Supreme Court rejected that argument in *Carpenter*, and this Court should do the same here. The so-called third-party

[12] As noted, each individual estimate of a user's location reflected in the LH service has a margin of error, which distinguishes it from CSLI. *See supra* n.7. But that does not undermine the fact that a user has a reasonable expectation of privacy in her location as it is reflected in LH information—especially given that such information draws on data that can be far more precise than is CSLI and is highly reliable in context. At the same time, the margin of error associated with LH data means that the government's effort to use this information for purposes for which the LH service was not designed creates a likelihood that the LH data will produce false positives—that is, that it will indicate that certain Google users were in the geographic area of interest to law enforcement who were not in fact there. That, in turn, means that the potential incursion on privacy is quite significant indeed.

doctrine, as the Court explained in *Carpenter*, traces its roots to *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979)—cases in which the government obtained "business records" of a defendant's bank (in *Miller*) and telephone company (in *Smith*) that revealed personal information about the defendants. In each case, the Court held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," *Smith*, 442 U.S. at 743-744, and concluded that no search had occurred. But the Supreme Court in *Carpenter* conclusively rejected the argument that the doctrine should extend to CSLI. 138 S. Ct. at 2219-2220. For one, the Court explained, "[t]here is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information" collected today by third parties of all kinds. *Id.* at 2219; *cf. United States v. Finley*, 477 F.3d 250, 259 (5th Cir. 2007) (individuals have a reasonable expectation of privacy in the contents of their text messages). For another, the Court reasoned, "the second rationale underlying the third-party doctrine"—voluntary exposure—did not justify the application of the doctrine to CSLI, given that, for multiple reasons, users did not genuinely "share" such data with phone companies. *Carpenter*, 138 S. Ct. at 2220.

Neither of the two "rationale[s] underlying the third-party doctrine" justifies extending that doctrine to the LH information here. *Carpenter*, 138 S. Ct. at 2219-2220. First, it is not the case that Google users have a "reduced expectation of privacy" in LH information. *Id.* at 2219. As described above, LH functions in effect as a daily journal of a user's whereabouts and movements with a potentially high degree of precision. It can reveal when a user was at her home (or someone else's), a doctor's office, a place of worship, a political meeting, or other sensitive locations. The information is far more revealing than the bank records or telephone pen

register information at issue in *Smith* and *Miller*, and users expect that information to remain private. *See supra* pp. 6-10.

Second, as in *Carpenter*, the fact that users voluntarily choose to save and share LH information with Google does not on its own implicate the third-party doctrine, to the extent that doctrine is still viable. 138 S. Ct. at 2220.[13] The Court in *Carpenter* emphasized that "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.* (quoting *Riley*, 573 U.S. at 385). For many users, the same is true of the location-based "services that [cell phones] provide," *id.*—including the ability to track one's own movements and enrich one's electronic footprint with that information. Moreover, unlike the business records of the third-party bank and telephone company in *Smith* and *Miller*, LH information is not compiled "for … business purposes" by the third party, *Smith*, 442 U.S. at 743—the key factor that justified the development of the doctrine in the first place. Rather, it is created and stored at the discretion of the user for the user's own purposes and remains in the user's control. Such relationships are common in the digital age. In *Warshak*, for instance, the fact that individuals transmitted their emails to a third party did not stop the court from finding that those individuals enjoyed a reasonable expectation of privacy in the contents of their emails. *See Warshak*, 631 F.3d at 288 (rejecting the applicability of the third-party doctrine and explaining that "the best analogy" was "cases in which a third party carries, transports, or stores property for another"—cases in which "the customer grants access to the [provider] because it is essential to the customer's interests"). The same is true here.

[13] *See Jones*, 565 U.S. at 417 (Sotomayor, J., concurring) (observing that the third party doctrine espoused by *Smith* and *Miller* is "ill suited to the digital age").

The government alternatively argues that *Carpenter* does not apply because the request here applied to a supposedly small area and a shorter period of time than the CSLI requests in *Carpenter*. Opp. 6-8. But there is nothing limited about a geofence search. As explained, *see supra* pp. 12-13, in order to conduct such a search, Google must search across the records of the account holders who entrust Google with their personal LH information. That is a significant incursion on privacy. Unlike the CSLI requests in *Carpenter*, moreover, which rested on the government's belief that particular suspects were involved in a crime—and which sought information only for those users—when the government seeks LH information via a geofence request, it does not know whose records it is searching for. The result is that the government obtains information associated not only with a specific person of interest whose actions might have given rise to probable cause or at least reasonable suspicion, but for numerous others who happened to have LH information from the area. The government's comparison to a "tower dump" (Opp. 8) fails for essentially the same reasons. A tower dump entails a search of records relating only to those mobile devices that were present in the defined area at the defined time; a geofence request requires a search across all Google users for their LH information. And a tower dump yields data that is significantly less granular than a user's LH.

Ultimately, although the time period covered by the warrant here is shorter than the CSLI requests in *Carpenter*, that distinction does not defeat Google's users' reasonable expectation of privacy. A shorter timeframe could make a dispositive difference when dealing with CSLI or tower dump information because a snapshot of such data, if sufficiently limited in duration, would not result in "a detailed and comprehensive record of the person's movements." *Carpenter*, 138 S. Ct. at 2217. It would reveal only that a particular device was at a particular place at one narrow point in time. But because of its greater granularity and precision, a Google

user's LH information allows the government to reconstruct a "detailed and comprehensive record of [the user's] movements," even if only for an hour or two—something that law enforcement would not be able to do using traditional investigative methods. *Id*. at 2217.

A request compelling production of Google LH information accordingly constitutes a search within the meaning of the Fourth Amendment. Unless an exception applies, the government thus "must generally obtain a warrant supported by probable cause before acquiring such records." *Carpenter*, 138 S. Ct. at 2221.

CONCLUSION

Google takes no position on whether the warrant in this case satisfies the requirements of probable cause and particularity or, if it does not, whether suppression is appropriate. But in resolving those questions, the Court should take into account the complete factual and legal context, and it should hold that both the SCA and the Fourth Amendment require the government to obtain a warrant to compel Google to search LH information via a geofence search. That result is compelled by the statute and the Constitution and the cases applying them. It is also the only result that takes appropriate account of the singularly broad and intrusive nature of a geofence search and the granularity of the intimate detail it produces. Given the capacity of geofence searches to intrude on personal privacy, their use should be supervised by a neutral magistrate and restricted to cases in which the government can establish probable cause.

