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)

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

UNITED STATES OF AMERICA	
v.	Criminal No. 3:19CR130
OKELLO T. CHATRIE	January 21, 2020

COMPLETE TRANSCRIPT OF DISCOVERY MOTION
BEFORE THE HONORABLE M. HANNAH LAUCK
UNITED STATES DISTRICT JUDGE

APPEARANCES:

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

Counsel for the United States

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

Michael W. Price, Esquire
National Association of Criminal Defense Lawyers
1660 L Street, NW
12th Floor
Washington, DC 20036

Counsel for the Defendant

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

I N D E X

E X H I B I T S

(The proceedings in this matter commenced at 11:07 a.m.)

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

The United States is represented by Kenneth Simon and Peter Duffey. The defendant is represented by Laura Koenig and Michael Price.

Are counsel ready to proceed?

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

MS. KOENIG: The defense is ready, Your Honor. Good morning.

THE COURT: Good morning.

MS. KOENIG: Your Honor, we are here on defense motion 28, which is the motion requesting discovery and the subsequent briefing after that.

THE COURT: You're going to have to speak up.

MS. KOENIG: I'm sorry. We are here on defense motion 28, which is the defense motion for discovery and the subsequent briefing after that.

The defense has one witness that we will present to help aid the Court in understanding the materiality aspects of the argument that we make related to the discovery requests. His name is Spencer McInvaille. He already has the proposed

exhibits on the bench. I'm sure the Court should have the proposed exhibits on the bench with all but 4 and 5, which are in the witness folder that we'll seek for admission later.

No. 4 and No. 5 are videos. We had initially thought that we would try to activate a cell phone in the courtroom using a wireless hotspot, and that proved to be a little difficult to try to practice for and enact. So what we did instead is we made visual representations in terms of videos. There are two short videos. And No. 4 is the activation of the cell phone that we will play at the same time we're describing with the witness what is happening.

And then No. 5 is the example -- plotting examples of three individuals whose location data was tracked with the geofence warrant data that Google had provided. In that video itself, there are no location coordinates that are disclosed. It does show a map, like a Google Earth map, with plots being pointed, and next to the plots is a date and time, but it does not have location coordinates.

I think it would be next to impossible for anybody in the audience to decipher any exact locations based on that. So we would proffer that the exhibit could be admitted. I should say it's next to

impossible for anybody sitting in the courtroom here today. I think it would be relatively easy for anybody who has unfettered access to that exhibit to figure out the location coordinates. And so we have a proposal, but if the Court would like us to have the entire exhibit published and submitted under seal, we can do that. But I do think that it could be published publicly here in the courtroom, but it would need to be under seal for all the reasons that we had submitted in ECF No. 68, and that the Court had ordered sealed in ECF 69, based on the raw data, because those plots are based on the raw data.

The only other issue before the Court is that both parties have agreed to ask the Court to cross-designate their experts as advisory witnesses. Ours, as I mentioned before, is Spencer McInvaille, and the government may call, in response to Mr. McInvaille, Jeremy D'Errico. And we have no objection, and they have no objection to either being cross-designated as advisory witnesses.

THE COURT: All right. Well, let me ask you first, do you or the government have a position as to whether or not the rules of evidence pertain to this hearing?

MS. KOENIG: I think that the rules of

evidence apply, but because this is relating to the admission of evidence, I think we're seeking -- I guess the purpose of this hearing is for the Court to order whether or not evidence will be disclosed. And so that relates to the admissibility of evidence, which under the rules of evidence operates under a relaxed standard. And so I don't think that, specifically, like hearsay rules would apply. I don't anticipate that that's going to be too much of a problem at this hearing.

THE COURT: All right. I'm going to ask the government to speak, please.

MS. KOENIG: Thank you, Your Honor.

THE COURT: So, first, Mr. Simon, I'd like to ask you to take a position on the defense's proposed course of action, whether you have any objection or different proposal, and I also want you to address whether you think the rules of evidence apply.

MR. SIMON: Judge, no objection to the use of the raw data in this courtroom or the cross-designation of the witnesses as advisory witnesses. And Special Agent D'Errico, we'll bring him in during the testimony of Mr. McInvaille.

With respect to, Judge, the Federal Rules of Evidence, we do believe they apply here, and I think

it brings into sort of the picture here a bigger question, which is whether, at this stage, whether in a motion for discovery hearing we're moving toward where we will be for a suppression hearing in February in terms of some of the testimony that I think will be gleaned here. We'll certainly listen to it, but there may be a relevance objection to a number of the -- some of the testimony elicited here.

I think with respect to the Federal Rules of Evidence, they should apply. And to the extent that they --

THE COURT: Do the rules of evidence apply in a motion to suppress?

MR. SIMON: Yes, Your Honor, I think the rules of evidence would apply here.

THE COURT: In the motion to suppress.

MR. SIMON: In the motion to suppress hearing, yes, Judge.

THE COURT: Well, what do I do, first of all, with the fact that you all disagree about what rules I should be applying?

MS. KOENIG: Your Honor, I'm looking at Federal Rule of Evidence 1101(d)(3), which says that these rules, except for those on privilege, do not apply to the following, and it says "miscellaneous

proceedings such as." And then jumping to the portion that would be applicable here, "The preliminary examination in a criminal case" -- I'm sorry. Not that. But (c) -- I'm sorry. (d)(1), which is the Court's determination under Rule 104(a) on a preliminary question of fact governing admissibility. But this is also a miscellaneous proceeding under (d)(3).

I think under either one of those the Court is looking at evidence in this case in a very preliminary matter, not in terms of finality of what would be presented at a trial or what would be presented in something where a final judgment would be rendered. And so based on those exceptions to when the rules of evidence apply, I think they don't apply, but even if they did apply in some fashion, it would be a very relaxed standard as in the motions to suppress.

THE COURT: Explain to me your position on the standard in the motion to suppress.

MS. KOENIG: Your Honor, and I apologize. I don't have the case in front of me, but I think there is case law from the Fourth Circuit which indicates that in a motion to suppress, because it is governing the admissibility of evidence, that to the extent that

rules of evidence are adhered to in any motion to suppress, they are under a very relaxed standard. I'm sorry I don't have the case cite, Your Honor.

THE COURT: That's fine.

MR. SIMON: Judge, I'll agree with that. I think the -- I was incorrect to the extent that I indicated that they would apply. And certainly to the extent they would, it would be a relaxed standard in terms of the suppression hearing. And here, the bigger point there, Judge, is just with respect to the testimony elicited and its potential relevance here to the motion for discovery. And I think we can get to that point based off of the testimony that they will elicit.

I think it would be helpful, Judge, to kind of note, and maybe for defense counsel, to the extent that they disagree, to put on the record where I think there is agreement at this point with respect to the motion for discovery, which paragraphs have been addressed sufficiently, which are still in dispute, and which relate purely to documents that might be in the possession of Google to the government's viewpoint.

THE COURT: Well, why don't you all discuss that together and see if you can put that on the

record in a stipulated fashion.

MR. SIMON: Okay. And, Judge, I'm happy to say it right now before the Court, and to the extent that defense counsel disagrees, I think some of this has already been put on the record. I just wanted to be clear before testimony was elicited about some of the paragraphs here. So in --

THE COURT: Just a minute. Let me catch up with you.

All right.

MR. SIMON: And so in ECF 28, this is the discovery motion, first, to note which have -- the parties agree have been made sufficiently and where that can be found. Paragraph 6 with relation to the physical access to any and all devices and software, to the extent that that would be provided, the defense agrees on page 1 of their reply that that is sufficient at this stage for their warrant. Same with paragraph 7, copies of the raw data produced and utilized by law enforcement. I think both parties now, obviously, recognize that that's been produced, and I think that's made clear on page 1.

The reply of the defendant, as well as paragraphs 11(a) and (b), that relates to communications concerning the geofence request in this

case, communications with Google, as well as any arrests and investigative reports. I don't believe there were any as it related to that, but to the extent that there were, they were turned over. And so there's agreement as to those three paragraphs.

There could potentially be additional disagreement about paragraph 2 and paragraph 8. So paragraph 2 is the anonymous identifier as it relates to Mr. Chatrie's -- pardon me -- anonymous identifiers provided by Google and its returns. The United States has made clear that that was provided and gave the last four digits of that as it's laid out in the raw returns from Google. It just seems that the defendant was unable to ascertain which account was his, but that number is in the raw data return in paragraph 2. So I believe we agree at this point that they have the anonymous identifier that relates to Mr. Chatrie.

And then for paragraph 8, all information about how law enforcement officials manipulate and analyzed the data in this case to identify the second and third rounds of the search process, there's no documented record of that in terms -- that would be turned over by a *Jencks*, or if there was some other sort of documented piece of that. There will be witness testimony to that point, and certainly to the

extent that it's involved in expert notice, we provided there. But I don't think that there's anything discoverable at this point, documentary evidence as to paragraph 8. Purely, there would be witness testimony. To the extent that our expert was involved in that, it would be certainly provided in the expert notice that the Court has ordered produced on February 3rd, to the extent that that comes.

With relation to paragraph (c), (d), and (e) of paragraph 11, it continues to be the position of the United States that to the special agent who's tasked with or who has a knowledge of those kinds of documents, they are not available. They do not exist. And, again, to the extent that that were to change, we'd provide those documents to the defense.

The remaining paragraphs, paragraphs 1, 3, 4, 5, 9, 10, all relate to documents that we have argued and continue to argue are in the possession, custody, and control of Google for purposes of Rule 16, and to the extent that there would be some sort of *Brady* requirement, Google is not a part of the United States' investigative team in terms of those documents. But, again, we produced everything that Google has provided to us. And so I think that is an accurate and fair lay of the land, but to the extent

that there's some disagreement there, I think defense counsel can inform the Court.

THE COURT: All right. So, I'm just going to make the finding so it's clear on the record that for purposes of this hearing with respect to the rules of evidence, I do think under Rule 1101(d), it is appropriate to apply the relaxed standard similar to that undertaken in a motion to suppress. It certainly makes no sense that it would be harsher than a motion to suppress, and it's quite possible that under some of the provisions in (d)(1), they may not apply at all, but we will address each issue as it comes up.

So I'll hear from the defense as to what is or is not in dispute.

MS. KOENIG: Your Honor, as it relates to paragraph 6 and 7 of document No. 28, we will agree that those have been provided sufficiently and satisfactorily.

As it relates to paragraph 2, which is the anonymous identifier, we still don't have any formal recognition of which identifier is Mr. Chatrie's. I think we have a good idea, but I don't want to foreclose that until we have witness testimony.

Paragraphs eight and eleven, we do anticipate presenting evidence as to why we need those requests

satisfied.

And then, as Mr. Simon indicated, the remaining paragraphs 1, 3, 4, 5, 9, and 10, we will lay a foundation as to why those are material, and then we'll get into the legal arguments about how that applies at this hearing.

THE COURT: All right.

MS. KOENIG: Thank you, Your Honor.

THE COURT: Mr. Simon, I'm sorry to make you bounce up and down, but the defense has provided a witness list and exhibit list. Do you have one?

MR. SIMON: Yes, Judge. I received it this morning.

THE COURT: No. Do you have one for me?

MR. SIMON: No, we do not have an exhibit list, in part because we're not certain we'll call Special Agent D'Errico, and so there's no formal exhibit list.

THE COURT: And no witness list?

MR. SIMON: No witness list, that's right, Judge.

THE COURT: Okay. Thank you.

All right. We can begin the process. And with respect to the pieces of evidence and the video or the ones that are under seal, I am inclined to have

this evidence on the record under seal rather than just having it viewed during the hearing itself. So I grant the motion to seal and place it in the evidentiary record. Does anybody object to that?

MR. SIMON: No objection, Your Honor.

MS. KOENIG: No objection.

THE COURT: All right. I want to be clear that I think for purposes -- I've read your briefing, and I understand that this is meant to elucidate to me the importance of what is or is not discoverable.

I want to be clear that both parties have to be exacting in whether they are talking to me about the Rule 16 standard or the *Brady* standard because they are not the same. And I want the arguments not to blend those standards because it's not helpful to the Court. Specifically, with respect to materiality, it's not the same test.

I also want you all to keep in mind that there is -- I want you to educate me about how I apply these standards. And the specific issue being that the *Brady* standard for materiality is whether it's a reasonable probability that had the evidence been disclosed to the defendant, the result of the proceeding would have been different. Under Rule 16, "materiality" is defined as some indication that the

pretrial disclosure of the evidence would have enabled the defendant to significantly alter the quantum of proof in his or her favor.

Now, obviously, these are both backward-looking tests, and so I want you to educate me about how I apply them forward-looking, because we don't have an outcome. And so I just want you all to be mindful of that as well.

I also need, at some point, for the defense to address the 17(c) argument raised by the United States. It is not addressed at all in briefing, and I think it's relevant, and so that's got to be addressed also.

So those are my preliminary comments.

MS. KOENIG: Your Honor, the defense first calls Spencer McInvaille.

THE COURT: Is there a witness exclusion motion?

MS. KOENIG: Your Honor, if the Court will order that we can cross-designate Mr. McInvaille and Mr. D'Errico as advisory witnesses, we don't need an order of sequestration because there would be no order witnesses presented.

THE COURT: All right. Agreed?

MR. SIMON: No objection to that, Your Honor.

THE COURT: All right. Okay. We'll move forward.

SPENCER MCINVAILLE, called by the Defendant, first being duly sworn, testified as follows:

MR. PRICE: Good morning, Your Honor.

THE COURT: Good morning. Can you place your name on the record?

MR. PRICE: Sorry. Michael Price with the NACDL Fourth Amendment Center for Mr. Chatrie.

DIRECT EXAMINATION

BY MR. PRICE:

Q Good morning, Mr. McInvaille.

A Good morning.

Q Could you please state your full name for the record?

A Spencer McInvaille.

Q Where do you currently work?

THE COURT: Can you spell it, please?

THE WITNESS: Yes, ma'am. It's M-c-I-N-V-A-I-L-L-E.

THE COURT: Thank you.

A I currently work for Envista Forensics. That's

E-N-V-I-S-T-A.

Q What do you do at Envista Forensics?

A I am a digital forensics examiner.

Q What does that entail, generally?

A I deal with various types of location data, cell phone forensics, records from phone carriers, various types of location information, GPS, several different forms.

Q Prior to working at Envista, were you employed?

A Yes. I was a law enforcement officer in Lancaster, South Carolina.

Q What did you do as a law enforcement officer in South Carolina?

A I was a violent crimes investigator. Part of my task was also on the Internet, Crimes Against Children Task Force, as well as mobile phone forensics, and location data examination.

Q Could you expand on that a little bit more? You used location data for what?

A Location data for various things. So investigations of various violent crimes. Also similar types of data for investigations of child exploitation, as well as locating fugitives from our county.

Q Thank you. Do you have any certifications that

are relevant?
A Yes. I hold certifications from Cellebrite for mobile phones forensics, as well as certifications for telecommunications. So dealing with the different networks that we see.
Q Have you had any training dealing with location data and interpreting location data?
A Yes, training in GPS, call detail records, historical records. I believe I mentioned GPS, and then various types of information that we get from Google and various places.
Q Do you recall how many hours of training you might have had?
A Quite a few. Several different classes.
Q Have you been qualified as an expert before?
A I have.
Q How many times?
A I believe 11 times.
Q Do you know what a geofence warrant is?
A Yes.
THE COURT: An expert in what?
MR. PRICE: Sorry.
BY MR. PRICE:
Q You've been qualified as an expert before 11 times. How have you been qualified?

A In mobile phone forensics as well as historical cell site analysis.

THE COURT: And who were the trainings with?

THE WITNESS: Cellebrite, as well as Terracom, and my company as well.

THE COURT: Thank you.

BY MR. PRICE:

Q So, we'll get into the details in a minute. I just want to ask you, generally speaking, do you know what a geofence warrant is?

A Yes.

Q Generally speaking, how does a geofence warrant operate?

A A Geofence request to Google is a request based on an incident occurring, determine that incident's location, and its date and time, and drawing some sort of boundary around that area that you would like searched. That request goes to Google for them to then search the users that could have been in that area at that time and then return that information for it to be analyzed.

Q Is that an iterative process?

A Sir?

Q Does that process take place in more than one step?

A Yes, it does take several steps.
Q How is that different from the usual way that you have seen location data produced?
THE COURT: You're going to have to pull up the microphone a little bit, because you're looking more at him than you are into the microphone. And it's hard for me to hear and I'm sure my court reporter, too.
BY MR. PRICE:
Q The location data in this case, how is that different from location data that you have seen in other cases?
A So, typically, when we're dealing with like historical cell cite information, different requests from Google, those requests are made based on individual users. So we know a certain account or a phone number that we're looking for, and we make a request to the correct company to get those records.
Q Thank you. Have you received any formal training or in-class training on geofence warrants?
A No, sir.
Q Why not?
A That is not available to non-law enforcement.
Q What materials have you reviewed that are related to the geofence warrant in this case?

A We have the returns from Google, the amicus brief from Google, the emails and correspondence between the detective and Google. I believe that's it.
Q Anything else? The warrant?
A Oh, as well as the search warrant. Excuse me.
Q What sort of experience do you have with Google's public-facing policies, their privacy policy?
A Just what you can find available on their website.
Q What is your past experience with Google's location data production? Is this typical?
A I have seen both geofence responses as well as account-specific responses.

MR. PRICE: Your Honor, at this time I'd like to tender Mr. McInvaille as an expert in the field of digital forensic examinations, mobile forensics, and cellular location analysis.

THE COURT: No objection, correct?

MR. SIMON: No objection, Your Honor.

THE COURT: He will be deemed an expert.

MR. PRICE: Thank you, Your Honor.

BY MR. PRICE:
Q I'd like to ask you some questions now specifically about Google and what Google provided to law enforcement in this case. How does Google say it categorizes different types of location data it

obtains?
A As far as Google, they classify them differently. They have Google location services, your web and app activity, as well as Google location history.
Q And can you tell us briefly what each one of those is? What is Google location services, generally speaking?
A So, Google location services is a service through Google that uses their various systems through your device to locate you so that you can navigate around town, find restaurants, all of the conveniences that we find in our devices.
Q And what about web and app activity?
A So web and app activity also track similar items. So searches, the things that you do within your apps. Those items are used and tracked across platforms with Google to, again, enhance the user's experience.
Q And then there's a third category, location history. What is that, generally?
A So, location history is essentially a kind of gathering of those pieces of information stored so that your device and your account can better aid you in finding relevant locations that you would want to use, as well as being able to keep the data that you generate.