Dated: December 20, 2019

Respectfully submitted,

/s/ Brittany Blueitt Amadi
Brittany Blueitt Amadi (Va. Bar No. 80078)
Catherine Carroll (Va. Bar. No. 50939; *pro hac vice* pending)
Alex Hemmer (*pro hac vice* pending)
WILMER CUTLER PICKERING HALE AND DORR LLP
1875 Pennsylvania Ave. NW
Washington, DC 20006
Tel: (202) 663-6000
Fax: (202) 663-6363
brittany.amadi@wilmerhale.com
catherine.carroll@wilmerhale.com
alex.hemmer@wilmerhale.com

Counsel for Amicus Google LLC

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.	)	

UNITED STATES' RESPONSE TO AMICUS CURIAE BRIEF OF GOOGLE LLC

The United States of America, by its undersigned attorneys, submits this response to the Amicus Curiae Brief of Google LLC. (ECF No. 59-1.)

ARGUMENT

I. THE DEFENDANT VOLUNTARILY CONVEYED HIS LOCATION INFORMATION TO GOOGLE.

Google confirms that the defendant voluntarily conveyed his location information to Google, even under the demanding standard for voluntary disclosure used by the Supreme Court in *Carpenter v. United States*, 138 S. Ct. 2206 (2018). *Carpenter* held that cell-site information was not voluntarily conveyed to the phone company because it was collected "without any affirmative act on the part of the user beyond powering up," because there was "no way to avoid leaving behind a trail of location data," and because carrying a cell phone was "indispensable to participation in modern society." *Id.* at 2220. Google's description of how its location services function demonstrates that these factors do not apply to the Location History information obtained by investigators here.

First, Google details the multiple steps the defendant was required to take for Google to collect and store his Location History information:

> [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, permits that device to share location data with Google, powers on and signs into her Google account on that device, and then travels with it.

ECF No. 59-1 at 8. Thus, Google's storage of the defendant's location information took far more than him powering up his cell phone: he had to affirmatively opt in multiple times to enable Google's collection and storage of his Location History information.

Second, Google confirms that even after the defendant chose to have Google store his location information, he retained the ability to delete it: "[t]he user can review, edit, or delete her Timeline and [Location History] information from Google's servers at will." ECF No. 59-1 at 8. Thus, the defendant could have avoided having Google store his location information, unlike the cell-site information in *Carpenter*.

Third, Google's description of its location services makes clear that having Google store Location History information is not indispensable to participation in modern society. As an initial matter, Google states that "many of Google's products and services can be used without a Google account." ECF No. 59-1 at 5. Google Search is quite useful, but one need not have a Google account to use Google Search. In contrast, the benefits Google describes from enabling Location History seem minimal. According to Google, these benefits for an account holder include the ability to "obtain personalized maps or recommendations based on places she has visited, get help finding her phone, and receive real-time traffic updates about her commute," as well as "the ability to track one's own movements and enrich one's electronic footprint." ECF No. 59-1 at 6-7, 22. Access to such features is far from indispensable.

In sum, the defendant voluntarily disclosed his Location History information to Google because he opted in to its collection and storage, because he had the ability to edit and delete it, and because its collection and storage by Google is not indispensable to participation in modern society. Google is correct when it states that the defendant "errs in asserting that '[i]ndividuals do not voluntarily share their location information with Google.'" ECF No. 59-1 at 9.

II. THE DEFENDANT HAD NO REASONABLE EXPECTATION OF PRIVACY IN TWO HOURS OF GOOGLE LOCATION HISTORY INFORMATION.

The Supreme Court "has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, 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." *United States v. Miller*, 425 U.S. 435, 443 (1976). This principle did not control in *Carpenter* because the Court concluded that cell-site information "is not truly 'shared' as one normally understands the term." *Carpenter*, 138 S. Ct. at 2220. In addition, *Carpenter* held only that "accessing seven days of [cell-site information] constitutes a Fourth Amendment search." *Id.* at 2217 n.3. Here, the defendant voluntarily conveyed his location information to Google under the reasoning of *Carpenter*, and investigators obtained only two hours of that information, rather than a "comprehensive chronicle of the user's past movements." *Id.* at 2212. Google's disclosure of location information therefore was not a Fourth Amendment search.

Google's arguments that disclosure of two hours of the defendant's location information was a Fourth Amendment search lack merit. Google points out that Location History information is more precise than cell-site information, and it argues that Location History information therefore

implicates greater privacy interests than cell-site information. *See* ECF No. 59-1 at 10, 20. But as the United States explained in its Response Brief, the Supreme Court in *Carpenter* assumed that cell phone location information would approach the precision of GPS, so the greater accuracy of Google location information provides no basis for giving it enhanced Fourth Amendment protection. *See Carpenter*, 138 S. Ct. at 2218-19; ECF No. 21 at 8-9. In *Carpenter*, the Supreme Court found that a cell phone user had a reasonable expectation of privacy in "the whole of his physical movements." *Carpenter*, 138 S. Ct. at 2219. A two-hour interval of location information cannot meet this standard, regardless of the accuracy of individual points within the interval.

Google also argues that a warrant should be required for Location History information because when Google responds to a GeoFence warrant, it must "search across all Google users for their [Location History] information." ECF No. 59-1 at 23. Similarly, it notes that a GeoFence warrant "is not tied to any known person, user, or account." *Id.* at 11. These facts, however, do not distinguish GeoFence warrants from other forms of legal process that do not involve Fourth Amendment searches or require a warrant. For example, tower dumps are not tied to any known person, user, or account, but a tower dump is not a Fourth Amendment search. *See United States v. Adkinson*, 916 F.3d 605, 611 (7th Cir. 2019).

Moreover, service providers commonly review large sets of customer records to produce information in response to appropriately limited legal process. For example, in the traditional telephone context, investigators use subpoenas to identify the people who placed calls to a specified telephone number. Obtaining this information is not a search under *Smith v. Maryland*, 442 U.S. 735, 742-44 (1979), which held that telephone users voluntarily convey dialed phone number information to the phone company. A phone company responding to this sort of subpoena, however, may review call records for all of its customers to find this information. *See Ameritech*

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

Similarly, the United States often uses a "specific and articulable facts" court order issued pursuant to 18 U.S.C. § 2703(d) to compel Google to disclose identity information for subscribers who accessed their Google accounts from a specified IP address during a particular time period. Internet users have no reasonable expectation of privacy in their IP address, *see United States v. Wellbeloved-Stone*, 777 F. App'x 605, 607 (4th Cir. June 13, 2019), so use of this investigative technique is not a search. Responding to such a court order, however, requires Google to review access records for all of its account holders. These examples demonstrate that a service provider's response to appropriately limited legal process does not become a search merely because the service provider must review a large set of records to find the responsive information.[1]

Google further asserts that the defendant retains a reasonable expectation of privacy in Google Location History information because it "is not compiled 'for . . . business purposes.'" ECF No. 59-1 at 22. As an initial matter, however, Google's Brief does not actually claim that Google does not use customer location information for its business purposes. Google states that location information is stored "primarily" for the user's benefit, ECF No. 59-1 at 8, but that formulation suggests that customer location information is also used for Google's business purposes. Google should clarify the extent to which it uses and benefits from customer location information, including both Location History information and any other Google databases that

[1] It would also be possible for Google to create an additional database of Location History information that would obviate its need to review the Location History information of all customers in response to a GeoFence warrant. Google could create a database that indexed Location History information based on its location in some sort of cellular grid. When Google received a GeoFence warrant, it would then need to review only location data from the relevant cell or cells, much like a tower dump. This possibility provides further evidence that producing GeoFence information does not become a search merely because Google reviews a large set of customer records: whether Google's production of GeoFence information constitutes a search for Fourth Amendment purposes should not depend on the internal structure of Google databases.

store location information pertaining to account holders.[2]

Moreover, even Google's limited discussion of its use of account holder location information shows that Google does in fact use that information for a "business purpose." Google compares location information to email, *see* ECF 59-1 at 22, but when an email service provider sends, receives, and stores email, it need not review or use the contents of the email. In contrast, Google's use and analysis of customer location information is essential to the location services it provides. For example, Google acknowledges that it uses account holder location information to provide "real-time traffic updates." ECF 59-1 at 7. This service requires Google to analyze location information sent to it by its customers and share the results of its analysis with other nearby customers. When a business uses information supplied by a customer to provide services, the customer retains no reasonable expectation of privacy in that information. For example, an individual retains no reasonable expectation of privacy in personal financial records shared with an accountant. *See Couch v. United States*, 409 U.S. 322, 335-36 (1973).

In addition, the principle that one retains no reasonable expectation of privacy in information revealed to a third party has never been limited to business records. For example, this principle applies to incriminating statements made in the presence of an informant. *See Hoffa v. United States*, 385 U.S. 293, 413-14 (1966). More generally, the roots of the third-party doctrine long predate *United States v. Miller* and *Smith v. Maryland*. 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). 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,

[2] Google states that "[Location History] information was the only location information produced to the government in response to this geofence warrant," but it does not address whether it stores other databases containing location information. ECF No. 59-1 at 9.

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)). In this case, Google's role is fundamentally that of a witness: Google observed the location of people present at the robbery, and the government called upon it to disclose its observations. Allowing litigants to obtain information from witnesses is critical to the truth-seeking function of the justice system: "[t]he need to develop all relevant facts in the adversary system is both fundamental and comprehensive. The ends of criminal justice would be defeated if judgments were to be founded on a partial or speculative presentation of the facts." *Nixon*, 418 U.S. at 709. It was not a search when Google revealed its observations to investigators.

III. THIS COURT NEED NOT ADDRESS GOOGLE'S INTERPRETATION OF THE STORED COMMUNICATIONS ACT.

This Court need not consider Google's argument that as a statutory matter, the Stored Communications Act ("SCA") requires a warrant to compel Google to disclose location information. *See* 18 U.S.C. §§ 2701-13; ECF No. 59-1 at 14-18. Investigators in this case obtained a warrant for the defendant's location information, and his motion to suppress is based solely on his allegation of a Fourth Amendment violation, not a statutory violation. If the United States ever attempted to compel Google to disclose GeoFence information via a "specific and articulable facts" court order issued pursuant to 18 U.S.C. § 2703(d), Google would then have the opportunity to challenge that order.

Another reason why this Court need not consider the SCA here is because the SCA provides no suppression remedy for a statutory violation. The SCA includes criminal penalties and civil damages for certain types of violations of the SCA, *see* 18 U.S.C. §§ 2701 & 2707, and it further specifies that "the remedies and sanctions described in this chapter are the only judicial

remedies and sanctions for nonconstitutional violations of this chapter." 18 U.S.C. § 2708. Courts have thus held that statutory violations of the SCA do not result in suppression. *See United States v. Guerrero*, 768 F.3d 351, 358 (5th Cir. 2014) ("suppression is not a remedy for a violation of the [SCA]"); *United States v. Smith*, 155 F.3d 1051, 1056 (9th Cir. 1998) ("the [SCA] expressly rules out exclusion as a remedy"). Thus, even if the defendant were to allege a violation of the SCA here, the appropriate focus for this Court would still be the defendant's Fourth Amendment argument.

The United States notes, however, that there is some reason to doubt Google's analysis of how the SCA applies to Google location information. For one example, Google argues that under the SCA, Google location information "qualifies as 'contents' of 'electronic communications.'" ECF No. 59-1 at 16. But Google selectively quotes only a portion of the definition of "electronic communication." Google states: "The SCA defines an 'electronic communication' as a 'transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part' by an electronic system.'" *Id.* (quoting 18 U.S.C. § 2510(12)). Google ignores a potentially significant exclusion from this definition: the definition excludes "any communication from a tracking device (as defined in section 3117 of this title)." 18 U.S.C. § 2510(12)(C). Google elsewhere states that Google's location services give one "the ability to track one's own movements," which suggests that a user who opts in to Google Location History may be using a tracking device. *See* 18 U.S.C. § 3117 (defining a "tracking device" to mean "an electronic or mechanical device which permits the tracking of the movement of a person or object"). If the location information users send to Google is a communication from a tracking device, the location information could not be the contents of an electronic communication. Again, however, because interpreting the SCA is not necessary to resolve the defendant's suppression motion, this Court

should not address the SCA here.