Q Thank you. I want to ask you to turn to what's been marked as Exhibit 1 in your folder there. Do you recognize the document?
A Yes, affidavit for a search warrant.
Q And is that the search warrant you reviewed in this case?
A Correct.
MR. PRICE: I'd like to introduce that into evidence as Exhibit 1.
THE COURT: Any objection?
MR. SIMON: No objection, Your Honor.
THE COURT: It's entered.
(Defendant's Exhibit 1 is admitted into evidence.)
BY MR. PRICE:
Q Could you read the first bullet point, page 2? I'm sorry, the second bullet point, the first full sentence beginning with "for each type."
A I'm sorry. I'm not picking up where you're at.
Q It's marked page 2. It's actually page 4 of the PDF.
A Gotcha. So, the second bullet point?
Q The second bullet, first sentence, please.
A "For each type of Google account that is associated" --

THE COURT: Sir, it's human nature, if you're reading something, to speed up, but our court reporter needs to get every word. So just read it as if you were saying it, not as if you are reading it. It happens all the time.

A I understand. That's all right.

"For each type of Google account that is associated with a device that is inside the geographical area described further and attachment to 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. The anonymized information will include numerical identifier for the account, the type of account, time stamp location coordinates, and the data source that 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."

Q I just want to call your attention to the first sentence there. It says "for each type." So what types of location information did this warrant ask Google to produce?

A Each, all, is what it appears to be.

Q What would that mean to you? "Each" meaning?
A Anything that Google retains as far as accounts with location that they can search.
Q Would that include the three types of location data that we just talked about?
A Correct.
Q I want to ask you to turn to Exhibit 2 in your folder there. Do you recognize that document?
A Yes, the Google amicus brief.
Q And that's the brief that you reviewed in this case?
A Correct.

MR. PRICE: Your Honor, this is already a part of the record, ECF No. 59-1. We don't seek to introduce it as evidence here but just to mark it as Exhibit 2 for purposes of this hearing.

THE COURT: All right. It will be marked. No objection, correct?

MR. SIMON: No objection, Your Honor.

(Defendant's Exhibit No. 2 is marked for identification purposes.)

BY MR. PRICE:
Q Would you turn to page 12 of that document for me and read the last sentence of the first full paragraph in parenthesis?

A "In order to comply with the" --
Q It begins with "in practice."
A Excuse me.
Q The last sentence of the first full paragraph.
A The first full paragraph. Excuse me. "In practice, although the legal requests do not necessarily reflect this limitation, such requests can cover only Google users who had location or LH, location history, enabled and were using it at the time in question."
Q Just so we're clear, what does LH stand for?
A Location history.
Q Okay. And so what is Google saying there?
A It's saying the request can only cover Google users who had location history enabled.
Q So they're saying they only produced one of the three categories?
A Correct.
Q All right. I want you to turn now to what's marked as Exhibit 3 in your folder.

MR. PRICE: And this, Your Honor, should be published only to the Court. It's under seal.

THE COURT: All right. So that will be published just to the Court and the parties under seal.

BY MR. PRICE:

Q Do you recognize the document?

A Yes.

Q What is it?

A It is the Google returns from Google, the returns.

Q And these are the raw data returns that you reviewed in this case?

A Correct.

MR. PRICE: Your Honor, these are marked as Exhibit A attached to document 68. We would like to mark them as Exhibit 3 here.

THE COURT: All right.

MR. SIMON: No objection.

THE COURT: Thank you. They will be marked as Exhibit 3 and entered under seal.

(Defendant's Exhibit No. 3 is marked and entered under seal.)

BY MR. PRICE:

Q So tell us what you see at the beginning of the raw data provided here. What types of location data did Google produce?

THE COURT: You're going to have to direct the Court as to what page you're looking at, at least. Somehow identify it.

MR. PRICE: Excuse me, Your Honor. It's page

6 of the PDF itself. I don't believe they have page numbers. It's the first page with data on it.

A So, this is the location history for various device IDs.

BY MR. PRICE:

Q How do you know that it's location history?

A It has locations, and this is what we typically get in return.

Q Does it indicate the source of the data here?

A It indicates what the measurement was taken from, as far as Wi-Fi or GPS.

Q Does it say whether it was data obtained from Google location services or web and app activity or location history?

A It does not.

Q So it doesn't say what type of -- as far as Google is concerned, not GPS or Wi-Fi, but the types of categories of data that we talked about before, it doesn't indicate that here?

A Correct. It doesn't specify the Google category that this falls into.

Q Why?

A I'm not sure.

Q How is that different from Google location data produced to you in other contexts that you've worked

on before?
A So, typically, if you were to see a return for a specific account, for one, the document is named by the user's account name as well as the user name, location history, and then the file type.
Q So it would indicate location history, for example, if it was produced from location history data?
A That's correct.
Q Do you know why Google doesn't do that here?
A I'm not sure.
THE COURT: Wait. When you say "typically," what do you mean? Typically, when you're just looking at a known account or typically when you're not looking at a known account?
THE WITNESS: When you are looking at account-specific requests, that's how it is shown.
THE COURT: Okay.
BY MR. PRICE:
Q So Google didn't indicate location history, but they said they did only location history. Do you know why they would have produced only location history data?
A No, I do not know.
Q Do you know why they wouldn't have produced web

and app activity data?
A I don't.
Q Do you know why they wouldn't have produced Google location services data?
A I'm not sure.
Q Why don't you know?
A There's not an explanation of why.
Q Would --
THE COURT: Not an explanation of why on the document, is that what you mean?
THE WITNESS: Correct, in any of the documents provided.
THE COURT: All right.
BY MR. PRICE:
Q Would Google have policies and procedures about this?
A I'm sure they would.
Q Why do you think so?
A Clearly, something guided them to provide a certain data or search a certain set of data.
Q Have you seen those policies or procedures?
A I have not.
Q What do you think they might tell you if you were to see them?
A I'm sure they would outline the process that

Google has outlined for their analysts who provide data in response to a legal process request.

Q Is that information in the warrant or application?

A The information -- I'm sorry?

Q Is that information in the warrant or application?

A The request?

Q The information that you might learn from looking at the policies and procedures.

A I don't see it in the search warrant, no.

Q And it hasn't been provided to you in any way?

A No, sir.

Q I'd like to talk a little bit now about location history specifically and what's involved in enabling it. In the amicus brief that you reviewed, Exhibit 2 that we've already talked about, Google says that this sort of trademarking is entirely voluntary, citing six steps. Can you tell us what those six steps are on page 8?

THE COURT: Are we back to --

MR. PRICE: We're back to Exhibit 2, Your Honor.

THE COURT: -- Exhibit 2?

MR. PRICE: Yes, Your Honor.

BY MR. PRICE:

Q The bottom of page 8.

A I'm sorry. I'm not seeing it on 8.

THE COURT: The paragraph starts, "The user thus controls her Google location history data, which is LH, unlike, for instance, the CSLI at issue in the *Carpenter* case that the parties have referenced for cellular data."

MR. PRICE: Excuse me, Your Honor. It's my fault. It's the first paragraph on page eight. And it starts on page 7, the last sentence. "Specifically, the user must opt into."

THE COURT: Okay. Make this clear. What do you want him to read from so I can follow you, please?

MR. PRICE: The paragraph starting on page 7 beginning with "specifically."

THE COURT: So it's the middle of the --

MR. PRICE: The last sentence on page 7 going into page 8.

THE COURT: Are you with us, sir?

THE WITNESS: I am.

THE COURT: All right.

A "Specifically, the user must opt into location history in her account settings and enable "Location Reporting," a subsetting within location history, for the particular device. And to actually record and save location history, the user must then sign into

her Google account on her device and travel with that device."

BY MR. PRICE:

Q So Google is saying that this is a fairly deliberative process. Do you agree that enabling location history requires such deliberate choices?

A Yes and no.

Q Can you explain a little more?

A So you do have to make the selection to activate location history. The method in which that typically happens and the way that you see it on the device is through prompts that tell you not that location history needs to be enabled, but that if you opt into certain functions, that it does improve your experience. You do not receive the type of information that would lead you to believe that what you have here contained in location history and what it can be used for is exactly what you're opting into.

Q So did you prepare a demonstration to illustrate this point?

A Correct.

Q All right. Let's talk about what you did. You made a visual presentation of the setup process?

A I did.

Q For an Android phone?

A I did.
Q And the visual presentation is in the form of a video?
A It is.
Q That's 4 minutes and 46 seconds long?
A Yes.
Q And you have that video on a DVD in front of you marked Exhibit 4?
A I do.
Q And you have reviewed that DVD prior to coming to court today and have verified it's the same video you created?
A I have.
Q You marked the DVD with your initials reflecting that?
A I did.
Q All right.

MR. PRICE: Your Honor, I'd like to move to introduce the video as Exhibit 4 and publish it.

THE COURT: Any objection?

MR. SIMON: No objection, Your Honor.

THE COURT: All right. It will be entered.

(Defendant's Exhibit No. 4 is admitted into evidence.)

BY MR. PRICE:

Q Before we get started with this video, I want to ask you a couple of preliminary questions. Is this the same phone that the defendant -- at issue here with the defendant?
A It is not.
Q Why is it not the same phone?
A This is a test device that we have at Envista.
Q Okay. Is it running the same operating system?
A It is an Android operating system.
Q Is it running the same version as the defendant's phone?
A This is running Android 7.
Q So it's one version earlier?
A It is. Android 8, I believe, was the defendant's phone.
Q Have you had an opportunity to compare version 7 and version 8?
A I haven't device to device, but I was able to review articles and literature that I could find between comparing the two, and they're very similar.
Q How did you make that determination?
A In comparison to what I've seen here as well as the various screenshots and things that I was able to find for that setup.
Q So just to be clear, the screenshots for version 8

are the same as version 7, to your knowledge?

A They're very similar, yes.

Q All right. So, let's go through this video. Can you talk us through the steps here on what you've done?

A Absolutely. So, when you first boot the phone up, this is the welcome screen that you would get prior to a phone being set up. So similar to it coming straight out of the box after you purchased it. So you will begin the process.

In this first screen, which is labeled "input method," you're going to --

THE COURT: So, listen. I'm going to ask you all to be very careful about establishing the record. If you're switching the screens you're looking at, you have to stop and be clear the first one is the start-up. Give us a moment to keep up with you. This is the second screen that pops up.

THE WITNESS: Yes, ma'am.

THE COURT: It does pop up or however you access it. So we need to slow down so I can follow you, because I haven't seen this before, and it's helpful for me to be able to be sure I'm absorbing what you're saying.

THE WITNESS: Understood.

A This is the second screen. This is the input method. So we're choosing what type of keyboard and icons that you would see in the -- through the process of setting up the device and then later that you will see in the device.

So here we're going to select that we would like the English keyboard, and we're going to move to the third screen.

Here we have to establish on the third screen an Internet connection so that we can complete the process. So here you will see several steps to complete that process.

Moving to the next screen where we will select the Wi-Fi access point to use to complete the setup.

So we enter the password here for that access point so that we can establish a connection.

THE COURT: To be clear, a pop-up came up prompting the entry of the password.

THE WITNESS: That's right.

A And after that's entered, we will be connected and move to the next screen. In this next screen, we have the terms and conditions for the device itself from its manufacturer. We will see several different terms and conditions, but this is the first relating to the manufacturer of the device.

BY MR. PRICE:

Q Before you go through that, or when you're going through that, can you tell us if that mentions location history or mentions Google, specifically?

A It does not.

So after scrolling through those items and clicking to the next button, you're prompted to either agree or disagree with the terms of service for the device.

THE COURT: Can I ask you a question? Did you go all the way through? How many terms and conditions are there?

THE WITNESS: There are six. That's the extent of them there.

A So now we'll move to the next screen, and it will check the connection for the device and take a moment before it moves to the next screen where we have to make indications or selections on the device.

BY MR. PRICE:

Q While we're doing this, I just want to be clear. The privacy policy for the phone itself, the ASUS policy, can you explain what, if any, relationship that has to Google?

A I did not see a direct relation or mention of Google in that setup.

So, we're finally to the next screen. On this screen it's asking if we have another device to use to set up this new device. So this would be if you want to transfer data and settings from one device to this new device that you're accepting up. Here, since I'm setting this up for the purposes of this and not trying to retain any previous data, I'm going to select "no thanks" and move on to the next selection.

So, again, it's going to run through checking the device for various things that it needs to complete for setup, and we'll move on to the next indication when available.

So, for Android devices to complete the kind of user experience and use all of the functions of the device, Android would like for you to activate or connect a Gmail account to the device itself. So here you can either enter in an existing account or create a new account.

For the purposes of this, we're going to create a new account. After that selection, it will move to a new screen. And on that new screen we will enter a name and some various other information so that we can begin to complete the account creation.

We're moving to the next screen.

THE COURT: I'm going to interrupt you a

little bit. You said the Android would like you to activate through a Gmail account. Is there an option not to?

THE WITNESS: You can skip that function.

BY MR. PRICE:

Q May I follow up on that?

A Yes.

Q What's the consequence of skipping that function?

A You lose much of the functionality of the device where you would go download applications from the app store and many of the other functions --

THE COURT: Are you getting to that later?

THE WITNESS: We did not skip that process. We're setting this phone up as if --

THE COURT: Are you going to testify about how that happens later?

THE WITNESS: About how --

THE COURT: If you don't use Google, what happens?

THE WITNESS: Correct. We can discuss that.

Q Please. So if we don't have --

THE COURT: Go back to the Android account, the screen before. So the person's index finger is covering the word "skip."

THE WITNESS: Correct.

THE COURT: On the screen, it says you can skip it.

THE WITNESS: Yes.

THE COURT: All right.

BY MR. PRICE:

Q In your experience, have you ever received a pop-up message when hitting skip?

A Yes. It does ask you are you sure you want to not set up an account on the device.

Q And it describes some of the features that you might be missing out on; is that correct?

A I do believe so.

THE COURT: Wait. I'm sorry. I got -- say that again, please.

THE WITNESS: That's all right. If you skip the function, it does ask you are you sure you want to skip this function as it may hinder you from being able to use the device to its fullest extent.

THE COURT: All right. What happens if you say you're sure?

THE WITNESS: Then you don't set up an account on that device, and then you aren't able to access things like the application store and other functions of the device that we would all normally use.

BY MR. PRICE:

Q Would you be able to use any Google service at all?

A I still do believe you would be able to use some of the functions of the device.

Q But the Google services in particular without an account?

A I do not believe you would be able to use like Google location services, and things like that, that help with your map functions. Location as a whole in the device would still be available, but many of the Google-related functions would not be available.

Q Like maps?

A Correct.

THE COURT: Anything else? I'm looking for specifics here.

BY MR. PRICE:

Q What about email?

A You would not have your Gmail account attached. There again, you wouldn't be able to access the app store, which is where you --

Q Can you explain what that is?

A Yes. That's where you download the various applications that you would use. So if you wanted to add your bank application or various other

applications that people typically use, you wouldn't have that functionality.

Q So you'd be left with what on the phone? What it came with?

A Essentially, yes.

Q And you wouldn't be able to install any apps from the app store?

A Correct.

Q Or use any of the Google app services?

A Correct.

THE COURT: I'm going to interrupt you again. I'm not an expert in this.

THE WITNESS: That's all right.

THE COURT: So, first off, I know we're talking about an Android because there's an Android at issue. Would this testimony be different under Apple?

THE WITNESS: Yes, it can be.

THE COURT: Do you know whether or not if you don't sign up with a Google account in Apple -- first of all, does it ask you to do that?

THE WITNESS: What? In Apple? No, I think Apple would probably prefer that you didn't use Google services. I think they would prefer that you use theirs.

THE COURT: Just making it clear.

THE WITNESS: But you can add Google services to your iPhone.

THE COURT: All right. And I want to be clear about -- you testified earlier about the system. So, this is an Android phone.

THE WITNESS: Yes, ma'am.

THE COURT: And is this the same kind of phone that Mr. Chatrie is alleged to have carried?

THE WITNESS: No, it's not the same device.

THE COURT: Why are they comparable?

THE WITNESS: They are running Android software.

THE COURT: Okay.

MR. PRICE: Perhaps I can ask a few questions to clarify, Your Honor.

THE COURT: All right.

BY MR. PRICE:

Q The current version or the phone that the defendant had was the Samsung S9; correct?

A Correct.

Q Did you purchase an S9?

A We did.

Q When you go through this process, what operating system does it load up?

A It loads with Android 9.

Q Is Android 9 significantly different from Android 8?
A It seemed to be. Between 7, 8, and 9, 9 seemed to be much more different than the comparison of 7 to 8.
Q And with 9, again, which is not at issue here, did you find that some of the information about location services was different?
A It does. It prompts differently, but you still end up with the same prompts for location services and location history.
Q Would a normal user who purchases an S9 today be able to downgrade and load the previous operating system through the normal process of setting up the phone?
A Not through the normal process. It's -- I mean, it's not terribly complicated, but it's not something that you would typically see from the average user.
Q You had to download special software from the Internet to even give this a try; is that correct?
A Yes. You would have to download the old firmware version and load it to the device.
Q When you attempted to do that and reboot the phone, what happened to the operating system you installed?
A On that device when you provide it with the old

software, it still wants to, without a connection or with a connection, still pushes towards that Android 9 interface and its functionality.

Q So, would it be fair to say that one of the reasons we used a different phone and a different operating system here is because it is the most comparable to the system and the phone at issue in this case?

A Between what I worked on, yes, it was more comparable.

THE COURT: And there's no material differences between the terms and conditions of this example and what Mr. Chatrie is alleged to have had?

THE WITNESS: That would be hard to speak to just because how often Google can change the terms. So at the time, across platforms, the terms would be the same as they come from Google, and through that Internet connection is where you're receiving those. So they seem to be, across platforms, the exact same terms and policies that come from Google. Most are dated with their release time.

THE COURT: Okay.

BY MR. PRICE:

Q You said -- you mentioned seeing articles that describe the setup process in version 8. Did those

have images of the setup process?
A They did.
Q Were they the same as the ones in version 7?
A Yes, they looked very similar.
Q Were both of those different than the information about location history provided in operating system 9?
A The materials are the same. It doesn't look different, but it's the same request and prompt from Google.
Q Thank you.
MR. PRICE: Your Honor, do you have any more questions before we proceed?
THE COURT: No. Thank you.
MR. PRICE: Okay.
A So we're going to go back into the setup process here. We're just creating the account by providing a name. After you provide the name, it will move on to the next selection.
On the next screen, it provides -- it wants you to provide a date of birth. That's typically for the play store so you can determine what you're going to download if it's appropriate.
THE COURT: Just to be clear, that screen was entitled "Google Basic Information."
THE WITNESS: Correct.

A And after that selection has been made, it moves to the next screen, which is "choose your Gmail address." It provides two selections that it created as well as a selection where you can create your own. I just opted to use one of the already generated addresses.

And it moves to the next screen where we'll now input -- and it prompts you to create a password for your account.

BY MR. PRICE:

Q In your expert opinion, is password 1-2-3 a strong password?

A It's a terrible password.

After you enter your password and confirm it, it will now prompt you to the next screen.

This next screen would like you to add a phone number to the account. It explains that there are several different reasons you would use this; to reset your account, receive messages, as well as make Google services relevant to you. And there's a scroll down here to add other -- to kind of further explain some of those -- what can be used and how you can use it.

Q To be clear, does this mention location history?

A It does not. And you can either skip, you can say yes, I'm in, and add a phone number, and then there's

also a "more options" selection. So I'm going to select "more options" here.

So it just takes you to the screen to give you the three different choices that you have here. You can not add your phone number, you can add your phone number with all of the features, or you can add your phone number only for security reasons. I did not add a phone number and moved on to the next screen.

Here it's going to show you your account name, your name, and you can select "next" to continue with the process.

THE COURT: The title of that screen is "Review Your Account Info," the new screen.

THE WITNESS: On the next screen after moving on, this is Google privacy and terms. Here is where it explains out and has all of the links to the various websites or web addresses within Google where you can read all of the terms and conditions for various -- the account itself, for like Google Play as well as the privacy policy.

This goes down quite a -- it has quite a bit of information contained within it as well as several links to Google's website with pages upon pages of information about their privacy policy.

BY MR. PRICE:

Q Just to be clear, does this screen say anything about location history?

A It doesn't yet. There is various information down this screen. You can still choose not to create the profile that you have begun to create. You can simply agree now and move on or you can select "more options."

Under "more options," we now get into some of the information that we spoke about earlier that Google has as far as their services, starting here with web and app activity.

Q Is there a default setting for that?

A The default setting for web and app activity there is the affirmative already. So it would be for you to deselect that if you didn't want that selection within the Google services.

The next being "add personalization." It is, as well, in the affirmative selection. It, again, would be up to you to deselect.

"YouTube history," the same. It is in the affirmative to save your Google or your YouTube history into your Google account.

And then, finally, "Google location history" being the final selection on this page. Out of that group, it is the only one that is not currently selected. It

would be up to you to opt into the Google location history at this time.

Once you get down to the bottom again, you still have the choice to not create the account or you can agree and move on with the account.

I'm going to press "agree," and move to the next screen. Again, it's checking the device. "Checking info" is what it displays, and you have to wait until the next prompt.

The next prompt is labeled "Google Services." It says you can turn on or off any service for the following account. And then it goes through and advises the different services, again, that you can turn on or off.

You'll see "automatically backup data" is in the affirmative position. "Google location services," again, affirmative. "Improve location accuracy," it is also selected. And "improve your Android experience," it is also selected.

"Keep me up to date," meaning receive emails about Google, is in the affirmative. And then if you agree, you can move to the next or deselect any of those.

It's going to ask to set up payment information on the next screen. You can choose to set it up or not. We said "no thanks" and continued. Again, checking

the device and waiting for the next prompt.

The next is for you to confirm the date and time for the device to be used, and we will select "next."

And then to this next screen it is "protect your phone." This is where you would enable a pass code or some kind of lock on the device to protect the device.

Q May I pause here, Spencer?

A Yes.

Q Sorry. Mr. McInvaille.

Prior to this step where you're setting up the pass code, can you tell us which of the three categories of location history have been enabled by default?

A So no location history has been activated, but location services and Google location services, as well as web and app activity are selected at this point.

Q And a user who's going through this process would see "location history" was turned off?

A Correct, if they opened the "more options" tab to see that.

So, moving on. I'm not going to set up a pin to the device. Then it's asking us to wait another second. It also then, on the next screen, says "review additional apps." It asks if you would like

to add these three other Google applications immediately to the device upon setup. Just due to them automatically downloading and updating, I selected that they not be downloaded. And we pressed "okay."

These final screens are referring to registering your device with the manufacturer, which is ASUS in this case. You can either create an account using an existing account or skip this function.

Moving to the next screen, still dealing with the ASUS account, whether or not you want to register, sign in, or register by Google ID, or you can skip.

On the next, it determines what data --

THE COURT: To be clear, you didn't undertake any of those options?

THE WITNESS: No, ma'am.

THE COURT: All right.

THE WITNESS: Those functions are not directly related to Google.

THE COURT: Okay.

A The next is accounts and sync for you to determine what accounts you would like to sync across your accounts.

THE COURT: Just so the record is clear, just say some of the stuff that's on the screen, please.

So back up, please.

THE WITNESS: Okay.

A So, on the screen you can add another account, you can sync data across your ASUS account, your exchange or email, as well as the application called Flickr, or your -- or the Gmail account that's selected here, and it is already preselected with the check to sync data for that account as you set it up.

Moving forward, it provides you with a prompt on the next screen for Google drive. It's a promotion to get storage from Google for your various information. We can skip this offer and move to the next screen.

We're finishing up the setup. This is where it tells you your device is now ready and you can make changes to your configurations in the settings area of the device. We'll click the check and move on to the next screen.

And the next screen is where it launches the device as you would normally see it as you were using it throughout the day.

Q So this is the normal setup process at this point. You've got a phone that you can use?

A Yes.

Q What happens when you click on Google Maps for the first time?

A So we've now made all of the selections to set up, and now we go to use the device. Here, once these initial pop-ups are done telling me kind of how to use my new phone, I'll go in and select Google Maps, which is an application already on the device.

Q Does it bring up a map immediately?

A It does not. So you will see the prompt here for "get the most out of Google Maps." It says that Google needs to periodically store your location to improve route recommendations, search suggestions, and more. You can opt in or skip.

Q What are the options? When it says opt in, it says what?

A "Yes, I'm in."

Q And the text, does any text on this screen mention location history?

A It does not.

Q So prior to this setting up the phone, we did see a screen with location history, and it was marked as --

A It was turned off.

Q It was off. And your understanding is that if you hit "yes, I'm in," what happens?

A Yes. If you select "yes, I'm in," it turns on Google location history.

Q And it doesn't mention location history in the text on this screen?
A It does not.
Q What happens when you click on "learn more"?
A It's a hyperlink to Google's website where all of the terms and conditions are located.
Q The entire privacy policy?
A All of the terms and conditions.
Q It doesn't direct you to anything specifically about location?
A No, but it is -- you can find it in there. It's there.
That's the end of the video.
Q So that is the end of the video?
A Yes.
Q Can you tell us, how long is that video? How long did it take you, the entire process, from start to finish here?
A Without stopping, 4 minutes and 45 seconds.
Q How many screens mention location history?
A I believe one.
Q And that was only if you clicked on "more options" and scrolled down; correct?
A Correct.
Q How many of them fully explained what location

history is?
A You would need to -- none. You would need to go look at the policies and terms.
Q Thank you.
So, the government says that we can function in modern society without enabling location services like this. Tell us, how did you get here today?
A I used my phone.
Q You were driving?
A Correct.
Q You used your phone to get directions?
A I did.
Q Did you look up where the courthouse was online?
A I did.
Q Did you plug it into Google Maps?
A Waze. Just about the same thing.
Q You didn't use a road map, did you?
A I did not.
Q Out of curiosity, when was the last time you used a road map?
A It's been quite some years.
Q You're a forensic examiner. You examine a lot of phones; correct?
A Correct.
Q How frequently do you encounter devices that are

also used for Google Search?
A Most.
Q What about Google Maps?
A Most.
Q What about Gmail?
A Very often.
Q And YouTube?
A Quite often.
Q How common is it for you to encounter phones with location services enabled?
A Pretty often.
Q What about location history, specifically?
A Typically, that's a hard function to see activated. It's not something you typically go seek out on the device to see if it's turned on. But based on the different returns that I see for Google account-specific requests, as well as these geofences, it's clear that a lot of people have this function activated on their devices because of how they show up in these returns.
Q Do you know what percentage of all devices use Google services?
A No, I don't.
Q Who would know that?
A I'm sure Google would.

Q Do you know --

THE COURT: I'm sorry. Say that again.

THE WITNESS: I said I would be sure that Google would know how many devices use their services.

BY MR. PRICE:

Q Do you know what percentage of devices have location history enabled?

A I don't.

Q What about web and app activity?

A I don't.

Q What about Google location services?

A I don't.

Q Who would know the answers to those questions?

A I would be certain that Google would have statistics on their services being used.

Q Thank you.

I want to turn now to the scope of the geofence warrant here.

THE COURT: Before you get there, if you enable YouTube or Google Search when the default has gone to location history off, do you get any kind of pop-up? Does it change the default?

THE WITNESS: So, across the platform for location history, it's my experience that that prompt comes from Google Maps, but there are certain, as far

as YouTube and things like that, other prompts for them to want to track the web and app activity and things like that that all fall into those categories that Google explained earlier or have explained in their brief.

THE COURT: But I'm asking specifically about location history.

THE WITNESS: So, no, they do not -- I have not seen them promote location history.

THE COURT: Do you know whether or not the default changes?

THE WITNESS: No, I do not.

THE COURT: You don't know?

THE WITNESS: I do not.

BY MR. PRICE:

Q When you were reviewing information about Android version 8 and you came across screenshots of the various prompts here, we saw one that looked just like this; right?

A It's the same screen, besides the sign-in information at the bottom with your account.

Q Were there other prompts that you discovered in your research that trigger location history enabling, such as when you go to photos, my places, for example?

A Nothing that directly activated location history.

Q In the sense that they didn't mention it specifically here?
A Correct, it's not mentioned as location history.
THE COURT: Is it activated?
THE WITNESS: It does activate the sharing of location data for that application but not directly linking the activation of Google location history to that selection.
BY MR. PRICE:
Q I want to turn to the scope of the geofence warrant and the question of whether it was really limited to 150 meters. How big was the geofence here, according to the warrant?
A I believe it was 150 meters.
Q I apologize for making you do math, but do you know what area that is in terms of square meters?
A I don't think I looked up square meters. I sometimes look it up on Google just to figure out how large of an area it is.
Q Would it surprise you if it was 70,686 square meters?
A No, that wouldn't surprise me.
Q Do you have an idea what that translates into in terms of acres?
A I did try to look it up in acres. It's about

17 acres.
Q Did the bank take up all 17 acres?
A No, it didn't.
Q What else was inside that radius?
A There was a parking lot -- well, a large parking lot, a church, and I believe the back of a hotel or very close to the parking lot and one side of the hotel was also encompassed in that circle.
Q I'd like you to return to Exhibit 3, that raw data on the spreadsheet there. Go to the same page you were on before, which is page 4 of the PDF itself.
A Okay.
Q Take a look at column F.
A Okay.
Q What's the label on column F?
A "Source."
Q What does that mean?
A It is telling you what type of calculation was made. So here it displays either Wi-Fi or GPS was used to provide a location.
Q So those are the two sources of location data at issue here?
A That is provided in the data, yes.
Q Do you know how many data points came from Wi-Fi here?

A There were quite a few. Probably out of the data, I believe over 600.
Q Would it surprise you if it was 605?
A No.
Q Okay. And that means how many came from GPS?
A There were quite a few. It was more than 60 or 70, I believe.
Q Would it surprise you if it was 75?
A That sounds about right.
Q So the percentage of the initial geofence warrant -- the percentage of the initial geofence returns that came from Wi-Fi, what would that be?
A Over 80 percent.
Q Would it surprise you if it was 88 percent --
A No.
Q -- coming from Wi-Fi?
Okay. Which is more accurate, Wi-Fi or GPS?
A GPS.
Q So based on your training and experience with Google location data in other cases, can you tell us, generally speaking, how Google uses Wi-Fi to locate somebody?
A Yes. So the phone is constantly scanning for Wi-Fi access points, so a router. It's constantly scanning and seeing the signal strength from those

access points. Based on the signal strength and Google doing a lot of work to understand where each of those access points is, they can generally understand where you are located based on several points, giving a specific distance to that point. So, several of those put together helps determine a location for the device.

Q Is it possible, because this data is coming from Wi-Fi with its own range, that the step 1 returns here included devices that were actually outside of the 150-meter radius?

A Yes.

Q Why? How does that work?

A So, of course, the signal coming from the Wi-Fi routers isn't bound by that arbitrary circle that's drawn. They can spill out farther. Google doesn't know the exact position of every Wi-Fi access point. So if it's off by where it thinks the access point is, that provides kind of an error in accuracy as far as where it thinks it is. So if the access point reaches out farther, it could think that the phone was in the circle if it saw that access point versus being outside.

Q What's the typical range of a Wi-Fi network?

A About 150 feet is kind of a general estimate.

Q So, how far outside the radius might the initial search have reached? Twenty-five meters?
A It possibly could have, yeah.
Q Fifty meters?
A Possibly.
Q So, step 1 can actually include devices that are up to 50 meters outside of that radius. Do you know what the effective reach, the effective area, of the geofence warrant was here?
A It makes it quite larger.
Q Surprise you if it's 125,000 square meters?
A No.
Q Which would be about 30 acres; is that correct?
A It's probably going to go up quite significantly by adding that extra area.
Q If you add that extra area, what else was inside the effective range of this geofence warrant besides the church and the bank?
A You would include the -- there's a mini store -- or a self storage north of the bank and church. Probably more of the hotel and hotel area. The road going past the church. There's a business across the street, the wooded area behind the church. There's quite a bit of stuff in that area. If you kept expanding, you would just keep --

Q What about residences or apartment buildings? Would it reach some of those, too?
A It possibly could have. There is a set of apartments that kind of backs up to kind of the back side of the bank, but there's a wooded area there.
Q Right now we're talking about theory, though. You don't actually know where any of those Wi-Fi access points are located; right?
A No.
Q Who would have that information?
A Google possibly.
Q Why do you think so?
A Well, they've got to have something to base the -- you know, they've got to know the general area of the access point to use it as a reference to derive location. With the GPS system, the reason we're able to determine location is because we know where the satellites are. So it's a point of reference to then find yourself.
Q And here we don't -- what's the equivalent to the satellites? We know where the satellites are, so we can figure out our GPS location?
A This would be knowing where the actual access point is.
Q And we don't know where those are?

A No, we don't know which points were used.
Q Have they been provided to you by Google?
A No.
Q What would having that information allow you to do?
A You could use their various functions to -- if you knew the access point that was used, its location, signal strength, you could, in essence, kind of recreate or at least see what the results are. Here we just see the results.
Q Would it allow you to figure out how many hits were likely outside the 150-meter radius to begin with?
A It could.
Q Do you know the range of the Wi-Fi access points in this case?
A No, not specifically.
Q Would Google have that information?
A I don't know that they would have the range.
Q Certainly it hasn't been provided to you, has it?
A No, it has not.
Q If you did have that range, what would it enable you to do?
A I don't know that we would ever get the range, and I don't know that range would exactly assist other

than knowing, you know, kind of how far some of the access points may reach. You would never end up with an actual range.

Q But it would allow you to try and figure out how far outside of the 150-meter radius some of those reach?

A It could. If you could determine just how far away you could actually see the church's Wi-Fi, it could be quite a bit of distance outside of the circle just based on how close they are to the outer edge of the circle.

MR. PRICE: Your Honor, do you have any follow-up questions?

THE COURT: Let me make sure I understand that.

Why don't you restate what you just said.

THE WITNESS: So if the -- again, the circle that has been drawn around this area for the search to be given to Google, that circle doesn't limit really anything other than Google in their search. Out in the actual -- in this area, if you went and looked, the church's Wi-Fi, which the church is located within the circle, their Wi-Fi could extend out past the circle. And due to that, those measurements could be taken and actually place you in the circle even if you

weren't in the circle.
BY MR. PRICE:
Q So, if I can clarify. Google doesn't know where the location -- doesn't know the location of the access point for the church's Wi-Fi; correct?
A They generally know where it is, but not down to the specific, exact -- you know, they couldn't walk into the building, I don't think, and point it out to you.
Q But they have a general idea where it is, and they know that it's in that circle; right?
MR. SIMON: Your Honor, I would ask that he stop leading the witness.
MR. PRICE: I'm just trying to clarify your point, Your Honor.
THE COURT: I think I understand.
MR. PRICE: Okay. I'd like to move on, if that's all right.
BY MR. PRICE:
Q I want to continue asking you about the scope of the warrant but shift slightly and talk about Google's process, Google's algorithm for determining device location. So, you just talked generally about how Google uses Wi-Fi to locate devices, but do you know mathematically how Google actually does that?

A Generally, I know the process, but know how they label a display radius or how well they determine the accuracy of their calculation, no.
Q What would you need to know to figure that out?
A I assume we would just need to know what Google knows as far as how they actually process this data to determine how accurate it is.
Q How would you describe that process? Is it an algorithm?
A I honestly don't know.
Q Why don't you know?
A It never -- I just don't know their inner workings. Again, I know generally how it operates, but we don't know the fine print here that they have labeled out as to how this works.
Q And if you did know the fine print, what would it enable you to determine in this case?
A It could possibly determine a little more information as to how accurate it is but, again, without knowing what they possibly have or could tell us, I don't know.
Q Would Google have documentation about how this process works?
A I assume they do.
Q Have you seen it?

A No, I have not.
Q What do you think those documents might tell you if you did see them?
A I honestly don't know. I guess it would outline their policies and procedures on how they're going to conduct a search, how they apply anonymity to these devices and, really, all of the background work that they do.
Q What would it tell you about how far the search may have reached beyond 150 meters?
A I don't exactly know, but, I mean, it could provide some insight into that.
Q To the Wi-Fi access points?
A If they can provide that, yes.
Q Was any of that information in the warrant or the application?
A No, I didn't see any type of request like that.
Q Has any of it been provided to you?
A I haven't seen anything.

THE COURT: So, by the application, you're talking about Defense Exhibit 1?

MR. PRICE: Yes, Your Honor.

THE COURT: Now, Mr. Price, we've been going for a little while here. Do you have a while more to go?

MR. PRICE: I'm afraid I have a little bit more, Your Honor.

THE COURT: Okay. That's fine. I think we should take a little break just to be sure that everybody is fresh. So we're going to take a 10-minute break.

I'm going to remind you, sir, that you will remain under oath. Don't speak to anybody about your testimony or listen to any commentary about it. And I'll ask anybody here to do the same.

We'll just start fresh as if we didn't take a break. All right? So let's take a 10-minute recess.

(Recess taken from 12:30 p.m. until 12:45 p.m.)

THE COURT: All right, sir. We'll resume your testimony.

MR. PRICE: Thank you, Your Honor.

BY MR. PRICE:

Q Mr. McInvaille, I'd like to turn to the question of whether the data provided by Google in steps 1 and 2 is truly anonymous?