CONCLUSION

Google confirms that the defendant voluntarily conveyed his location information to Google. This Court should deny the defendant's motion to suppress the fruits of the GeoFence warrant.

Respectfully submitted,

G. ZACHARY TERWILLIGER
United States Attorney

By: /s/

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

Nathan Judish
Senior Counsel, Computer Crime and
Intellectual Property Section
Criminal Division
United States Department of Justice

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 10th day of January, 2020, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send an electronic notification of such filing to the following:

Laura Koeing
Office of the Federal Public Defender (Richmond)
701 E Broad Street
Suite 3600
Richmond, VA 23219
Email: Laura_Koenig@fd.org

Paul Geoffrey Gill
Office of the Federal Public Defender (Richmond)
701 E Broad Street
Suite 3600
Richmond, VA 23219
Email: paul_gill@fd.org

Michael William Price
National Association of Criminal Defense Lawyers
1660 L Street NW
12th Floor
Washington, DC 20036
(202) 465-7615
Email: mprice@nacdl.org
PRO HAC VICE

_____/s/_____
Kenneth R. Simon, Jr.
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	)	
	)	
v.	)	**Case No. 3:19cr130**
	)	
OKELLO T. CHATRIE,	)	
Defendant	)	

DEFENDANT'S RESPONSE TO GOOGLE'S MOTION TO FILE AMICUS CURIAE BRIEF IN SUPPORT OF NEITHER PARTY

Okello Chatrie, through counsel, responds as follows to Google's motion to file an *amicus* brief in support of neither party:

INTRODUCTION

On December 20, 2019, Google moved this Court to file an *amicus* brief in support of neither party, ECF No. 59, and included its proposed 24-page brief as an attachment. ECF No. 59-1. Mr. Chatrie recognizes Google's interest in this case and appreciates the additional context that Google presents in its brief. Most of the new information that Google proffers strongly supports Mr. Chatrie's motion to suppress evidence obtained from a "geofence" general warrant, *see* ECF No. 29, including the limitless breadth of the search involved and Google's handling of Location History information as communications content akin to a "virtual journal." *Id.* at 6.

Nonetheless, Google seeks to bolster the degree of voluntariness involved in keeping such a journal, giving the misleading impression that such data collection is always, or even generally, informed and intentional. Furthermore, the information Google has provided is incomplete. The defense has requested in discovery information on the categories of data Google collected, stored, and provided to law enforcement, as well as the specific inputs and algorithms used to produce the

responsive Location History data in this case. Google addresses some but not all of these issues in its brief, seeming to pick and choose what it wishes to address.

Consequently, Mr. Chatrie must object to the Court's consideration of Google's brief without further opportunity to obtain discovery from Google and examine Google representatives capable of providing answers to the legal and factual questions raised by their brief. A thorough understanding and examination of the technology at issue here is essential to the full and fair resolution of the significant constitutional issues raised by this case. Google has already demonstrated its willingness to participate in these proceedings. This Court should require its future participation as necessary to assess to the accuracy of the new facts it seeks to interject, or alternatively, to reconsider the motion to participate as *amicus*.

ARGUMENT

I. Google's Brief Supports Mr. Chatrie's General Warrant & Search Arguments

Google distinguishes the geofence warrant at issue here from other types of law enforcement requests, emphasizing that it requires a uniquely broad search of all Google users' timelines. *See* ECF No. 59-1 at 11. Whereas typical requests compel Google to disclose information associated with a specific user, "[g]eofence requests represent a new and increasingly common form of legal process that is not tied to any known person, user, or account." *Id*. Even so-called "tower dumps" are more limited in scope than geofence warrants. As Google explains, a tower dump "requires a provider to produce only records of the mobile devices that connected to a particular cell tower at a particular time." *Id*. at 14. As a result, the number of people directly affected by a tower dump has an upper limit, *i.e.*, the number of devices actually present in the area. By contrast, a geofence search has no such cap because "Google has no way to identify which of its users were present in the area of interest without searching the [location history] information

stored by every Google user." *Id*. In other words, the initial stage of *any* geofence warrant necessarily entails searching *every* user for whom Google has location history data.

Google's explanation of the search process supports Mr. Chatrie's argument that geofence warrants are unconstitutional general warrants. As Mr. Chatrie contends, geofence warrants are overbroad and lack particularity because they "authorize the search of an unlimited number of people's location data," ECF No. 48 at 4, rendering them unconstitutional from the outset. *See also* ECF No. 29 at 16-24. Regardless of how many devices Google initially identifies—be it 9, 19, or 9,000—the process of doing so is the same: "Google must search across all [Location History] journal entries to identify users with potentially responsive [Location History] data, and then run a computation against every set of coordinates to determine which [Location History] records match the time and space parameters in the warrant." ECF No. 59-1 at 12-13. There is no probable cause to justify such a boundless search, and the discretion it affords to both Google and the government demonstrates a profound lack of particularity. Such a warrant is no warrant at all, but an unconstitutional general warrant. *See* ECF No. 29 at 17-21.

Google's description of Location History information as a personal "journal" further reinforces this conclusion. *See* ECF No. 59-1 at 6. Google states that Location History information is not a "business record" in any traditional sense, but "is essentially a history or journal that Google users can choose to create, edit, and store to record their movements and travels." *Id*. Thus, from Google's perspective, it is akin to email stored on Google's Gmail service or personal documents stored remotely on Google Drive. *Id.* at 9, 17. Google asserts that it "is stored with Google primarily for the user's own use and benefit," *id.* at 9, and as a result, treats it as communications "contents" for purposes of the Stored Communications Act. *Id.* at 16-17.

In this light, Google functions as a trusted bailee of location history information that is created by and belongs to individual Google users. Thus, as Mr. Chatrie contends, his location information is his personal property—his own papers and effects—even though Google may be responsible for collecting and maintaining it. *See* ECF No. 29 at 15; *see also Ex parte Jackson*, 96 U.S. 727, 733 (1878) (finding a Fourth Amendment interest letters entrusted to mail carriers). Google, in turn, owes a duty to Mr. Chatrie to keep his location data safe and not disclose it to others. *See, e.g.,* 18 U.S.C. § 2702(a)(1) and (2) (prohibiting service providers from voluntarily divulging the contents of communications); Google, Privacy Policy (Dec. 19, 2019), https://policies.google.com/privacy?hl=en-US#infosharing (describing the limited circumstances in which Google will disclose user data). As Justice Gorsuch recognized in *Carpenter v. United States*, the Fourth Amendment protects one's papers and effects that are held by a third party through such a bailment. 138 S. Ct. 2206, 2269 (2018) (Gorsuch, J., dissenting) ("Whatever may be left of *Smith* and *Miller*, few doubt that e-mail should be treated like the traditional mail it has largely supplanted—as a bailment in which the owner retains a vital and protected legal interest."). Likewise, Justices Kennedy, Thomas, and Alito all acknowledged that the third-party doctrine should not apply where businesses are the bailees or custodians of records with a duty to hold them for a defendant's use. *Id.* at 2228, 2230 (Kennedy, J., dissenting).

By compelling Google to turn over Mr. Chatrie's location history, the government infringed on his property interest in that data. Such a trespass constitutes a Fourth Amendment search and seizure, just as surely as if the government had searched and seized papers in Mr. Chatrie's hotel room or safety deposit box. *See Stoner v. California*, 376 U.S. 483, 490 (1964) ("[A] guest in a hotel room is entitled to constitutional protection against unreasonable searches and seizures."); *Couch v. United States*, 409 U.S. 322, 337 (1973) (Brennan, J., concurring)

(suggesting that individuals have a reasonable expectation of privacy in the contexts of a safety deposit box).

In this case, however, the government went even further. The geofence warrant here is the digital equivalent of searching every safety deposit box in every branch of a global bank to find one piece of stolen property. Yet any warrant purporting to authorize such a search would be an impermissible general warrant, void as a basic principle of both English common law and the Fourth Amendment. *See, e.g.,* William Hawkins, 2 *A Treatise of the Pleas of the Crown* 84 (Professional Books 1973) (P.R. Glazebrook, ed) ("I do not find any good Authority, That a Justice can justify sending a general Warrant to search all suspected Houses in general for stolen Goods, because such Warrant seems to be illegal in the very Face of it"); *Grumon v. Raymond*, 1 Conn. 40, 43 (1814) (holding that a warrant to search all suspected places, stores, shops and barns in town for stolen goods was an unlawful general warrant). The same principle applies here. Google's analogy to personal journals simply underscores the property rights affected by a geofence request and highlights the impermissibility of a general warrant authorizing the search of all such data.

II. Enabling Location History Does Not Defeat Mr. Chatrie's Expectation of Privacy in His Data

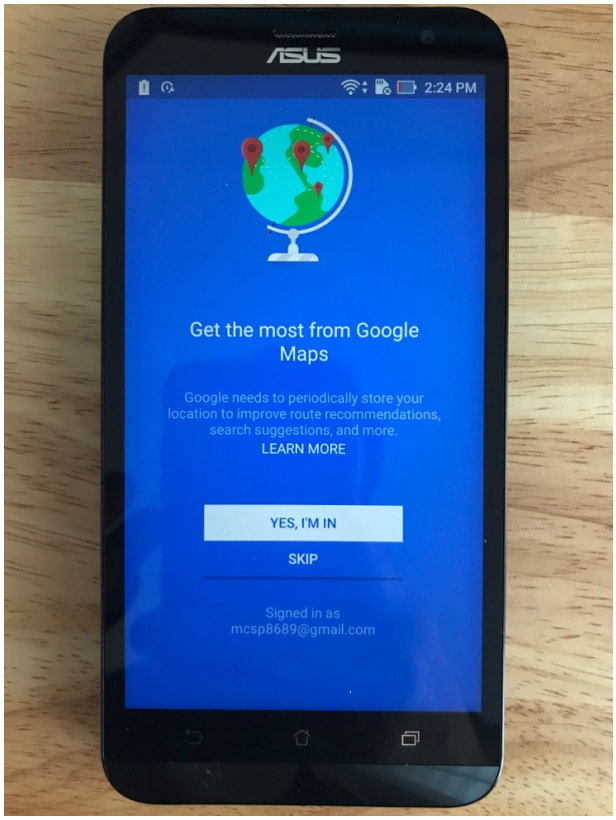
Although Mr. Chatrie appreciates Google's comparison of Location History information to a personal journal, it is not at all clear that it is a journal most people intend to keep. Google points to the account settings users must enable for the Location History service to function, claiming that the defense "errs in asserting that '[i]ndividuals do not voluntarily share their location information with Google,' . . . and that the acquisition of user location records by Google is 'automatic and inescapable.'" ECF No. 59-1 at 9. But in practice, the process for enabling Location History is not nearly as deliberate or informed as Google's brief may lead one to believe.

Google states that Location History will function only when a user takes multiple affirmative steps to enable it. According to Google, a user must (1) opt into Location History as a setting; (2) enable the "Location Reporting" feature; (3) enable the device-location setting; (4) permit location sharing with Google; (5) power on the device and sign into Google; and (6) travel with the device. *Id.* at 8. Yet virtually all of these steps may be accomplished in the first few moments of setting up and using a new device, such as the Samsung Galaxy S9 used by Mr. Chatrie, while the full consequences of doing so would not be apparent the ordinary user.

The Samsung Galaxy S9 is a mobile device that uses Google's Android operating system. As a result, one of the very first steps in setting up an S9 is to log into or create a Google account, the prompts for which appear prior to even creating a passcode for the device. *See, e.g.,* Tech ARP, *Setting Up The Samsung Galaxy S9 For The First Time*, YouTube (Mar. 8, 2018), https://www.youtube.com/watch?v=n-giid2lc_4. While it is possible to skip this step, attempting to do so yields a pop-up warning from Google that doing so will prevent the user from: downloading apps, music, and games; syncing services like Calendar and Contacts; or activating "device protection" features. *Id*. In short, most of the features commonly associated with a modern mobile device, apart from voice calls and web browsing, would be unavailable to an ordinary user who does not log into a Google account. As a result, requirement (5) is quickly satisfied without any reference to Location History. Moreover, the S9 comes out of the box with the device-location setting enabled, satisfying requirement (3). Disabling this setting renders the device incapable of many basic functions.