A No, I don't believe it is.

Q We're going to talk about it, but thank you. So Google says that the data produced to law enforcement here is in anonymized form. You reviewed it. Can you take a look again at Exhibit 3 and tell us what you

see?
A Yes. So they provide device identifiers, date, times, locations, the source of that, and then a radius inside of that data.
Q So you said device identifiers. Can you tell me -- column A. Take a look at column A and the column numbers in the far left. What are those numbers?
A That is the anonymized device ID.
Q Do you know what Google does to anonymize this data?
A I don't know specifically.
Q Do you know their process?
A I do not.
Q Why don't you know?
A It's not -- I don't know that it's published.
Q Would Google have that information?
A I'm sure they do have it.
Q What about the latitude and longitude coordinates in columns D and E?
A That's the estimated location of the device.
Q Are those masked in any way?
A No.
Q So that's the actual location data here?
A Yep. To their knowledge and to ours, yes.

Q What were you able to do with this supposedly anonymous information?
A With the step 1, you can take the information and, by device ID, plot out each of the devices and their locations that were returned in that first step. And then in the second step, it is the same devices but with an expanded time frame and the absence of a restriction on location.
Q So you took these latitude and longitude coordinates from columns D and E, and you did what with them?
A You can plot them on the map. I organized them by the device IDs.
Q So did you do that here? Did you prepare a demonstration for us?
A I did. There's a subset of those in a demonstration.
Q Let's talk about what you did for that demonstration. You made a visual representation of some of this data provided by Google?
A Correct. So I took -- by device ID, I mapped out each of the locations provided. And we did that in two steps. So you have the first step that shows the location for a particular device during the first step or the first return from Google.

We then take that same device ID and now use the data that was returned based on the step 2, which removed the circle, the limitation as far as location, and the expanded time frame, and then you can see general movements for a portion of that data.

Q So this visual representation of some of the data, here you made a short video?

A Yes.

Q Two minutes and 46 seconds?

A Correct.

Q And you have that video on a DVD marked Exhibit 5?

A Yes.

Q Have you reviewed that DVD before coming into court today to verify that it is the same one as the video that you made?

A I did.

Q And you marked the DVD with your initials reflecting that?

A I did.

MR. PRICE: I would like to move to admit the video into evidence as Exhibit 5 and remind the Court that this is under seal because it is based off of the same raw data.

THE COURT: All right. No objection?

MR. SIMON: No objection, Judge.

THE COURT: All right. It's entered under seal.

MR. PRICE: Thank you, Your Honor.

(Defendant's Exhibit No. 5 is entered under seal.)

BY MR. PRICE:

Q Mr. McInvaille, can you please walk us through what we are looking at here?

A Okay. So this is device ID 965610516. This is the stage 1 request information that came back on that number.

THE COURT: Can you say the device number again?

THE WITNESS: Yes. It's 965610516.

THE COURT: Okay.

BY MR. PRICE:

Q And for our purposes today, how do you want to refer to this?

A This is the -- the color is the easiest. So this is green. What you'll see on the map is the locations that we've been discussing throughout. The circle, which is in red, represents the geofence that was laid on the map, as well as a green dot with a date and time, of which that was the estimated location for that device at that time.

Q Where's that dot located?
A For this particular map, it's there on top of the -- which is the church.
Q All right. Why don't you go ahead and play it and tell us what happens next.
A The video will sit here for just a moment so that you can see the beginning. So, I'll pause here. We're moving back in time now. So, in the stage 2 request, we kept the same device identifiers but now expanded the time frame to before and after the incident, as well as removed the location restriction.
THE COURT: So this is a stage 2?
THE WITNESS: Correct. So this would have been -- this would have been the data -- the data used to create this portion here was from the stage 2 production that Google made.
THE COURT: So it's the broader time frame before and after. And what's the other distinction?
THE WITNESS: No location restriction. So instead of just asking for inside of the circle, there was no restriction on this request.
THE COURT: How do we know that?
THE WITNESS: I believe it's indicated in the search warrant. That would be the next step, or -- it was either there or in the email request. I can't

recall right offhand.

THE COURT: All right.

A So the first point that shows up is at 3:50 p.m. that afternoon. And you see that the dot is located on top of the hospital. I believe it was Johnston-Willis, if I'm correct. There at the hospital. And what you'll see at the beginning is several points are located in a cluster at that location prior to leaving that location. And I'll start now.

You see several of those points appear. And then now we see them begin to move away from that location, and they will move in a southern direction.

BY MR. PRICE:

Q Tell us, what does the increased spacing indicate to you?

A Definitely there was some travel from the area of the hospital down south to now where you see the original circle where we saw in the very beginning.

So, in this portion here, you will notice the kind of general direction of travel as well as the timing of that travel.

And in the next portion, you will see where --

THE COURT: Why don't you put those numbers on the record.

THE WITNESS: Okay.

THE COURT: The timing. Down south is down a road, which I think is marked as Commerce Road?

THE WITNESS: I can give them, yes, ma'am.

THE COURT: And then it returns to the church. So what kind of time frame is that in?

THE WITNESS: So, this is 28 seconds in the video. And you will see the first dot in the northern portion of the frame is at 4:36:59. The next being just south of that. And I don't recall the name of that. It looks to be Courthouse Road, possibly. The next dot is at the intersection of Hull Street and Courthouse at 4:39 p.m.

THE COURT: I don't want to identify who the user is. I just want a sense of the timing. So, you say you see there's travel. Is it five minutes? Is it 30 seconds?

THE WITNESS: I understand.

From the intersection of Courthouse Road and Hull Street, there is -- to the next point is about -- just over four minutes. And then arrives at a residence.

THE COURT: Okay. Now, what I'm really trying to get a sense of is how far the distance is, without specifics, and how long it takes. So, for

instance, Johnston-Willis Hospital was not in the red circle; correct?

THE WITNESS: Correct.

THE COURT: Do you have an estimate of how far outside the red circle it was?

THE WITNESS: Bear with me one second. More than seven miles.

THE COURT: All right. That's the kind of general information I'm looking for. Okay?

THE WITNESS: Yep. Moving into the area, once it comes down south towards the circle, you have -- from the time it gets here to then in the circle and then past the circle is about three -- excuse me -- four minutes and some seconds, and then moves even farther down to a particular residence.

THE COURT: And the residence is also outside the circle?

THE WITNESS: Correct, it is.

THE COURT: All right.

THE WITNESS: So once it gets to the area of that residence, you will see again another cluster of points showing up indicative of that device stopping at that general location.

THE COURT: Okay.

BY MR. PRICE:

Q Can we just summarize what happened with Mr. Green here?
A Yes.
Q Where did Mr. Green start?
A The hospital up north.
Q And then he drove south?
A Correct.
Q And passed by the bank, the church, what?
A So it appears, based on the timing -- I'll scroll back here. It appears, based on the timing of those three points, that the device was passing by. So not that it necessarily had to stop inside of the circle when it shows up. That dot that you see inside the circle at 4:41:45 is the one that shows up in the stage 1 return.
Q And that's inside the church or the bank?
A It shows on top of the church.
Q So after passing by the church, after showing up on the church, you said it settles on top of a single-family residence?
A It does.
Q Were you able to determine whose house that was?
A I reviewed tax records for the county and determined some names for that location.
Q And were you able to include -- draw a conclusion

about the likely identity of Mr. Green?
A Not necessarily the exact identity, but generally a family, I assume, who lived there.
Q Would that information be identifiable to law enforcement as well?
A It could be, yes. They're resources to look at.
Q Let's go ahead and take a look at the next one.
A So, moving to the next example, this device ID is 907512662. And what you see on the map is the -- is a single dot on top of the church. And what this is is the return for that device ID during the stage 1 production by Google.
THE COURT: And it's blue?
THE WITNESS: Yes, it is.
BY MR. PRICE:
Q Why don't you go ahead and --
A So, in the beginning of now the data for that same device ID that begins prior to the incident, it shows up at the apartment complex just to the south of the circle, less than a thousand feet away. And during that time, you'll see -- as it begins, you'll see several points show up in that general area of the apartments. And then shortly after, you will start to see a trend in movement to the north, likely by the road there beside the church.

Based on the timing, you have about a minute and eight seconds, or so, until the -- from the time the device is last showing at the apartments to the south where it originates up until the point that it gets up to -- towards Hull Street.

When we continue, it begins to move down Hull Street before making another trend down to the south towards another residence. So once we get down to this other residence farther south of the circle, we see several dots appear on a single-family residence here. Remains there just a bit before leaving and heading back north.

THE COURT: Before doing what? I'm sorry?

THE WITNESS: Before heading back north. And in the video, you'll see it returns back to the beginning location at the apartments.

And just for reference, Judge, just about -- it appears to be over a mile away from -- the residence is -- from the circle down south.

BY MR. PRICE:

Q Can you walk us through the chronology here like you did with Mr. Green? Can you walk us through the chronology for Mr. Blue?

A So, blue begins at the apartments here shown on the map, leaves in a northern direction, very likely

up the road beside the church, heads up to Hull Street. Appears to head to the right on Hull Street before coming back and making a southern travel down to that house that's a little over a mile away from the circle. And then after making that visit, returns back to the apartment complex where it began.

Q So what were you able to determine about the likely identity of Mr. Blue from this data?

A So, blue is a little more difficult just due to it originating in an apartment complex. As we all know, many people live in an apartment complex, and this is not precise enough to show which apartment is being used.

But based on the other travel to that known location, the single-family residence down south, determining identity of those individuals based on tax records and other open-source information, that, in conjunction with other open-source means, could help you determine who could have left from the apartment complex.

Q Let's talk about those additional databases.

THE COURT: Before you get there, how long of a period of time did this cover in tracking the blue dots?

THE WITNESS: Both -- all of these, based on

the stage 2 request, are all an hour before the incident and an hour after. So that's how it's bracketed.

THE COURT: Well, this particular one.

THE WITNESS: It's very close to that. It appears the first point shows up at 3:55 p.m. The final showing up almost 5:50 time frame.

THE COURT: Okay. And is there any spot for the blue example that appears inside the circle other than the step 1 return information?

THE WITNESS: No, ma'am, it does not.

THE COURT: All right. I'm done.

BY MR. PRICE:

Q Based on your experience as a law enforcement official, are you aware of any additional tools that may be available to law enforcement to help identify somebody based off of this open information that you have?

A Yes. We had information like Sky X and Linx that we could use to search names, locations, things such as that, that would help during an investigation, trying to identify people based on places that they frequent.

THE COURT: You're going to have to describe what those are and maybe spell them.

THE WITNESS: Okay. Linx is L-i-n-x. It's essentially a database that we had access to. People's -- different agencies' reports and things would go in there so you would be able to search names and vehicles, things like that, so you could see past history on different people based on if they were involved in different things.

BY MR. PRICE:

Q And one of those different things, would that be a traffic ticket?

A Yeah, it would be as simple as a traffic ticket or just filing some type of report from something being stolen. It could be really anything, any interaction with local law enforcement or anybody who entered that data into a report.

Q And something like that would give you an address associated with a name?

A Yeah, you could have several identifiers. You could have varying things from addresses to vehicles.

Q Did that happen in this example?

A Was that requested?

Q When you were looking at the data for Mr. Blue, did you come cross any records of one of those incidents?

A So a name that was listed under tax records for

the residence that was visited down to the south, one of those individuals did have where they had paid a traffic ticket in the past just a few years back. Same address.

Q So, would law enforcement be able to figure out the identity of Mr. Blue using these tools?

A I think generally you could, based on the combination of information. Again, it would -- not so much down to maybe the specific person, but I think you could narrow it down to a very small group of people based on these locations.

Q Thank you.

Can we turn to the final example here?

A So, here in the third example, we're looking at device ID 1305167661. On the map you will see three yellow dots. They also have corresponding times.

These dots show up at the -- either both -- there are two on the bank and then one right beside the bank. And then, again, we're going to move into stage 2 of the request and see the data prior to this, earlier in the day, for this same user.

Q So we're going back one hour now?

A Yes. So this starts at 3:51 p.m. And what you'll see is a data point again on top of a single-family residence. And for a moment here, you will see

several locations show up there at that same residence prior to moving just a short distance north.

THE COURT: So is the single-family residence outside the circle?

THE WITNESS: It is. In just a moment when this zooms out, I can tell you the approximate distance.

Just after being at the single-family residence, it moves just a very short distance north to this location, which is the Manchester High School there on Bailey Bridge Road. It appears to show up there in front of the school for just a brief moment before continuing north.

I would say it's approximately three or four miles from the circle is that original location.

BY MR. PRICE:

Q So the single-family residence where this starts an hour before the incident is how many miles from the --

A A few. Three or four miles at least.

Q Okay.

A So, continuing, you'll see the trend north as it moves towards the red circle. So then you see that device move into the circle there at the original dots that we spoke of that show up at the bank, which would

have been returned in the stage 1 request.

As we continue, you will then see that device move out -- move away from the circle and then move over to another kind of business area there on the same -- on Hull Street for just a moment before heading back south to its original location down at the single-family residence. And, again, that happens in that same time period as we've been speaking about.

Q So, can you just summarize the chronology for Ms. Yellow as well?

A Yes. So, again, that device starts out south of the red circle at that single-family residence, moves up towards the area of the Manchester High School. Continuing north after that and going to the bank. Leaving the bank area, going to some other -- in the general vicinity of those other businesses on Hull Street before returning back to the original location of the home.

Q So based on that information, were you able to draw a conclusion about the likely identity of Ms. Yellow?

A So, again, I started with tax records for that residence, located a name for an individual there. Also looked at that individual's information on Facebook and was able to see a group, a family, a

husband and wife, who also have a high school-age son in some of their pictures, referenced some of his ROTC events. So, yeah, I would say that, generally speaking, we were able to determine a likely group of people that that device belongs to.

Q And would this information be as identifiable to law enforcement as it was to you?

A Sure.

Q Even in this anonymized form?

A Yes, it is.

Q Thank you.

THE COURT: Let me just make clear. Of the yellow points that you have just indicated, how many other than the three that showed up at step 1 or stage 1 are inside the circle?

THE WITNESS: Just those three.

THE COURT: All right. Thank you.

BY MR. PRICE:

Q So, do you agree with Google's characterization of the step 1 and step 2 returns as anonymous?

A I do not.

Q Why?

A Our location and our frequent locations or our trend of locations in a particular amount of time is indicative of our identity. Individuals, different

groups of families even, you know, go to different places. So, yeah, our location is part of our identity.

Q Why does Google describe it as anonymized, then?

A Because all they did was strip away the unanonymous ID that can later be revealed. That's all they stripped away.

Q Do you know how they came up with the anonymized figures here?

A I don't.

Q Do you know if they have any relation to the actual Google ID?

A I don't know that.

Q Why?

A I haven't seen it published.

Q Would Google have policies and procedures that are relevant to this question?

A I would assume they do.

Q Why do you think so?

A They receive many of these requests a day, a year. I would think that there's some process or, you know, policy that dictates how these will be responded to and searched.

Q What might those policies tell you?

A Kind of hard to say. I'm sure, again, it would

dictate how they do the request, what they deemed acceptable based on the request. It could be anything.

Q And has any of that information been provided to you?

A Not that I've seen.

Q All right. Thank you.

So, I want to turn briefly to the question of voluntariness here. I seem to have misplaced a page. Here we go. I'm sorry.

So, we talked a lot about step 1. I want to turn now to steps 2 and step 3 and the question of how law enforcement worked with Google to narrow the 19 initial hits down to 9 and then 3. Can you tell us what occurred at step 2 in this process?

A So step 2 ended up being 9 of the original 19 that showed up in the circle. And then for that nine, they expanded time frame again to an hour before and an hour after and removed the geographical limit.

Q Have you reviewed any of the correspondence between law enforcement and Google about this request?

A I have.

Q Can you turn to the document marked as Exhibit 6 in your packet?

A Yes.

Q Do you recognize the document?
A Yes, I do.
Q What is it?
A It's an email between -- I believe it's Detective Hylton and -- as well as the -- it just says the Google team. So I assume Google's legal response group.
Q And it's the correspondence that you've reviewed in this case?
A Yes.

MR. PRICE: I'd like to introduce that into evidence as Exhibit 6, please.

THE COURT: Any objection?

MR. SIMON: We won't object, Your Honor.

THE COURT: Okay. It will be entered.

Just for the record, Hylton is H-Y-L-T-O-N.

(Defendant's Exhibit No. 6 is admitted into evidence.)

BY MR. PRICE:
Q In this request for step 2 data, starting from 19, how many users does Google -- does law enforcement ask Google to provide additional information on in step 2?
A It appears all 19.
Q All 19. Okay. So, step 1 was 19, and step 2 they also requested all 19, expanded data on all 19?

A It is with, you know, another sentence that if they feel it's unreasonable, that they may use the numbers that are listed 1 through 9.
Q Who's "they" in that case?
A I'm sorry?
Q Who's "they" referring to?
A "They" being -- Hylton appears to be the author of this email. So he advised that they could, if they saw that this request was unreasonable, that they could use 1 through 9 if it fit more likely.
Q "They" being Google?
A Oh, Google, yes. I'm sorry.
Q So, Google is the person who's going to determine what's relevant. Okay. Can you turn to Exhibit 7, marked Exhibit 7?
A Okay.
Q Do you recognize the document?
A Yes, I do.
Q What is it?
A Another correspondence between Hylton and Google.
Q And that's the correspondence that you reviewed in this case?
A Yes.
MR. PRICE: I'd like to introduce that as Exhibit 7, Your Honor.

THE COURT: Any objection?

MR. SIMON: No objection, Your Honor.

(Defendant's Exhibit No. 7 is admitted into evidence.)

BY MR. PRICE:

Q Can you tell us what that document says?

A Again, it says it's writing to inquire about my correspondence on 7-1 and 7-2. It's, again, requesting the same -- it's the same exact request, just a follow-up on, I assume, a nonresponse from Google.

Q And how many users does that ask for additional data on?

A The request doesn't change. All they did was add the paragraph at the top. So, the 19, but still with the added piece that you could just do the 1 through 9.

THE COURT: Use the language correctly. It says "If this request seems unreasonable, please keep in mind that Google device numbers 1 through 9 may fit the more likely profile of the parties involved." You don't need to paraphrase it. You should say it. Thanks.

BY MR. PRICE:

Q I'd like you to turn to Exhibit 8 in your packet,

please. Do you recognize that document?
A I do.
Q What is it?
A Again, correspondence with Hylton and Google team.
Q And this is concerning which step of the process?
A Still appears to be the step 2, but it has now been just narrowed down to devices 1 through 9.
Q Do you have any idea how law enforcement --
THE COURT: Well, first of all, is Exhibit 8 being moved into evidence?
MR. PRICE: Oh, yes, Your Honor. I'm sorry.
THE COURT: Any objection?
MR. SIMON: No objection, Your Honor. I don't think it's on the screen.
THE COURT: It does need to get on the screen.
MR. PRICE: It is right now.
THE COURT: Pardon me? It's not on the big screen.
THE CLERK: It just takes a minute once it's admitted.
THE COURT: Got it. That's why it wasn't on, because it wasn't admitted. So that is also entered. Thank you for doing it correctly. All right.
(Defendant's Exhibit No. 8 is admitted into

evidence.)

MR. PRICE: Thank you.

BY MR. PRICE:

Q Mr. McInvaille, do you know how law enforcement finally narrowed their list down from 19 to 9?

A I don't know the specifics, no.

Q Why don't you know?

A It's not in the correspondence that I've seen.

Q Did any of those nine seem like odd choices to include to you?

A I'm trying to remember the color. The color was blue, I believe. That, if I had to say, blue is an odd entry into this group.

Q Were there any others?

A Really, the -- I mean, honestly, once you -- well, for the stage 2, both green and blue would have been odd for the moving to the stage 9 process.

Q Why did the inclusion of Mr. Green in the stage 2 process strike you as odd?

A There was just one single point at the church.

Q At the church, not the bank?

A Right.

Q And compared to other people?

A Some -- there were others that were -- that showed up at both the church and the bank. There were some

that just showed up at the bank, and then there were a few that only showed up at the church with just single points.

Q So who would know why law enforcement included Mr. Green in stage 2?

A I'm not sure.

Q Would law enforcement know?

A I assume they would.

Q Would Google know?

A They may if they had discussion with --

THE COURT: You said they would or would not?

THE WITNESS: I assume they would.

BY MR. PRICE:

Q Would the magistrate judge who issued this warrant know?

A Oh, I don't know.

THE COURT: I'm sorry. You're sort of looking down.

THE WITNESS: I'm sorry. I don't know.

THE COURT: You don't know?

THE WITNESS: No, ma'am.

THE COURT: Just to be clear, can you identify what numbers blue and green are on the list?

MR. PRICE: With the corresponding device ID?

THE COURT: Yes.

THE WITNESS: Yes. Green is 965610516. Blue is 907512662.

THE COURT: And can you look at the list and identify which ones those are in 1 through 9?

THE WITNESS: Yes. It is -- the green is number 5 on the list. Blue is number 8 on the list.

THE COURT: All right.

BY MR. PRICE:

Q Let's talk about step 3 here for a second. You reviewed the correspondence with Google about step 3?

A Yes, I believe so.

Q Can you turn to Exhibit 9, please, in your packet? Do you recognize the document?

A Yes.

Q What is it?

A Another email from Hylton to Google legal team.

Q And that's the correspondence you reviewed in this case?

A Yes.

MR. PRICE: I'd like to introduce that as Exhibit 9, please, Your Honor.

THE COURT: Any objection?

MR. SIMON: No objection, Judge.

THE COURT: All right. It will be entered.

(Defendant's Exhibit No. 9 is admitted into

evidence.)

BY MR. PRICE:

Q What additional data did the government receive from Google in step 3?

A I'm just going to read it. "Please send subscriber information for the above device IDs as soon as possible."

So they asked -- law enforcement asked for the subscriber information for all three devices, device IDs, listed in this request.

Q Can you turn back to the raw data in Exhibit 2, please? Oh, I'm sorry, Exhibit 3. And the first page of the last return, it is the fifth from the last page. It says "Stage 3 Return.CSV" at the top. Sorry. The fourth from the end.

A I have it.

Q Do we have it on the screen? Great. Can you tell us what is in column A?

A Column A is the Gaia ID.

THE COURT: To be clear, this is a two-column listing, which differs from the earlier listings that had several, A through F or E. This just has A and B, and it has four rows under it.

Sorry to interrupt.

BY MR. PRICE:

Q Do you know what a Gaia ID is?
A It's what they call the Google accounts ID, administration ID.
Q So, what's the significance of providing the Gaia ID in this case?
A So, this is the unanonymized number now. In this column here, it's displayed as a formal just because of how the table was printed. So that's not the full number.
THE COURT: I'm sorry. Google accounts what?
THE WITNESS: Google accounts ID administration.
THE COURT: Okay. Pardon me.
BY MR. PRICE:
Q And you're saying that the plus 11 in all of those numbers indicates that the number is actually much longer?
A Yes, it is.
Q And that gives a -- corresponds to the pseudonymous device IDs?
A Correct. So, you have the Gaia ID, which is the actual ID for the user. In a corresponding column to the right of that marked device ID, which is what we've been seeing in the stage 1/stage 2 requests, and that is the anonymous number. So now what it's

giving you is it's labeling the anonymous number with its real number now so that it can be identified.

Q Do you know how law enforcement narrowed the list of nine down to these three?

A No, I don't.

THE COURT: Do you know who narrowed it down to three?

THE WITNESS: I believe Hylton was the requester for that.

THE COURT: Okay.

BY MR. PRICE:

Q Did any of these three seem like odd choices to include to you? We just talked about --

A Yep. So, the device ID ending 2662, which was the blue example that we reviewed, that is the ID that you see earlier in the day at the apartments passing by the -- on the road there past the church and then returning back to the apartments. That ID made it to the final three.

Q Why did it strike you as odd that that ID would make it to the final three?

A From looking at the data, it appears that the device only passed by the location, not having time to stop. It just doesn't appear that there was time in there to even stop through the geofence based on the

data that was given in stage 2.
Q Do you recall what time of day Mr. Blue hit inside that geofence?
A It was 4:35:45.
Q How many minutes was that before the incident?
A I believe about 20 minutes. I don't know the exact time. I think it was just before 5:00.
Q So he only hit once in the church 20 minutes before the robbery?
A Correct.
Q But he was included in the final three here?
A Correct.
Q Do you know why law enforcement might include someone who wasn't at the bank or in the parking lot?
A I'm not sure.
Q Do you know who might know?
A I assume Hylton, since he made the request.
Q What about the magistrate judge who issued this warrant?
A Oh, I have no idea.
Q So, you can't tell, based on the information you have, how the government went from 19 down to 9 down to 3?
A No.
Q What would you need to know?

A I assume their thought process as to what constitutes needing to know more about each dot that shows up.

Q So you'd want to know how the law enforcement officers made their determinations here?

A Yes. I would assume that there's a reason behind choosing certain IDs over another.

Q Anything else you would want to know?

A I'm sure that would be helpful, just the reasoning behind it, and just the application how it was -- how the data was applied to the map to get an understanding of what it was telling you.

Q All right. Thank you very much.

THE COURT: I want to ask one question about these exhibits. These communications, Exhibits 6, 7, 8, and 9, is there anything on the exhibits themselves to identify the date and time they were transmitted?

THE WITNESS: No, I do not think there are. The only one that has any reference of date and time was one of the follow-up emails that references a prior request on 7-1 and 7-2, but that's all.

THE COURT: All right. Thank you.

MR. PRICE: No further questions at this point. Thank you, Your Honor.

THE COURT: All right.

Mr. Simon, do you anticipate a long cross?

MR. SIMON: Judge, I think probably between 30 and 45 minutes.

THE COURT: Why don't we, then, just take, again, a 10-minute recess just so that we can all catch our breath. I do appreciate that you all showed up timely. I want to be sure that we keep things moving, and so it will just be ten minutes. I have 2:26. And I'll ask you all to be back again. Sir, you will remain -- I'm sorry. 1:26. Daylight Saving Time happened.

Sir, you will remain under oath, and I'll advise you again, don't speak to anybody about your testimony, and I'll ask everybody here not to speak to him. All right? Ten-minute recess.

(Recess taken.)

THE COURT: All right. Mr. Simon, are you prepared for cross?

MR. SIMON: Yes, Judge.

THE COURT: I remind you that you are under oath, sir.

THE WITNESS: Yes, ma'am.

CROSS-EXAMINATION

BY MR. SIMON:

Q Mr. McInvaille; is that right?

A Yes, sir.

Q Good afternoon.

A Good afternoon.

Q Mr. McInvaille, you've been called to testify in this hearing. And your testimony, if I understand it correct, is that you have -- you have to opt in in one form or another into Google to collect your location history; is that correct?

THE COURT: Now, Mr. Simon, you're definitely going to have to be closer to the microphone. It's natural to look at the witness, but when you do that, your face is away from the microphone.

MR. SIMON: Understood, Judge. And my apologies.

BY MR. SIMON:

Q Mr. McInvaille, you've been called to testify in this hearing today. And, as I understand, your testimony on direct examination was on a few fronts. First, you say on location history the user has to opt in for the collection of that location history; correct?

A That's correct.

Q And your testimony with respect to the clarity about that location information -- if we could pull back up exhibit -- Defense Exhibit 4 and just go to the end of that video and pause it.
A The very end?
Q Yes, the very end of Defense Exhibit 4.
A Okay.
Q Okay. And so once that clears off the screen, can you read what -- this is the 4-minute-45-second mark of Defense Exhibit 4. Can you read for the Court what's there on the screen there?
A Yes, sir. It says "Get the most from Google Maps." Then "Google needs to periodically store your location to improve route recommendations, search suggestions, and more. Learn more." And then the indicator is "yes, I'm in" or "skip."
Q And you didn't click the "learn more" box in this simulation; is that right?
A Not in the video, no, sir.
Q Okay. But if you did click that "learn more" box, you'd be told about what type of information they're storing, how long they're storing it; right?
A It takes you to the Google terms and privacy agreements. It takes you to their website where all of that is located.

Q So if you wanted to know, you could know; right?
A Correct.
Q It's clearly on that screen; right?
A That's where you would navigate to it, yes.
Q And with respect to your work with geofence warrants -- you testified that you generally work with geofence warrants. Can you say that with more clarity? How many times have you examined a geofence warrant?
A I don't know about how many times. I've looked at several throughout several states. I see them quite often in North Carolina where I do a lot of work. A dozen.
Q Okay. A dozen. And so your understanding -- right? -- is that there are three steps; correct?
A Well, that's what they outlined in the brief, yes.
Q Okay. And you've looked at the search warrant in this case in Defense Exhibit 2; right?
A Correct.
Q Okay. And in that process, there's a multistep process. Step 1 is going to be from 4:20 to 5:20; is that right?
A I believe so, yes.
Q Okay. And that's going to be what we've been talking about as inside the box; right?

A Correct.

THE COURT: Wait a minute. What are you referring to?

MR. SIMON: We're referring to Defense Exhibit 2, Your Honor. This is the search warrant in the case he was testifying to earlier about the difference steps --

THE COURT: The search warrant is Exhibit 1. The Google amicus brief is Exhibit 2.

MR. SIMON: My apologies, Your Honor. I've been asking the witness about Defense Exhibit 1. My apologies.

THE COURT: That's all right.

BY MR. SIMON:

Q And I'm referring to what would be, essentially, the fourth listed page of Defense Exhibit 1. That'll be attachment 2. It starts as attachment 2 and basically outlines this process, this three-step process. First step is going to be inside that 150-meter radius; correct?

A You're on page 3?

Q I'm just asking you about the search warrant.

A Yes, it is.

Q Okay.

THE COURT: Well, he's allowed to look at the

documents.

MR. SIMON: Understood, Judge.

THE COURT: So, you should give your answer based on the documents.

A I just thought you referred me to a page. That's just what I was clarifying.

BY MR. SIMON:

Q Okay. And so stage 1 gives you points that are inside of that 150 meter radius; correct?

A Correct.

Q And then law enforcement can get additional location information for 30 minutes before; correct?

A Yes.

Q And then 30 minutes after; correct?

A Correct.

Q And that's stage 2; right?

A Correct.

Q But in stage 1, you only get points that are inside that radius; correct?

A That's correct.

Q All right. Now, you've been testifying a little bit about the anonymous nature of the returns in this case. And the raw data is Exhibit 3, but I won't necessarily walk you page by page through that. But you've testified about a Mr. Green, a Mr. Blue, a

Mr. Yellow; right?
A Correct.
Q And Mr. Green, in your three-pass video, Defense Exhibit 5, that starts at about the 28-second mark and it ends 1516, the identifier. You don't know who Mr. Green is; correct?
A No, sir.
Q And Mr. Blue, that starts at about, I think, the 1 minute and 50 second mark of Defense Exhibit 5. You don't know who Mr. Blue is; correct?
A No, sir.
Q And with respect to Mr. Yellow, that starts about the 2 minute 27 second mark of Defense Exhibit 5. You don't know who Mr. Yellow is; correct?
A No, sir, I don't.
Q And that means they're anonymous; right?
A No, not that they're anonymous. Just that I can't positively identify the person.
Q But your testimony to this Court today under oath is that you don't know who Mr. Green is; correct?
A I do not know.
Q And Mr. Blue, you don't know him; right?
A No.
Q Mr. Yellow, don't know him; right?
A No.

Q Okay. Now, you've been in law enforcement before you joined Envista. You're with Envista now; right?
A Correct.
Q Okay. And when you were with law enforcement, you wouldn't go to a judge or place in an affidavit that you can get a search warrant on a home based on the data you reviewed in stage 3 at stage 1; correct?
A From which stage?
Q Let's say stage 2. Stage 2. You wouldn't go get a search warrant based on this information that you plotted in Defense Exhibit 5; correct?
A Not from stage 2, no.
Q Okay.
THE COURT: A search of what? Of which data point?
MR. SIMON: Well, we're talking about -- we can go one by one, Judge.
BY MR. SIMON:
Q Mr. Green -- this is at the 28-second mark that began. The testimony on direct examination was that this was a single-family residence that you went back to; correct?
A Correct.
Q And based on what you reviewed at stage 1 and stage 2 about Mr. Green -- this is the identifier, the

anonymous identifier that ends 1516 -- you wouldn't go and get a search warrant based on that information; correct?

A No, I would not.

Q You would need to know more; right?

A Yes.

Q And the same with respect to Mr. Blue. You said Mr. Blue went back to an apartment; correct?

A Correct.

Q And then he went to another residence; correct?

A Correct.

Q And you wouldn't get a search warrant for either that apartment complex or that home based on those returns; correct?

A No, I wouldn't.

Q Okay. And that's because you don't know who they are; right?

A Correct, or what you would be searching for.

Q Now, with respect to Mr. Yellow, again, with the single-family residence, you wouldn't try to get a search warrant based on that information; right?

A No.

Q You would want to know more?

A Yes.

Q Okay. And speaking to wanting to know more, you

were talking about being a bit befuddled as to why they might be looking at all these other people -- right? -- at stage 2 and stage 3; correct?

A Correct.

Q All right.

MR. SIMON: Can we pull up Defense Exhibit 6?

BY MR. SIMON:

Q Defense Exhibit 6, do you see that first listed number there that ends with 5659?

A Bear with me.

Q I'll give you a minute.

A Yes, I do.

Q Okay. Let's look at Defense Exhibit 7. Do you see that first listed number in Defense Exhibit 7, do you see that?

A Correct.

Q That's the same as that first listed number in Defense Exhibit 6?

A It is.

Q And then Exhibit 8, Defense Exhibit 8, this is when it's narrowed down to nine; correct?

A Correct.

Q And what's the first listed number there? It's the same one as the first listed in Defense Exhibits 6 and 7; correct?

A Correct.
Q And now let's look, finally, at Defense Exhibit 9. The first listed number is the same as the first listed number in 6, 7, and 8; correct?
A Correct.
Q Did you plot that number?
A I did.
Q Okay. And what did you come to find out about that number based on your expert opinion?
A There were points within the area, of course inside the circle, in the initial request. Those were both at the church and the bank. And the stage 2 portion of that same person's data, it shows travel from that area south, away from that area. I don't exactly recall the exact area to describe it, but south, away from the circle.
Q So based on your expert opinion, looking at this case, in your expert opinion, is that the device that likely was involved in the crime here?
A Yes, it could have been.
Q Okay. Now, with respect to your understanding of Google, you're here to testify about materials that Google might turn over; correct?
A Correct.
Q That the defendant wants Google to turn over;

correct?
A Yes.
Q You never worked for Google?
A No.
Q Okay. To the extent that you've worked with Google, have you seen them provide, in a geofence warrant, any additional information than what's been provided to the United States here?
A I've never seen it requested.
Q You've not -- well, let me rephrase. Have you seen -- the stage 3 returns you've seen in this case; correct? The stage 3 returns you've seen?
A I have seen them, yes.
Q You've seen the longitude and the latitude in this case?
A Correct.
Q Okay. And you know it's a geofence warrant; right?
A Correct.
Q You've worked with some other geofence warrants; correct?
A Correct.
Q Are all of those from Google, all those geofence warrants?
A Yes.

Q And Google has provided the same information; correct?
A Yes.
Q Okay. Nothing different; right?
A I mean, besides the particulars of the case, no.
Q Besides the fact that it's a different crime committed elsewhere; right?
A Yes.
Q And different devices then available. In those cases, not all of them, but let's say the vast majority of them, they were prosecuted; correct?
A I mean, either they are or are currently being, yes.
Q Okay. Now, with respect to the specific request made in this ECF No. 28, you've reviewed the motion for discovery that the defendants filed; is that right?
A I don't know about the motion.
Q But you have been made aware of the different requests that the defendant is making in this case; right?
A Correct.
Q Okay. And your testimony earlier was that some of this could be helpful; right?
A Yes.

Q Might be helpful; correct?
A Yes.
Q Are you familiar with the facts of this particular case?
A Not the entire case, no.
Q Are you familiar with the fact that a search warrant was executed in this case on three residences?
A No, sir.
Q Are you familiar with the fact that there's eyewitness testimony placing a blue Buick behind the bank?
A No, sir.
Q Okay. So, you're not familiar with the facts of this particular case; correct?
A No. I've been -- this is what I've looked at.
Q So, when you say it could be helpful, you say that on a blank slate; right?
A Yes, just in terms of the request itself, yes.
Q Okay. Now, let's talk about one of the holy grail requests, it seems. You were talking about an algorithm; correct?
A Correct.
Q And that algorithm, to your mind, you would be able to crack Google's case, know exactly what they're doing and how they're doing it; right?

A Sure.
Q Okay. Would you know how to do that?
A Probably not.
Q Okay. So, your testimony in this case under oath to this Court is that this information should be provided by Google, but you personally could not do anything with it; correct?
A I don't know that I can, but I would assume it's quite complex.
Q Okay. Too complex for you to get?
A Could be.
Q Okay. Are you prepared to -- it seems that in talking about Google, your testimony is at no point going to be that you know anything for a fact; correct? With respect to Google?
A From like -- from --
Q In terms of the requests that the defendant has apprised you of, that they've made you aware of that they want from Google, your testimony has consistently been could be, may be, but you don't know; correct?
A Correct. We don't know what we can get from Google because we don't know what process, policies, documentation they have on the process.
Q And because of that, you can't actually sit here and tell us what would be helpful; right?