Requirements (1), (2), and (4) are likely to occur simultaneously when opening an application like Google Maps for the first time. When setting up an Android device similar to the S9, the defense immediately encountered a full screen from Google prompting the user to "Get the most from Google Maps," which states only that "Google needs to periodically store your location to improve route recommendations, search suggestions, and more." A button reading "YES I'M IN" is highlighted while options to "SKIP" and "LEARN MORE" were not.

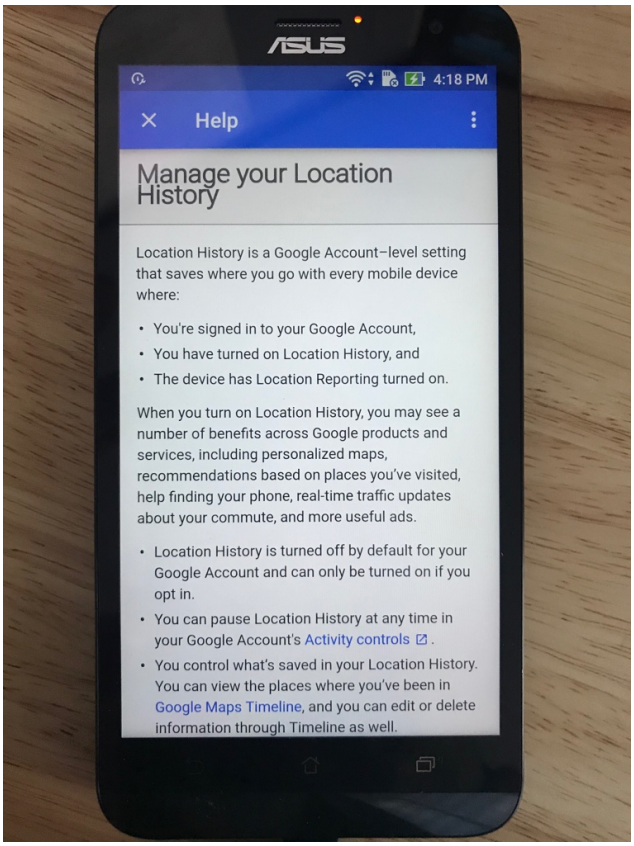
Figure 1



Clicking "YES I'M IN" enabled Location History and turned on Location Reporting, apparently satisfying both requirements (1) and (2), despite the fact that neither Location History nor Location Reporting are mentioned by name. The "LEARN MORE" section informs users that their location information will be reported to Google by enabling Location History, presumably satisfying requirement (4) at the same time. Significantly, there appears to be no way to enable Location History without also enabling Location Reporting and permitting location sharing with Google. In short, requirements (1), (2), and (4) are not independent requirements, but part and parcel of a single click. Consequently, after just the first few minutes on a new Android device like the S9, most users will have accomplished steps (1)-(5)—simply by setting it up, opening Maps, and following Google's prompts. All that remains is to move around in order to satisfy requirement (6).

Critically, the full consequences of taking these initial steps is likely not apparent to the ordinary user. There is nothing in the on-screen prompts to indicate that tapping "YES, I'M IN" will start a log of every step a user takes and share it with Google. It does not mention Location History or Location Reporting explicitly. And while the "LEARN MORE" section mentions "Google Maps Timeline" as a way to "view the places where you've been," it does not elaborate. Instead, Google takes that opportunity to explain why users should enable Location History, stating: "When you turn on Location History, you may see a number of benefits across Google products and services, including personalized maps, recommendations based on places you've visited, help finding your phone, real-time traffic updates about your commute, and more useful ads." When presented with the option in this fashion, it is easy to see how users may enable Location History without realizing the full implications of their decision.

Figure 2



Consequently, Google's description of the opt-in process for Location History does not accurately reflect the user experience, making it appear as if the decision is more intentional and informed than it really is. This raises significant doubt about the degree to which enabling Location History is truly informed and voluntary, as Google's six requirements may be quickly and easily satisfied without any mention of Location History or Location Reporting. Rather, ordinary users

like Mr. Chatrie are very likely to be unaware that Location History is on. Even computer security experts have reported not realizing that the feature had been enabled. *See, e.g.,* Matt Boddy, *The Google tracking feature you didn't know you'd switched on*, Naked Security (Oct. 3, 2017), https://nakedsecurity.sophos.com/2017/10/03/the-google-tracking-feature-you-didnt-know-youd-switched-on/. In this sense, Location History is effectively "inescapable and automatic" for ordinary Google users.

Even if enabling Location History requires a weak affirmative step, Mr. Chatrie still maintains a reasonable expectation of privacy in his data. All cell phone users, for example, must agree to share their cell site location information with the phone company, pursuant to the company's terms of service and as required for the phone to function. But doing so does not waive their Fourth Amendment protection in that data, as the intended scope of that sharing is limited accordingly. As the Florida Supreme Court recognized in *Tracey v. State*, conveying personal information to a third party for personal purposes cannot be considered disclosure for all purposes, especially to parties who were not involved in the transaction. 152 So. 3d 504, 522 (Fla. 2014). Simply because a user knows that the service provider detects his location "for call routing purposes, and which enable cell phone applications to operate for navigation, weather reporting, and other purposes, does not mean that the user is consenting to use of that location information by third parties for any other unrelated purposes." *Id.*; *see also Carpenter*, 138 S. Ct. at 2219 (citing *Riley v. California*, 573 U.S. 373, 392 (2014)). Consequently, Mr. Chatrie had an expectation of privacy in his Location History information that he did not forfeit by conveying it to Google for his personal use.

Finally, Google asserts that it disclosed only an "anonymized" list of user accounts in steps one and two of the geofence warrant process. *See* ECF No. 59-1 at 12-13. But as Mr. Chatrie

argues, "[t]he fact that Google masks the true "Device ID" with a pseudonym does not make the data anonymous." *See* ECF No. 68 at 3. Precise geolocation information is "inherently identifiable," capable of revealing "each person's unique path through life." *Id.*; *see also* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701, 1716 (2010) (compiling computer science research showing that it is possible to "reidentify" or "deanonymize" individuals from ostensibly anonymous data). As a result, the Court should not discount the intrusiveness of the initial data returns disclosed by Google. Had the government obtained the contents of user emails but asked Google to redact the to/from information, there would be no doubt that a search had still occurred. The same holds true for geolocation information.