A Correct.
Q Okay. Now, I'm going to jump back a little bit here. You've been qualified as an expert here, but I want to talk to you a little bit about your training and expertise. We received your C.V. in this case. I'm sure you're aware of that; right?
A Yes, sir.
Q Okay. And you've received approximately 100 hours in location training; correct?
A Somewhere in that area. I don't know the exact number.
Q Okay. But would it sound correct to you if I told you that approximately half of your training came from Envista Forensics, your employer? Correct?
A Correct.
Q All right. And Envista is a company -- as far as you're concerned -- right? -- you're going out and you're just testifying primarily for defendants across the country; right?
A We do plaintiff work. We work both sides in civil cases as well as criminal cases.
Q Okay. How many cases have you testified in for a prosecution of a defendant?
A None as an expert in Envista.
Q But when you were in law enforcement, you did?

A Correct.
Q Okay. Now, the stage 3 returns in this case, that's going to be the returns that come -- that's going to be the raw data we get. I'm sorry. That's not the stage 3. The raw data that we get in this case that has the latitude and longitude; right?
THE COURT: Which one are you asking about? Are you asking about Exhibit 3 or stage 3 returns?
MR. SIMON: I'm -- Judge, it's actually -- the stage 3 return is also the Defense Exhibit 3. So, that's just the three levels of that return that's under seal.
BY MR. SIMON:
Q And I'm asking, just generally, about the latitude and longitude coordinates in this case. You could plot those; correct?
A Correct.
Q And you were testifying on direct examination, essentially, that the Google information in this case is 100 percent accurate; right?
THE COURT: Wait. Wait. Wait. I want to be sure I understand what you're doing.
MR. SIMON: Sure.
THE COURT: The stage 3 return has two columns, A and B, the G-A-I-A ID the device ID. It

doesn't have latitude and longitude that I can see. So if you're offering that presumption, you need to tell me the basis of it.

MR. SIMON: Your Honor, you've corrected me. I'm talking about the stage 1 and 2 returns as a part of the geofence. I'm saying stage 3 because in my mind, I'm just thinking about the latitude and longitude, but that's incorrect.

THE COURT: Which is not in stage 3 at all.

MR. SIMON: Correct.

THE COURT: So we've got to make the record clear.

MR. SIMON: Correct. And I will correct myself.

BY MR. SIMON:

Q The stage 1 and 2 returns, they are Defense Exhibit 3, that's going to be the latitude and longitude coordinates for a certain number of devices; correct?

A Correct.

Q The stage 1 was for 19; right?

A Correct.

Q And stage 2 was for 9; right?

A Correct.

Q And with respect to your testimony on direct

examination in Defense Exhibit 5 -- and I'm not asking for it to be pulled up, but in Defense Exhibit 5, you put particular points at particular places; right?

A Correct.

Q Now, if you'll look with me at column G there, the map display radius, it's your understanding -- right? -- that Google is approximating this information; correct?

A Correct.

Q So, when you testify on direct examination to this Court and you say this is where the person was at this time and I know it for 100 percent certainty, that's not correct; right?

A It's an estimated location of the device.

Q But your Defense Exhibit 5 doesn't show that it's estimated; correct?

A That's what I testified to.

Q Defense Exhibit 5 shows a particular point at a particular place; is that correct?

A That's the latitude and longitude provided.

Q Okay. But the display radius here, it's your understanding that Google tells you that a certain point could be within a certain display radius; right?

A Correct.

Q Okay. And so Defense Exhibit 5, if it were to

impress upon this Court that it is a point at a particular place at a particular time, you wouldn't actually say that; right?

A No. It's an estimation of the device's location.

Q Okay. So, Defense Exhibit 5 isn't accurate; right?

A It's accurately plotted based on the latitude and longitude, yes. That dot does not mean that the device is exactly on top of that dot.

Q But if I look at Defense Exhibit 5 -- and we can pull it up if you'd like -- Defense Exhibit 5 indicates that it is a particular dot at a particular point in time; isn't that right?

A Again, from the latitude and longitude.

Q Okay. But that's how it is plotted in --

THE COURT: That's asked and answered. You've made your point.

MR. SIMON: Okay. Understood, Judge.

BY MR. SIMON:

Q With respect to those points and the accuracy thereof, wouldn't that inform your discussion of the anonymous nature of the returns in this case?

A As far as how big the radius is?

Q Correct.

A Yes, it could.

Q So, if you see a radius is a certain circle, you wouldn't be able to say that because it's here, I know for certain that that's where I should be checking; right?
A That's correct.
Q You'd check the next place; right?
A You could have to check multiple, yes.
Q Check maybe the block; right?
A I don't know about the block, but, yeah, it could be more than one place.
Q But you'd give consideration to column G? You'd say let me look at what that display radius is; right?
A Sure.
Q Just to be clear, your understanding of the display radius is that it's giving you the sort of plus and minus on accuracy; right?
A That's their approximation of within this area.
Q Okay. Now, you were in law enforcement for a period of time. How long were you in law enforcement?
A Eight and a half years, I believe.
Q Okay. Eight and a half years. And in your time in being in law enforcement, if you were to get sort of the stage 1 and stage 2 returns that law enforcement received in this case, you would assess multiple points over a period of time; correct?

A Correct.
Q And you would assess those points for a number of reasons; right?
A Sure.
Q You would assess maybe whether you could look into some further connection with the potential perpetrator of the crime; right?
A Correct.
Q You'd maybe check if they -- you'd look at it to see if maybe they could be a witness to a prosecution; right?
A That's possible, yes.
Q And if you knew that there was evidence in a case that showed the potential -- or the perpetrator of the crime, they had a phone to their ear, you might say let's see who else is there, see if they have a connection to that robber; right?
A Correct.
Q So when you are befuddled at stage 3 and stage 2 when there are multiple devices requested, that befuddlement comes because you don't really know all the facts of this case; right?
A Correct. I'm looking at the data and how it comes out.
Q Okay. Now, just to be clear, the data in this

case, its accuracy can be assessed at this point in time; right?

A Based on what they have provided, you can see -- I mean, they're giving you their determination of how accurate they think it is.

Q Okay. But if you had the algorithm, you wouldn't be able to do anything with that; right? We've established that.

A It's possible. We don't know.

Q Okay. With respect to the anonymous identifier from Mr. Chatrie in this case, the anonymous identifier, as you understand it, is going to be the column that's in the far left corner of Defense Exhibit 3; correct? That's going to be column A at the stage 1 and stage 2 returns?

A Yes, it can be located in there.

Q And that's the anonymous identifier for these folks?

A Correct.

Q All right. And so presumably, if there's evidence in this -- or if there's argument in this case made by the United States that a particular account was at a particular place in time, you could plot the coordinates for the anonymous identifier related to all these accounts; right?

A Correct.
Q And you could see which account would match up to the allegations by the United States; right?
A Yes. And if you're talking about from stage 1 to the final stage, you can compare those three, yes.
Q And you could find out who that account belongs to, by your testimony, if you were to get at least the -- well, let's just talk about stage 3. If you get the subscriber info, you know who it is; right?
A Right, it provides subscriber information.
Q But until stage 3, you don't actually know who has what account; right?
A No, sir.
Q And that's the stage where the United States only got three subscribers; right?
A It's stage 3, correct, yes.
Q And, again, about that stage 3 piece, you testified on direct that you were again -- I'm using the word "befuddled" -- but you were a little surprised that Mr. Blue ended up in stage 3; right?
A Correct.
Q And -- but, as we've talked about, there might be multiple reasons to look at an account; right?
A There could be, yeah.
Q So it's not just that the United States or

Mr. Hylton here would be looking at who committed the crime; right?
A It's possible.
Q You'd be looking at maybe who also had some other involvement; right?
A Correct.
Q And that's what you would do when you were in law enforcement; right?
A Correct.
Q Okay. You'd run to ground everything you could?
A Sure.
Q Okay.

MR. SIMON: Nothing further, Your Honor.

THE COURT: Redirect?

REDIRECT EXAMINATION

BY MS. KOENIG:

Q A few questions, Mr. McInvaille. Thank you for your testimony today.

I wanted to make sure that I understood what you were saying in response to Mr. Simon's questions. You've worked on several geofence warrants; is that right?
A Correct.
Q Or cases involving geofence data.

A Correct.
Q And did you say that just the teams that you've worked with have never sought this extended discovery that we have sought here?
A Correct. I've never seen it requested.
Q And when did you first start seeing, in your practice, these geofence warrants come about?
A I believe I have one from a 2017 case.
Q Would it be logical, then, to see more litigation as a new technique comes out?
A Absolutely.
Q And if we were able to go -- let's go through -- so, in going through -- you testified on cross-examination that we don't know exactly what we would be able to get from Google until we ask for it; right?
A Correct.
Q And if we were able to get information from Google that indicated how they came up with this process, how would that inform our ability to look at the legality of this warrant that they sought?

MR. SIMON: Objection, Your Honor. I don't know what his basis would be to know the legality of it.

THE COURT: I actually think that calls for a

legal conclusion, and he's not a lawyer.
BY MS. KOENIG:
Q How would that inform our understanding of the data?
A It could help you understand, of course, these display radiuses, how they determine that that's what they approximate. It could tell us more about the -- for instance, in the Wi-Fi, if they record what Wi-Fi was used to generate those points. Several of those items could help you better understand how they came up with the data that they provided.
Q Let's break it down a little bit. So, you've talked about how Google provided an estimate of the display radius; right? Do we have any way of checking that with any degree of certainty?
A No.
Q And the only way we can get that is if we get the method that Google used to create that radius; right?
A Correct.
Q And is that what we generally think would be encompassed in the algorithm?
A I would assume so, or at least their processes of generating this evidence.
Q When we say "algorithm," what do we kind of mean?
A I think more than, you know, than we're looking at

some elaborate mathematics here, that it's more of just maybe what you guys are referring to and that we've been talking about. It's more of their underlying process of taking unknown data or their location history data and turning it into what we see here.

Q And then going -- you know, you were able to talk with us about a couple of examples of Mr. Blue, Mr. Green, Ms. Yellow as to what we think a path of travel may indicate; right?

A Yes.

Q And if we were able to have the access point, if we knew that you had an access point, what would you then be able to do to help us assess the accuracy of the data that's indicated to come from a Wi-Fi source?

A That would just give you the known location that Google used to approximate this location. Then you can -- if you wanted to, you could go try to determine those locations, try your best to determine if it was -- if it seems like an appropriate estimate of the location or not.

Q And if you have the Wi-Fi access point, would you be able to take some kind of a device and go out and map the range of a Wi-Fi source?

A To an extent, yes, you could go find out where the

access point is and where you might be able to access it from.

Q And so, for instance, if we were able to get data from Google that indicated that a device ID had connected with the hotel Wi-Fi access point, could you roughly map out the range of the hotel Wi-Fi access point?

A Again, knowing the location of whatever access point was used, if it still exists and is there and has not been changed, you could generally determine maybe how far away from that location you could be and still connect to it.

Q Would that enable us to better understand how some individuals who appear to be passing by this area of the red circle, how they possibly got captured into the circle even though the data indicates that they may not have actually stayed at that location?

A It could help, yes.

Q In terms of -- and I want to go back to Defense Exhibit 1, which is the warrant --

THE COURT: Before you go there, I just want to be clear. As to Defense Exhibit 3, column G says "Maps Display Radius (m)." Can we confirm that it's meters?

Q Do you understand that to mean "meters"?

A Yes, it's meters.

MS. KOENIG: Thank you, Your Honor.

MR. SIMON: That's my understanding, Judge.

THE COURT: Okay. I just want to be clear.

MS. KOENIG: Sure.

BY MS. KOENIG:

Q When we are talking about the warrant itself, is the warrant indicating to the judge that they obtained this warrant from, is the application for the warrant indicating that they are looking for suspects?

A Yes, I do believe it is.

Q You don't recall any mention to the judge, "Well, maybe we're going to look for witnesses to the event" -- right? -- by trying to get this geofence data?

A Bear with me just a second. I know it asked for unknown subject. I don't recall about others. Bear with me. The quotation there references other people, but that was a quotation, I believe, that they alleged by the suspect, but -- I don't know that -- bear with me. I may not see it, but -- I don't see anything that refers to, based on what the law enforcement wrote, that there is any mention of witnesses, but again --

Q Thank you, Mr. McInvaille.

Does it -- going back again to -- so, have you

actually plotted out all 19 people?
A Yes.
Q And have you plotted out the extensive data for all nine individuals?
A Yes.
Q Were you able to determine that the examples that we provided are not just isolated in the sense that it's not just these three individuals whose data appeared odd to you?
A When we say "odd," I think that's referring to just some of those that have single points within the circle and no other data to really go off of. And then based on once you see the larger set of data, you see a trend as though they're passing by. So that is what makes it appear that the point that references them into the documentation actually reveals their anonymous ID number in there.
Q When we're trying to get information from the law enforcement agents or the government about why they chose to narrow the 19 down to the 9, why is that? Why do we need that information? What does that mean to you?
A For me, it would help understand just the -- the reasoning behind certain people making it to certain points. For the case, that would help me understand

the -- you know, how things are playing out as far as this data goes.

Q And if you were better able to understand why the government did what they did, would you be better able to assist Mr. Price, and myself, and Mr. Chatrie, eventually, as to what this selection process meant?

A Sure.

Q And if we were to get -- so, you mentioned -- far earlier in your testimony today, Mr. Price had asked you, are you aware that Google does provide trainings on this geofence data?

A I don't know that it comes directly from Google, but there are places to get training that I've seen for Google location history services, that mix of data.

Q Was there at least one time where you tried to sign up for such a training?

A Yeah. I believe there was a webinar that detailed information about these types of requests and how to frame them and use them.

Q Were you able to successfully sign up for that?

A No.

Q Why was that?

A It was restricted to law enforcement only.

Q Did you then do some further checking and find

that Google -- that whoever is providing this information about the geofence warrants, that information seems to be restricted to law enforcement?
A From what I've seen, yes, it is.
Q Okay. And if you were able to access those training materials, would you anticipate that you would then be better able to understand how Google used this process and provided the information?
A I can only assume so, but I would assume a training on that particular subject could help in the understanding of different factors involved with these.
Q Likewise, that same thing with Google's policies and procedures about how they search the data and how they create this location data, would that also assist us in understanding if it existed, and it was provided, how this information applies in our case?
A Yes, because, I mean, you see the difference in what the government has asked but in comparison to what Google said in their brief as to what they provided. So there's something in place that kept them from fully responding. I don't know if that's the proper way to put it, but providing exactly what the government asked for.
Q Is it fair to basically sum it up to say that

there's a lot of questions that we have that you've done your best to answer, but you just can't because you don't have this data from Google?

A Yes.

MS. KOENIG: No further questions, Your Honor.

THE COURT: All right. Can this witness be excused?

MS. KOENIG: Yes, Your Honor.

MR. SIMON: Judge, could I just ask a few more questions on recross?

THE COURT: That's not our norm. Is there an objection from the defense?

MS. KOENIG: No, Your Honor, unless it elicits something else, if I could have the last word.

THE COURT: We're definitely not going down that rabbit hole.

MR. SIMON: That's fine. It's not a huge deal.

THE COURT: All right.

So, sir, thank you for your testimony. You're excused from testifying.

THE WITNESS: Thank you.

(The witness was excused from the witness stand.)

MS. KOENIG: Your Honor, the defense has no further witnesses at this time.

THE COURT: All right. Is there any evidence from the government?

MR. SIMON: Your Honor, no, we won't elicit any testimony.

THE COURT: All right. Well, I'll hear argument.

MS. KOENIG: Your Honor, could we take just a few minutes of a break? Mr. Price, he would love to eat a little bit of a sandwich first.

THE COURT: All right. We do not want anyone passing out in the courtroom.

MS. KOENIG: Thank you, Your Honor.

THE COURT: Again, I'm keeping it to ten minutes just to keep us on schedule.

MS. KOENIG: We can make that happen.

THE COURT: We'll take a ten-minute recess.

(Recess taken from 2:25 p.m. until 2:35 p.m.)

THE COURT: All right. I'm prepared to hear argument. I want to make one thing clear because both parties here were asking our witness, our expert, about what the judge decided. And I want to be clear, in Chesterfield County, magistrates are not judges. So this person who signed it appears to be David

Bishop. And as far as I recall, to be a magistrate in a county, all you need is a college degree. You don't even need a master's, and you definitely don't need a J.D. And because you all have been using the nomenclature "judge," I want to have you all respond to that, if you could.

MS. KOENIG: I think that the Court's recollection is accurate, Your Honor. I think we just get so used to seeing magistrate judges in this building sign off on warrants. It's a colloquial term, and it is does not indicate the person has a J.D. necessarily or significant legal training of any sort.

THE COURT: Well, I need something on the record about that. I think you have to have some kind of college degree. I think we don't know if this person has anything other than a college degree because the record is blank as to that.

MS. KOENIG: That's right.

THE COURT: All right. Mr. Simon.

MR. SIMON: Judge, I can't speak with 100 percent certainty as to rules in Chesterfield, but it is my understanding, as a general matter, that the Court is correct, that you don't have to be a lawyer with a J.D. or --

MR. DUFFEY: Judge, I'm sorry to interrupt. We would ask for time to check that because I know that used to be the rule, but something tells me they changed that, that there is a requirement. Could we file something?

THE COURT: Yes, I would want you to file it. Everybody referred to it the same way. So I'd prefer that you all, if you can agree to what the requirement is, file it jointly on the record.

MR. SIMON: Will do, Judge.

MR. DUFFEY: Let's do that.

THE COURT: I don't claim to know whether or not that's changed.

MR. PRICE: Your Honor, it is apparent that we are not dealing with an ordinary search warrant here. It's not an ordinary search. It's not an ordinary warrant. And it's also apparent that we are not dealing with an ordinary amicus. Nothing about this case is ordinary. And that is the point.

That is why the defense is requesting the discovery that we are requesting here. And it's also why we believe that the search in this case involves an unconstitutional general warrant that is infinitely overbroad and profoundly lacking in particularity.

Think about the extraordinary breadth here.

Google initially is searching all of its users in order to identify who might be in that circle. More than 1.2 billion of them. It is hard to imagine how you end up with a broader search than that regardless of who ends up in the circle.