III. Google's Brief Raises More Questions Than It Answers, Requiring Further Discovery from Google

In moving this Court to participate as *amicus*, Google acknowledges that it is no mere observer. Instead, because of its role in executing the geofence warrant, Google recognizes that it is "well situated to explain the nature of the data and the steps Google takes in response to geofence warrants like the one at issue here." ECF No. 59-1 at 2. In fact, as Mr. Chatrie argues in support of further discovery, Google functioned as "a private actor participating in a specific criminal investigation at the behest of the government." ECF. No. 49 at 2. And as a result, the defense maintains that Google's direct and central role in the search and seizure of Mr. Chatrie's data has made it a part of the investigative team and subject to discovery. *Id*. at 2-3.

By participating as *amicus*, however, Google seeks to pick and choose which information to disclose. Some of the information in Google's brief is responsive to Mr. Chatrie's discovery request. *See* ECF No. 28. But at the same time, some answers are conspicuously absent. Mr.

Chatrie therefore requests that the Court order Google to provide further discovery to the defense or else reconsider its order granting Google's motion to participate as *amicus*.

Clear answers to Mr. Chatrie's discovery requests are material to his defense because "there is a reasonable probability" that if they are "disclosed to the defense, the result of the proceeding [will be] different." *See United States v. Bagley*, 473 U.S. 667, 682 (1985). Under Rule 16, each are material because "there is a strong indication" that each "will play an important role in uncovering admissible evidence, aiding witness preparation, corroborating testimony, or assisting impeachment or rebuttal." *See United States v. Caro*, 597 F.3d 608, 621 (4th Cir. 2010).

A. Sensorvault, Location Services, and Web & App Activity

Two sets of unresolved factual issues about Google's response to the geofence warrant remain unanswered by Google's brief. The first set concerns what categories of data Google collected, stored, and then provided to law enforcement. Mr. Chatrie requested "[d]etails concerning Google's Sensorvault," such as "how the location data is captured and collected," "how often Google collects location data" on Android and non-Android phones, and "how many individuals' tracking information is in the Sensorvault." ECF No. 28 at 2-3. He also requested information on any "data that Google initially determined to be potentially responsive to the warrant" but ultimately excluded." *See id*. at 4. However, Google's brief did not mention Sensorvault or the other categories of location information it collects, such as Web & App Activity. ECF No. 59-1. These facts are material because they illustrate Google's cooperation with law enforcement and speak to the geofence warrant's overbreadth and lack of particularity and probable cause.

Google collects location data from users through several mechanisms, of which Location History is only one—Web & App Activity, for example, is a separate category of location data, as

is Google Location Services. ECF No. 28 at 4-5; ECF No. 48 at 6-7. The geofence warrant required Google to turn over "[d]ata" on "each type of Google account that is associated with a device that was inside the geographical area" described in the warrant. ECF No. 54-1 at 4, 9. The warrant did not limit its reach to Location History information. But Google did, apparently. Google proffers that it limited step one of the search to Location History data, meaning that it did not include location data generated by Web & App Activity or other sources, contrary to the plain language of the geofence warrant. *See* ECF No. 59-1 at 12 ("In practice, although the legal requests do not necessarily reflect this limitation, such requests can only cover Google users who had LH enabled and were using it at the time in question.").

Google, however, provides no support for this assertion or rationale for why it would restrict its search to Location History data, as opposed to including Web & App Activity or Google Location Services. Instead, Google seems to be admitting that it did not fully respond to the warrant based on some sort of internal protocol. In discovery, Mr. Chatrie has requested all such policies, guidelines, and protocols, *see* ECF No. 28 at 2. In fact, Mr. Chatrie specifically requested: "Any and all Sensorvault data that Google initially determined to be potentially responsive to the warrant … but excluded from the Sensorvault data ultimately Google provided to law enforcement officials in this case, including the reason(s) for the exclusion." *Id.* at 4. The defense needs to know, for example, the extent to which this protocol was developed in conjunction with law enforcement. Information indicating that Google worked with law enforcement officials to develop this protocol would support Mr. Chatrie's argument that the geofence warrant granted too much discretion to non-judicial officers in violation of the Fourth Amendment's particularity requirement. *See* ECF No. 29 at 17-24. It also bears on Mr. Chatrie's assertion that Google was functioning as part of the prosecution team. *See* ECF No. 49 at 2-5.

At the same time, Mr. Chatrie should not be required to simply accept Google's unsupported assertion that the geofence warrant searched only Location History information. It is clear that Google collects other types of location information via Web & App Activity and Google Location Services, and the warrant appears to request all of it. But these other functions require even less informed opt-in than Location History, operating even when Location History has been disabled. *See* ECF No. 48 at 7 (Location History "is an opt-in feature but one that has no effect on the GPS, Wi-Fi, and other location data transmitted to Google through Location Services or Web & App Activity."). Indeed, the lack of informed consent to such data collection has been the subject of civil lawsuits in the United States and Australia.[1] Consequently, any location data shared through Web & App Activity or Google Location Services may be even less voluntary than the data obtained through Location History, further supporting Mr. Chatrie's Fourth Amendment arguments.

Similarly, the defense understands that Google maintains all three forms of location information in its "Sensorvault" database. *See* ECF Nos. 28 & 38; H. Comm. on Energy and Commerce, 116th Cong., Letter to Sundar Pichai (Apr. 23, 2019); Jennifer Valentino-DeVries, *Google's Sensorvault Is a Boon for Law Enforcement. This Is How It Works.*, N.Y. Times (Apr.