But even that circle is not what it seems. And that's what we learned here today. Google says its data points are not facts but estimates. And if these are estimates, then we need to know how Google is making those calculations. We need to know what goes into it in terms of the inputs. That would be the Wi-Fi location points. As well as what Google does with that information. That would be the algorithm.

It's also why defense is asking for Google's policies and procedures in terms of responding to this. It is absolutely unclear to us why Google may have -- and we're not even certain they did -- why Google may have included only location history in this warrant return.

They have other types of location data. The government requested those in the warrant. The warrant does not specify location history versus some other type of location data. So there's a factual question lingering here about whether the data was

limited to that one category or not, and if so, why.

If it wasn't limited to location history, then we have a whole set of other questions about how voluntary that location data transmission was.

Location history, Your Honor, is arguably the most voluntary of the three. That's not to say it is voluntary in the Fourth Amendment sense, but as you can tell from the setup process, the first two types of location data, web and app activity and Google location services, are enabled by default and really require no affirmative action on the part of the user other that signing in with your Google account when you start up the phone.

So if those two types of data aren't at issue, then the argument about lack of voluntariness, for example, gets even stronger than it is here.

That also speaks to the lack of particularity in this warrant. Again, it is as unclear to us as it perhaps was to the issuing magistrate that this data would be searching everybody, that it would potentially expand beyond the scope of that radius. And, frankly, that it may not be as anonymous as the government and Google insinuate that it is.

The lack of particularity in this case cuts from beginning to end, from the information presented

to the magistrate about the scope of the warrant, about how anonymous that data really is.

In the middle, the government goes back to Google in step 2 and asks for additional information on all 19 users that were identified in step 1. It's not clear why they did that, but that certainly doesn't seem to be the thrust of the warrant and application that were presented. In fact, the warrant only says that the government will attempt to narrow it down. It is unclear whether they attempted here or what that attempt looked like. But in two instances, they went back to Google and asked for information about all 19 again. It doesn't appear that the government narrowed its request until the third time.

THE COURT: Well, to be fair, they said if you think the 19 is unreasonable, take the top 9; right?

MR. PRICE: And that is absolutely the language that we're focusing on here, Your Honor. It does appear that the reasonableness determination was left up to Google and not a judicial officer.

THE COURT: What's the upshot of that?

MR. PRICE: Well, the Fourth Amendment requires particularity in the search, that the government present all the information that it has

that's relevant to the judge. And the process of narrowing here is one of those limiting factors that a judge would presumably consider when deciding whether to issue a warrant like this.

So if there is a representation that the government is going to narrow down its list or that it's going to, in some way, limit the scope of what it asks for, that's information that needs to be presented to the Court, not to Google. And it's great that Google decided to, on its own, limit the scope of the step 2 returns, but that, unfortunately, does not absolve the government when it comes to particularity. The *Groves v. Ramirez* case decided by the Supreme Court just a few years ago made that point clear.

Even if the limitation, as a practical matter, comes from law enforcement or the responding party, that is not the same thing as a judge making that determination.

And the fact that it may cut one way in one case doesn't mean that it's not going to cut the other way in a different case, and that is why the determination is left up to the courts and not to Google.

THE COURT: Are you arguing at all about whether or not the fact that it was limited in some

respect -- you seem to argue it was limited by Google and not the government. Are you arguing either under Rule 16 that that suggests any kind of joint investigation or that under *Brady* it makes Google a member of the prosecution team?

MR. PRICE: So, our position here, Your Honor, is that Google did function as a member of the investigative team. And I think it is important to look at that in the broad sense. These policies and procedures do not appear to have been created in a vacuum. And the process of requesting data in steps and pseudo anonymizing it appears to be something that a lot of thought was given to. Our question is whether that thought and that process involved the government as well.

And it is unclear, for example, why Google may have chosen location history to provide as opposed to web and app activity or Google location services. Why?

I do believe that if we were to receive discovery from Google or the government about this process, this would likely not be the first time that Google and the government have talked about how the process should go.

So to the extent that Google is creating this

process, is responding to the government without any judicial intervention in between them, at least for step 2 and step 3, would seem to indicate that Google and the government -- at least for those steps, if not for the process more broadly -- were, in fact, working together.

And for Rule 16 purposes, that would subject Google to discovery in the same way that the government would be required to process discovery.

THE COURT: Well, let me ask you this: I told you at the beginning of this hearing that you were going to have to address the government's argument about 17(c). And so why aren't you just issuing a subpoena to Google?

MR. PRICE: Honestly, Your Honor, we considered it. And then Google interjected and decided to file an amicus brief in this case.

Our understanding of the way that Google has responded to subpoenas in the past has been to oppose them fiercely and to move to quash any sort of subpoena like this.

So we were, frankly, a little surprised but also happy that Google, on its own, decided to submit what we would consider to be an initial round of discovery, an affidavit, in the form of an amicus

brief.

And so at this point we would like the opportunity to follow up on that with them.

THE COURT: So why follow up now through justice argument rather than by issuing a subpoena?

MR. PRICE: If Your Honor feels it would be helpful, we would be more than happy to issue a subpoena to Google.

THE COURT: I don't give legal advice to either side, but I'm asking why you don't do it.

MR. PRICE: The reason that we didn't do it was because Google, in a somewhat extraordinary move, decided to come into this case on its own and provide an amicus brief with information relevant to some of the questions that we had in discovery. In fact, their brief does answer some of those questions. The problem is that it doesn't answer others, and it raises even more.

THE COURT: All right. Go ahead. Keep arguing.

MR. PRICE: I was going to say, even at the end of this process it is unclear how we get from point A to point B. It is not clear how the government went from 19 down to 9 to 3 requesting additional information about users who were, as we

learned today, pretty clearly unconnected to the crime.

If you have somebody who only hits once in the church, not the bank, and all of the other stage 2 data shows that that person was likely to be just driving next to the road -- on the road next to the bank, it does raise a question about why that person then advanced to stage 3.

Was the government just curious? It's unclear to us. And the fact that there is no judicial process after the warrant is signed initially I think raises serious questions about the propriety of the government or Google getting to decide which users get de-anonymized at the end. And especially given some of the candidates that made it to step 3, it doesn't appear that there is an obvious explanation. So we would like to know more information about how that process worked.

With respect to voluntariness, this is an issue because the government is arguing that there was no search here at all because this information was shared voluntarily with a third party, Google. In fact, what we learned is that that can be accomplished in a matter of minutes, in under five minutes, simply by clicking on "yes, I'm in" without any reference to

location history whatsoever.

So there is this factual question lingering here about how voluntary this is. How many people actually click "yes, I'm in"? That, to us, seems to be a pretty important fact to have here. And it doesn't seem likely that people are going into the depths of their settings on their telephones to enable location history specifically. So it raises the question: How is this happening? How is it happening if it's not really that intentional? And it does seem to be occurring through these pop-up screens. And so we want to know how common this is. Does this happen with most people or is it rare?

THE COURT: But what does that go to as far as what I have to decide? So, if you learn the percentages -- I'm looking at a motion for discovery under *Brady* and Rule 16. So, if you find out the percentages, what does that go to?

MR. PRICE: It ultimately goes to the merits of our suppression argument. The Supreme Court in *Carpenter*, for example, talked about the ubiquity of cell phones and the way that they are used today, the way that most people have them, they may as well be appendages. And if that is similar with respect to location history, in other words, if we were to learn

that 95 percent of users have location history enabled, it brings us much more in line with the reasoning in *Carpenter* about voluntariness. So that would be the relevance here.

The same goes for information about the inclusion of web and app activity and Google location services. So those are those other two types of data that Google supposedly didn't turn over. But if those were involved in this process, if they fed into location history, for example, then I do think we would be having an entirely different conversation about voluntariness.

THE COURT: So, one of the things I'm struggling with in this case is I'm going back to materiality, and I need you all to educate me about this a little bit. But materiality talks about, for instance, under Rule 16, whether or not it significantly alters the quantum of proof in the defendant's favor if the evidence is suppressed. Right?

And so is there a different kind of standard for materiality under evidence that would support a motion to suppress rather than evidence that supports information at trial, a defense at trial?

A lot of these cases are post trial, right?

And so we're dealing with something that might be a unicorn. I don't know if I've seen anything like it. I think if you had something dead-on, both of you would have given it to me, but I'm not sure that I see that.

So, is there a difference if you're trying to get information for a motion to suppress versus information for your actual defense?

MR. PRICE: So, we haven't, obviously, gotten into the trial phase of this case. In fact, Your Honor, we hope not to get to that phase and believe that this motion is, in fact, dispositive. And I believe the government actually agrees with us on that point.

If the defense succeeds on its motion to suppress, that will be the deciding point, I believe, in this case. And if the Court were to suppress the results of the geofence warrant, presumably that would entail the suppression of all the fruits thereof, and there would be no more case. So --

THE COURT: Well, that actually goes to another question that I have. I don't think that your brief included anything about fruit of the poisonous tree, but the United States made clear that there's this plethora of information other than what was found

through the geofence and the Sensorvault information that makes it -- I can't remember, actually, what they argued. I don't know if it's harmless error or -- it doesn't matter because there's just tons of information that otherwise shows guilt by a great degree.

MR. PRICE: I'm sorry. I don't have my suppression motion in front of me, but I am certain, Your Honor, that we asked to suppress both the results of the geofence warrant and their fruits.

And it is my understanding that the only way that the government came to have any physical evidence in this case was as a result of learning my client's identity from that geofence warrant, and that absent the geofence warrant, there would be no physical evidence.

If the government is planning to make an independent source argument, we haven't seen it.

THE COURT: All right.

MR. PRICE: I would add that it appears the government has the same question as the defense when it comes to the inclusion of only location history. It is certainly not what the government asked for in its warrant. And it appears that this is a policy that Google has internally. It is unclear to what

extent the government was aware of it, but it seems as if they were not here. And we are both wondering why Google responded the way that it did.

In short, Your Honor, I think we're -- what we're asking for, if I can sum it up, is fairly straightforward. It's the Google policies and procedures relating to geofence warrants. We want to know about location history versus web and app activity and Google location services. We want to know the percentage of devices that have these features enabled. We would like to know about the Wi-Fi access points and the algorithm used to determine an estimate of location based on that. And we would like information about the narrowing process.

Every one of those pieces of discovery goes to either breadth, particularity, or voluntariness. They are material, central to each one of those arguments. And to round out the point here, Your Honor, we believe the information about those is, well, required under both Rule 16 and *Brady*.

I understand your point about not having an ultimate outcome in this case, but if we tweak Rule 16 or interpret Rule 16 and *Brady* to mean the outcome of the suppression hearing and thus the outcome of the case, then we think under either standard we would be

entitled to the discovery we are seeking today.

THE COURT: So, the United States is basically saying there's nothing written -- I think their briefing says there's nothing written about what they do to narrow down the process. And so you just need to wait until the detective -- I think it was Hylton -- testifies. Why is that not correct?

MR. PRICE: So, we have asked the government for information about the analyst who did the work here. It's not clear that that was Detective Hylton. It's not clear what his process was. We would love the opportunity to discuss it with him and to discuss it with Google.

THE COURT: The analyst where?

MR. PRICE: Whoever for law enforcement was responsible for the narrowing process, what information they used to make that determination, presumably, in addition to what they received from Google.

THE COURT: All right. Okay.

MR. PRICE: All right. Thank you very much, Your Honor.

THE COURT: Thank you.

MR. SIMON: Judge, just to start where they ended, with respect to the culling down of the

anonymous identifiers, the folks we went from 19 to 9 on, Detective Hylton made that decision. And the Court was correct on our representation about that. That testimony will be provided, but there's no current documentation that would sort of fall within the ambit of discovery rules. And I think what we are doing in this case is commensurate with what is done in all cases. And rightfully so. There's no requirement to create a document like that. The testimony will be presented, and he will be cross-examined, I'm sure forcefully.

And with respect to any other analyst involved here, Special Agent D'Errico, who we were considering calling, certainly they will be provided expert notice as to his testimony. And the Court has already ordered that to be produced on February 3. So we will fall in line with the requirements there.

With respect to Detective Hylton, who did make the determination on culling them down, we will elicit testimony from him on that point, but there's nothing currently in hand.

With respect to Google, there is some discussion -- I think the Court hit the point straight on. Rule 17 provides a process by which you get documents from a third party if you want more than

what, in this case, magistrate order process, legal process provided. That is the standard.

It sounds like the defense counsel acknowledges that, is willing to undertake that process. And to the extent that it's difficult, I think that's neither here nor there for the Court. It's just a process that has to be undertaken and is considered in the Federal Rules of Criminal Procedure.

With respect to the point about Google sort of working hand-in-hand with the United States, that point's been briefed in this case. There's no -- there's really no -- how do I say it? -- sort of substance to that claim.

Google did what was required of it in relation to court-ordered magistrate order process. And the negotiation piece there, there were several emails brought to the Court's attention today. All of those indicate -- right? -- that there is some pushback potentially from Google. And certainly to the extent that we want something from them, we can't compel that from them personally. It all goes back to that search warrant.

But more importantly, the cases cited by the defendant sort of noting when a company like Google -- when a third party might be -- not a company like

Google, but a third party might be brought into the -- being a part of the investigative team for purposes of *Brady*, which is really the only point there, because we don't believe there's a constructive possession or a due diligence requirement under Rule 16. The most recent Fourth Circuit precedent is somewhat old, but it's very clear that there is no constructive possession. It's got to have been actual control.

And so we're clear there that --

THE COURT: The issue there wouldn't be constructive possession. It would be joint investigation under Rule 16.

MR. SIMON: Under Rule 16. But, Your Honor, my point is is that there is no joint investigative team precedent in this circuit under Rule 16 in terms of producing something under Rule 16. But we would concede that to the extent they were to be seen as an agent in this case for the government, much like, I guess, a special agent, we'd have to certainly produce documents created in that course. So I guess as a practical matter, it ultimately does extend to that *Brady* sort of joint prosecution consideration. But under Rule 16, the *Pinto* decision is clear. There's no -- when the bail bondsman right there has the document, says you don't have to get that, there's no

construction possession. They're not a part of your prosecution team or they're not a part of the prosecution.

And so I guess there is sort of --

THE COURT: Well, what the defense is saying is that it's a little bit fact bound, right? I mean, the cases that have dealt with this do suggest that, in the Fourth Circuit or not, do suggest that if the more sort of independence and collaboration that goes on between a third party and the government, the more likely it is considered under Rule 16 or under *Brady* to either be a joint investigation or the entity to be a member of the prosecution team. It's not quite as black and white as you say, I don't think.

MR. SIMON: Sure. And, Judge, just to -- and I understand the Court's point. Even considering that, even acknowledging the point about the fact-bound nature of the inquiry as to whether we turn over stuff in the possession of Google that we don't have, the cases cited by the defendant don't support their viewpoint. And we've briefed that point, but every one of those cases, one, there's no process mandated from a magistrate saying you have to turn this over pursuant to the Fourth Amendment probable cause being found under Rule 41 for this evidence, the

search warrant.

And certainly, unlike those cases, Google is not brought into this case to prepare documents for purposes of this investigation.

So, *McCormick*, I guess, is the case out of the Tenth Circuit, and all the other cases are state court decisions from California, but they all focus on folks who are literally brought into the prosecution for purposes of the prosecution, and the documents and anything they can provide is for purposes of the prosecution.

Just from a factual standpoint, Google is providing to us business records that they created in the course of their business that they provided and didn't create because the United States started investigating the defendant in this case. These are just documents that they had in their possession. So, that's a meaningful difference in terms of sort of how they come into this process.

And it would also go to the broader Sixth Amendment piece, which is kind of an argument made in the reply brief that these business records are not testimony for purposes of the Sixth Amendment. I think there's clear case law on that point.

Google is not involved in this investigation

because we went to Google and said, We need you to create some documents or do something for purposes of this investigation. What they had were business records that they turned over.

But even considering cases where there might be more of a sort of private hybrid, the cases cited by the United States, the decision in the Seventh Circuit, which I think is the *Gray* decision, which talked about sort of Indiana hiring a private entity to do some work on behalf of Medicare. And they had documents created in the course of their business that were relevant to the prosecution. They turned those over, but that didn't turn that private company into an arm of the prosecution and as part of the investigation.

There's also the more -- sort of the legal point here, which is the *Collins* decision in the Southern District of New York, which says you have to consider the fact that even if the United States wanted to go back and tell Google to turn this over, it's necessarily circumscribed by the basis upon which they got the information in the first place. Right?

So, in *Collins*, they wanted to go back and search -- they wanted -- the defendant wanted the United States to go back and search the computer of

somebody who had provided previous consent. And the District Court there said they can't do that. They have to -- they can't just tell the individual to turn over their computer. That would be much the same way.

I think Google has made it clear in this case that they respond to legal process. They don't respond to the United States saying, "Give us documents or else." They don't respond to the United States saying, "We're investigating something and thus you need to participate and help us out." And that's just the reality of the situation.

We had to -- we were required to get process, and that's what happened here. And that's why Google is engaged with this investigation at all.

And even with respect to the stage 2 -- right? -- so stage 1 you just turn over the coordinates inside the radius, and in stage 2 there's an attempt to narrow down to get additional location information. So, basically, a total of two hours of location information was gathered for only nine devices. But that second stage gives you 30 minutes before and 30 minutes after. So that's what defense counsel has referred to as that culling down process.

That process is set forth in the search warrant. And there's some discussion of what Google

turned over and why they sought to turn over certain documents. The numbered page 2 of Defense Exhibit 1, which is the search warrant in this case, particularly attachment 2, says Google will provide anonymized information regarding the accounts that are associated with the 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, the time stamp, location coordinates, and the data source that this information came from, if available. That's what was provided in this case.

We received latitude-longitude coordinates. We received a time stamp on them. We received the source; Wi-Fi, GPS, and otherwise. I think it's Wi-Fi and GPS. And so the search warrant's pretty clear about what's being requested.

And the bottom line as it relates to the possession, custody, and control argument, whether it be under Rule 16, which plainly lays that out, is that there's no case law supporting the premise. And the underlying premise is very simple. Once you get a search warrant, and once you serve it on a Yahoo!, a Google, an Apple, an AT&T, if they respond in accordance with that search warrant, they are part of

your investigation team.

And to the extent that there's a broad search here, there's a broad search also in those cases as well. I think to the extent that there's a second stage here, that would be the only argument that would really be any -- would provide any meaningful difference or any difference in this case. I don't believe it -- meaningful because, again, it's provided for in the warrant. There's no -- there's no Google correspondence with the United States with no regard for that warrant. So everything is circumscribed by that. And I believe the reasoning out of the Southern District of New York in the *Collins* decision is to that point, that the defendant has to acknowledge, even based on their own argument, that we can't just go to Google and tell Google to turn over an account without some legal process.