[1] While the merits of these civil lawsuits are not relevant to Mr. Chatrie's motions in this criminal case, both acknowledged the difference between Location History and Web & App Activity. The Northern District of California discussed how "turning 'off' Location History" does not mean "the places you go are no longer stored" by Web & App Activity. *See* Order Granting Defendant's Motion to Dismiss at 2, *In Re Google Location History Litigation*, No. 5:18-cv-05062-EJD (N.D. Cal. Dec. 19, 2019). "[T]urning 'off' Location History only prevented general location tracking." *Id*. By contrast, the Web & App Activity setting is "'on' by default and saves certain information about a user's 'activity on Google sites and apps.'" *Id*. In short, "the two settings are distinct." *Id*. *See also* Concise Statement at 9, NSD1760/2019, *Australian Competition and Consumer Comm'n. v. Google Australia* (N.S.W. Oct. 29, 2019) (alleging that "where Users had Location History turned 'off' (or 'paused') and the Web & App Activity setting turned 'on' . . . Google obtained and retained Personal Data about the User's location.").

13, 2019); Kate Cox, *Feds Reap Data From 1,500 Phones in Largest Reported Reverse-Location Warrant*, Ars Technica (Dec. 13, 2019), https://arstechnica.com/tech-policy/2019/12/feds-reap-data-from-1500-phones-in-largest-reported-reverse-location-warrant/. Google, however, does not mention Sensorvault or explain how it might segregate Location History data in order to conduct a geofence according to its protocol. Further discovery about the Sensorvault system—such as Google's own description of it, the system's access control and maintenance policies, and how much of which kind of data it contains—is therefore highly relevant and material to Mr. Chatrie's suppression argument. Indeed, the government's case for probable cause relies on statistics citing the number of Android and non-Android users that have their location data stored with Google. ECF No. 41 at 3-4. Mr. Chatrie therefore deserves an opportunity to verify these claims with Google.

B. Wi-Fi Access Point Locations and Google's Algorithms

The second set of unresolved factual issues concerns the inputs and algorithms used to produce the Location History data provided to law enforcement. Mr. Chatrie requested the "location/source" of the "WiFi access points for individuals' location tracking data," ECF No. 28 at 1, which Google did not provide. He also requested the "algorithms used in analyzing and storing the location data," and "all information about the accuracy of the location data," which Google did not provide. *Id*. at 1-3. This information is material because it speaks to the geofence warrant's overbreadth and lack of particularity.[2]

Most significantly, Google appears to have included devices in the step one warrant returns that were actually outside the 150-meter radius authorized by the geofence warrant. In this case,

[2] This information would also help to evaluate the accuracy of the location data, which may become relevant at a later stage in these proceedings. The raw data shows that the margin of error tends to be quite large for the data points based on Wi-Fi. *See* ECF No. 68 Ex. A.

multiple users appear to have been ensnared in the geofence as a result of driving close to, but outside of the 150-meter radius. If true, this fact would strengthen Mr. Chatrie's argument that the warrant was overbroad and lacked particularity. Indeed, that is why the defense requested discovery concerning the location of Wi-Fi access points known to Google, as well as the algorithm Google used to determine which devices were inside the radius and responsive to the warrant.

To wit, Google's brief contains multiple statements that the data points are "probabilistic estimates" with "a margin of error" and include not just a "set of coordinates" but "a value . . . that reflects Google's confidence in the reported coordinates." *See* ECF No. 59-1 at 10, *Id*. n.7, 13 n.8, 20 n.12. Google does not, however, explain how these estimates, margins of error, or confidence values are calculated. It does, however, recognize that these estimates may include "false positives – that is, that [they] will indicate that certain Google users were in the geographic area of interest to law enforcement who were not in fact there." *See* ECF No. 59-1 at 20 n.12.

The most likely explanation for these false positives has to do with the location of the Wi-Fi access points used to determine device locations. *See* ECF No. 49 at 7. "A Wi-Fi access point can be a router, switch, Ethernet cable hub, or some other device that creates a wireless local area network." *Id*. The raw data shows that some of the location data points were based on Wi-Fi but it does not provide the location of the access points themselves. ECF No. 68 Ex. A. This is significant because when locating users, Google's algorithm appears to assume that any device connected to an access point within the 150-meter radius is also located within that radius, equating the location of the access point with the location of the device remotely connected to it. This is a false assumption. A Wi-Fi access point within the radius has its own range, which may extend well beyond the 150-meter radius. *See* Bradley Mitchell, *What Is the Range of a Typical WiFi Network?*, Lifewire (Oct. 28, 2019), https://www.lifewire.com/range-of-typical-wifi-network-816564 (last

visited Jan. 9, 2020) (stating that Wi-Fi networks have an average outdoor range of 300 feet). As a result, devices connected to such a network may be falsely included in the warrant returns even though they were physically outside the geofence.

Even with inputs that Google proffers are "highly reliable in context," Google acknowledges that its algorithm may allow for a large margin of error when locating a user. *See* ECF No. 59-1 at 20 n.12. The resulting location information may still be "sufficiently precise and reliable for the purposes for which [Location History] was designed" (*i.e.,* the commercial context), but not necessarily "for purposes for which the [Location History] service was not designed" (*i.e.*, the law enforcement context). *See* ECF No. 59-1 at 10-11 n.7, 20 n.12; Andrea M. Rodriguez, et al., *Google Timeline Accuracy Assessment and Error Prediction*, 3 Forensic Sci. Res. 240, 245 (2018) (conducting experiment and finding that Google's estimated locations with margins of error have a hit ratio of 52% when using GPS and 7% when using Wi-Fi). Such inaccuracy is not just a trial issue. As Google acknowledges, it makes "the potential incursion on privacy is quite significant indeed." *See* ECF No. 59-1 at 20 n.12.

The only way to evaluate this impact is to look at the specific inputs, including the Wi-Fi access point locations, and the algorithm responsible for determining user location based on them. This information is directly relevant to Mr. Chatrie's overbreadth and particularity arguments, as it would likely show how people outside the 150-meter radius were swept into the geofence.

CONCLUSION

Google's brief supports Mr. Chatrie's argument that the geofence warrant in this case was a general warrant, devoid of the probable cause and particularity required by the Fourth Amendment, requiring suppression the search results and all fruits thereof. But because Google effectively served as a member of the investigative team in this case, and because its brief does

not fully respond to Mr. Chatrie's discovery requests, the defense requests that the Court order Google to provide further discovery to the defense or else reconsider its order granting Google's motion to participate as *amicus*.

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

CERTIFICATE OF SERVICE

I hereby certify that on January 10, 2020, I filed the foregoing with the Clerk of Court using the CM/ECF system, which will send a notification of such filing (NEF) to all counsel of record.

_____/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

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