In this case, if you argue there's a reasonable expectation of privacy, that's a search warrant. And so we think it's clear that Rule 17, Federal Rule of Criminal Procedure 17, provides the basis upon which the defendant would get these materials from Google.

And both parties over the course of -- now I guess it's been a few months -- received an email from

Google's outside counsel, reaching out to both sides talking about the amicus brief. So we certainly have known who the sort of lead lawyer for Google has been for some time. And even before that the defendant knew who we had corresponded with, who the United States had corresponded with in terms of executing this warrant. And so that goes back to the *Cameron* decision from the District Court in Maine, which, again, I think, is insightful. They know who to serve the subpoena on. They've got it. And they can go about that process. Again, it seems that they've acknowledged that that is the path to take for a third party and to receive these documents. And should Google seek to quash that subpoena, that would be analyzed under Rule 17, and appropriately so.

THE COURT: If it is the case that they decide to issue a subpoena to Google, what happens next?

MR. SIMON: Judge, I think that's where this is, as the Court noted, a more difficult situation. It is a hybrid, right? So, the defendant has noted -- has argued that Rule 16 should apply in reference to a suppression hearing in terms of sort of this third-party request for materials.

The only decision cited for that is a

District Court decision that applied a 1970's Fourth Circuit decision that had nothing to do with Rule 16. I think that was cited in the *Cranson* decision out of the Fourth Circuit. It has nothing to do with Rule 16.

And what we know from the Supreme Court is that when we talk about materiality, we're talking about in preparation for the defendant's defense, the Supreme Court says that goes to rebutting the government's case-in-chief, and arguably you could say we certainly can see that the geofence warrant is how we know this defendant was the target of the investigation.

So, there could be an argument that that's enough to be a part of the government's case-in-chief as opposed to a constitutional claim, which we believe this is, that doesn't really go to the merits of the evidence against the defendant.

And so in *Armstrong*, that was a selective prosecution claim, said the prosecution shouldn't have been brought. It's unconstitutionally -- they proceeded on an unconstitutional basis or there shouldn't be a prosecution. And the Supreme Court made clear that there should be a different standard there when it comes to a claim like that. That does

not go to the defendant's defense. The defendant's defense is actually rebutting against the government's case-in-chief.

This is a little different because there's evidence -- there's evidence gathered from the search warrant in this case. So I'd acknowledge that.

But ultimately, this case can proceed, I believe, to a suppression hearing without ordering Google to turn these documents over. I say that for a few reasons, because there are undisputed facts. There are undisputed facts as to there being other Google users whose information was collected as a part of this warrant. Undisputed 19. It's undisputed that Google has many, many, many users. Probably can be part of the public record how many users Google has or how many people are sort of a part of Google's customer base.

Irrespective of how many, the Court's going to have to acknowledge that there are over certainly a million, and if we go to a billion -- I don't know the number, but it's out there how many people Google does business with.

It's also undisputed that we've got location information for these people that expands outside of the box for stage 2. All right. So we know that

there are nine people's information we received that was outside the box for stage 2.

There's been no evidence elicited in this case that any information received in step 1 was necessarily from somebody who was outside of the box of that stage 1 search warrant at stage 1.

And so I think the real facts that are at issue are really undisputed. We say there are a lot of Google users, that it's voluntary. Even their witness said yes, it's voluntary. And the question, the voluntariness question, to the extent it's informed by *Carpenter*, the *Carpenter* decision -- and, again, this isn't the suppression hearing, and we're going to argue that issue when it comes up, but the *Carpenter* decision talked about the ubiquity of using cellular telephones by powering them on and maybe them hitting off of a cell tower, and that this information occurs over, I think, a seven-day -- basically, the cell towers collect this information once you power the phone on. Everybody has to use it.

I don't think there's any argument in this case that you necessarily have to use Google to have a cell phone, certainly not to talk on it, certainly not to text on it, certainly not to travel. There are other applications to use to travel.

And so to the extent that the litigation needs to be prolonged for purposes of this information, I don't necessarily see it, but that ultimately would be an issue that Google addresses in response to a Rule 17 subpoena responding to whether this information is relevant, whether it's oppressive, and the other considerations that go with Rule 17. But it's my position that the Court can proceed to address the constitutionality of this warrant on the basis of certain undisputed facts as set forth.

I don't think this information from Google is going to give the Court any more understanding than what has been provided, that there are lots of users.

THE COURT: Let me ask you this: The defense said that there's an issue about it only being location history and not the other information. So, respond to that.

MR. SIMON: Again, the search warrant request for time stamp location coordinates and the data source for those coordinates, that's what this search warrant provided. It's not clear to me at all that that is somehow a material issue in this case. I mean, how would that be material to -- and the Court was asking about sort of how you apply that standard, but how would that be material to the accuracy of this

information? Because, ultimately, that's one of the pieces that goes to sort of the merits of the claim. What value would more points give us --

THE COURT: The expert testified that it doesn't normally just say location history. And I don't have anything to the contrary, right?

MR. SIMON: Judge, no, that -- I mean, what I can tell you is that what we -- certainly what he responded to in terms of this geofence warrant to get that, this is what Google provides, and there was some, I think, lack of clarity about what this search warrant asks for. But this search warrant says to provide the time stamp location coordinates and data source for each type of Google account.

There is another search warrant in this case that is for historical Google information. That's been made part of this record in this case, and there is -- there is some sort of web activity and sources like that, but that is sort of about the broader count. It's not clear to me that geofence warrants, at any point, provide more than what we've been provided here.

THE COURT: But he testified they do. It may not be clear to you, but you can't testify to this.

MR. SIMON: Well, Your Honor, I believe the

record will show that the witness, when asked whether the information provided in response to a geofence warrant has been in addition to what we have here, he said no. I think he did state that with respect to warrants that go to other types, when it's a user-specific search warrant, you know which account you're going after, then you get that additional information, but not with respect to the geofence search warrant.

THE COURT: Okay.

MR. SIMON: And, Judge, I do think that it is -- with respect to significantly altering the quantum of proof, I think the Court has that correct, that that has to be the standard. And with respect to how you apply that standard, it is backward-looking in a case where we haven't gone to trial yet, but I think it's undisputed that evidence was found at these three different locations, that there was a statement of probable cause, that there was certainly an admission post-Miranda in this case to the crime. And so materially altering the quantum of evidence from a Rule 16 standpoint --

THE COURT: You have to agree that the way you got there is through the geofence information.

MR. SIMON: That's right, Judge.

THE COURT: So it's a little bit problematic to say, Listen, once we identified the guy, then we knew which house to search, and then we got everything. Then the way we identified him was through the geofence warrant, but we're not going to say the geofence warrant is material because once we used it to go to his house, there was all this other proof. That strikes me as too much tautology for the government in this case.

MR. SIMON: And I understand that point, Judge, and I think that's correct, that the first -- we can't deny that everything else flowed from the geofence warrant.

Materiality goes to, I think, something more than just saying sort of what happens, like how material was the geofence warrant to the case. Materiality goes to whether we're going to be led, based on articulable facts, to something that is going to significantly alter the quantum of proof for this Court.

There is not a single request made by the defendant in this case that is going to significantly alter the quantum of proof because, again, we've agreed on certain basic points. Google --

THE COURT: Okay. I think I've got that

argument.

MR. SIMON: Okay.

THE COURT: All right. Is there any response?

MS. KOENIG: Very briefly, Judge. As it relates to -- because I think we've got two separate pieces. We have -- one is the information we're requesting from the government about how they made the process themselves to go down from 19 to 9 to 3. And that doesn't involve the question of getting Google involved.

THE COURT: So, you're away from the microphone.

MS. KOENIG: I'm sorry.

THE COURT: I heard about every fourth word.

MS. KOENIG: Sorry. I want to start with the first question, which is the information that we have sought from the government about how their actual investigators, Detective Hylton and anybody else that was involved in that process, narrowed down the scope of the data sought from the 19, to the 9, to the 3. That doesn't involve this issue about whether Google was on the investigative team. I think it's very clear that Detective Hylton would be a part of the investigative team.

THE COURT: Why isn't it enough that they say they don't have to create information for you, just wait until he testifies?

MS. KOENIG: So, we could do it that way. But the reason we cited the case that we cited, which is *Wilford* from the District of Maryland -- and this is at least the quickest place I can put my hands on it is in our reply brief, on page 9 of the reply brief related to the discovery motion.

And I think the mechanics of how this would work is we could do discovery finding on the stand, but what Detective Hylton would essentially be testifying to is I plotted all these points, and I had the 19, down to the 9, down to the 3, and here's the reasons why. We're then going to have to be able to very quickly -- and I don't know physically how we would do this because we would have to essentially have access to Mr. McInvaille's entire mapping process, which, you know, we showed you 3 pathways today, but there would be 19 pathways. And the reason I think that the *Wilford* court required the material information related to pretrial motions must be produced before the motions hearing is to ensure its effective use.

I think we would be wasting a lot of the

Court's time in some senses because we would need to take a break, take Mr. McInvaille back in the back, have him show us how this all works so that we could cross-examine the detective. So that's problem number one.

And problem number two, I think, is all we need to do is interview Detective Hylton. We've asked for that conversation to happen. I know Mr. Duffey, very, very early on in this case, had suggested that maybe we could do that, and then that discussion fell through, and then here we are.

But I think it matters, as we've talked about, that the crux of this case at this juncture is the motion to suppress.

I did want to, before moving on to the last few points, make sure that when the materials that we're seeking -- one item which we had in small print on our prepared materials Mr. Price accidently left out, in addition to the policies and procedures and the Wi-Fi points and those lists that he had provided. We are seeking also information about the process that Google used to create this anonymous ID that they listed as device ID in column A on the stage 1 and 2 returns.

The device -- as we've indicated, I think, in

some of the briefing, there is some concern that we have that that ID is not necessarily just something that was generated for the purposes of this warrant. Perhaps it's related to or is a number that resides on an individual phone.

If that is the case, then that means that that number is a Google tracking number, that yes, it doesn't have Laura Koenig or someone else's name attached to it, but it is not anonymous in the sense that it cannot be refound. So that's another point that we wanted to make sure we're clear on that's what we're requesting.

I think point number two, as it relates to Google, is that the government, I think, in sum, is availing themselves of this process. And if Google isn't made to provide the information that we are seeking, then we have a limited, ineffective way to be able to test the data, its accuracy, its range, the radius that Google has turned over. And that's why we're seeking, as we've discussed, the access points, the algorithm, or whatever process Google uses to do that.

I think it is important, imperative, for us to remember that unlike some of the other analogies that the government is drawing to other types of

subpoenas or warrants that are served on technology companies like, for example, call detail records, those are business records. Google has stated in its amicus brief that the data that it provided, this is not a business record that Google keeps. Google has to, instead of searching one user's account, search all 1.2 billion of its users is what they proffered. That makes this a very different type of search than the analogies that we have been talking about.

In terms of Mr. Simon's representation that we agree on some things, I think we need to know the details for this Court and any reviewing court, should that become necessary, to be able to work with. Are we talking about a million users? Are we talking about a billion users? Those numbers make a difference. They made a difference to the Court in *Carpenter*, and I anticipate that any future Court, as well as this Court, need to know that information to be able to effectively decide the issues in this case.

Last point, in terms of what Mr. McInvaille had testified about, the location history versus the web activity and the Google location services, he had indicated that the cases that he has worked on where there was an individual user's data sought had come with an indication of the source of that, whether it

was the web activity or the Google location services or location history.

In the geofence data, what I understood him to say is that in the geofence data he has seen in other cases, just as in this case, there is no indication on the spreadsheets that Google provides as to what the source of that data is. That information only comes in the amicus brief, and that's why we're seeking to be able to test that through cross-examination, not simply from a proffer from Google.

Thank you, Your Honor.

THE COURT: All right.

All right. I'm going to get my thoughts together for about ten minutes, and then I'm going to speak to you about my response to your argument.

All right. We'll take a recess.

(Recess taken from 3:30 p.m. until 3:50 p.m.)

THE COURT: All right. Well, clearly, we have in front of us a case of first impression involving technology that both parties, to some degree, are claiming ignorance to and which affects what has been received by the government in a manner that implicates important Fourth Amendment and federal rules issues.

So, here, I have a couple of concerns about what is before me. So, one is your first set of briefing was very good. It did not separate out the standards of materiality under Rule 16 and *Brady*. And it did not separate out how the Court should find whether or not there's a joint investigative team under Rule 16, and, separately, whether Google would be a member of the prosecution team under *Brady*.

So we can't merge those standards because they are different. If they end up being the same, then you have to tell me why. And I do think we have some absence of facts, but the issue, of course, really is how the record I have now affects, first, materiality, and materiality as it pertains in this case looking forward.

So, you all have to do some thinking about how you take a standard that is based on cases that are on habeas usually or appeal, about how it would affect it backward to what happens here as to how it would affect a decision looking forward. It's an importantly different procedural posture.

And just concluding that it would affect materiality needs to be explicated a little bit more under each standard. And you have to use the language that I'm going to have to apply, which is looking

forward, not looking backward, and whether that changes anything. If you don't think it changes anything, then tell me that. And tell me why you don't think it changes anything.

There's note passing. Do you want to say something to me?

MS. KOENIG: No, Your Honor. I was just trying to anticipate where the Court may be going, thinking we will probably want to get a transcript. And I just simply passed a note to say did they want to split the cost of the transcript. I'm sorry that we were note passing.

THE COURT: All right. So, I do want additional briefing. I want it based on the testimony today and the evidence that is currently before the Court. So you probably will need a transcript. You figure out how to pay for it.

And I do think that there is some continued dispute as to exactly what standards apply and how. And I want you to tell me what to do about that before we get into the suppression hearing itself.

So, whatever the government may or may not have any obligation to turn over, the process of narrowing down, I'm just going to tell you there's some practical sense of whether or not Mr. Chatrie is

going to be able to cross-examine that on the fly, whether that's practical, because it's a lot of information.

And so I'm going to ask you to take that into consideration. We can have a two-part hearing. We can do whatever you think is appropriate.

We are in a different procedural posture here, and I do believe that the parties should address some of the things that they disagreed about, some of the things they've agreed about. Certainly I need to know about what the magistrate is just so that's on the record and clear about who that is.

I'm happy to have you all file that by Friday. I think that's a single Westlaw search, and I'm hopeful it can be a joint stipulation. It may or may not matter. I just want to be clear because everybody kept saying "judge."

So I don't know how quickly we can get a transcript.

(Discussion with the court reporter.)

THE COURT: I'll tell you, based on what I have in front of me, this would be my proposed schedule. I would continue with the expert disclosures. I think that's going to help flesh out the record, in any event. And we're going to have a

motion to suppress one way or the other. Is there any objection to that?

MR. SIMON: No objection, Judge.

MS. KOENIG: Not from the defense, Judge.

THE COURT: All right. I think that's going to help you submit your information.

You can speak with the court reporter as to when you will be able to get a transcript, but in any event, you can be planning your arguments with respect to the legal aspects in the meantime.

I'm willing to wait for complete briefs both as to materiality and as to member of the prosecution team or joint investigation until February 18. That gives you plenty of time to address those issues. Obviously, it means we will not have the motion to suppress on the 20th and the 21st.

And I do want you to address the issues that have come up today. Just give me the information that you think I need, and why, and apply the law as I actually have to apply it as far as the standards and as far as the facts.

On the 18th, I would like you to file cross motions as to materiality and as to the joint investigation, including the facts and the standards that have to apply.

Then I want responsive cross motions on the 25th, seven days later. And you all can address whether or not you seek more argument, whether you seek more evidentiary hearing, whatever you want to address in your first motion. And then I will take it under advisement and schedule what I think is appropriate once I have the full record on the 25th.

All right?

MR. SIMON: Yes. Thank you, Judge.

MS. KOENIG: I understand. Thank you.

THE COURT: So I am going to say that I think you all are working hard at this. It is a case of first impression, and it is coming at a weird procedural posture. I think that when we're talking about a warrant that implicates even a million folks who we can presume at least a million minus two of them were definitely not involved in the robbery, we have to be really careful about what we're doing.

And certainly if it's a billion, I think that's something that we really have to be careful about, and I want to be careful about how I find my record. So that either way, I may get it wrong, but I'm going to make as good a record as I can, based on what I have, and you all are helping me do that, but I can't do it just yet. It's a lot of information, and

it's new technology, and I really need to get it right.

So, is there anything else?

MR. SIMON: Judge, are you sufficient -- are we sufficiently good on the Rule 17 piece here? There need not be additional briefing there, right?

THE COURT: I think both parties here acknowledged it was an option; right?

MR. SIMON: Correct, Judge.

THE COURT: I am disinclined to give a party instructions about what to do. Some things seem more straightforward than others, but that's not for me to say. I don't think I can give advice. I don't think I need further briefing because it's certainly an option. And it's an option I think even if Google is a member of the prosecution team. It is a belts-and-suspenders issue. All right? Does that answer your question?

MR. SIMON: Yes, Judge.

THE COURT: Ms. Koenig, do you have any comments or questions?

MS. KOENIG: I do not, Your Honor. Thank you.

THE COURT: All right. Okay. Thank you all for your efforts. I know it was a long day.

(The proceedings were adjourned at 4:00 p.m.)

I, Diane J. Daffron, certify that the foregoing is a correct transcript from the record of proceedings in the above-entitled matter.

/s/

_____ _____

DIANE J. DAFFRON, RPR, CCR DATE

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 SUPPLEMENTAL MOTION TO SUPPRESS EVIDENCE OBTAINED FROM A "GEOFENCE" GENERAL WARRANT

Okello Chatrie, through counsel, submits this supplement to his motion to suppress all evidence and fruits obtained from a "geofence" general warrant, ECF No. 29, pursuant to the Court's Order entered on May 13, 2020. *See* ECF No. 103.

INTRODUCTION

This case turns on a novel and invasive form of electronic surveillance, a so-called "geofence" warrant, involving the search of "numerous tens of millions" of Google users to generate a single investigatory lead. *See* ECF No. 96-1 at 4. Local police had no suspects in the robbery of the Call Federal Credit Union, so they decided to enlist Google to sleuth for them. Investigators went to a Virginia magistrate and, without conveying critical information, obtained a staggeringly broad and unparticularized warrant to go fishing in a pool of private location data that most people have never heard of. They demanded the location information associated with all Google users who happened to be in the vicinity of the bank during rush hour on a Monday evening, and thus, caused Google to search numerous tens of millions of accounts at their behest.

The basic facts involved are found in Mr. Chatrie's initial motion to suppress, *see* ECF No. 29 at 4-7. In short, the warrant followed a three-step process Google developed: "Step One" required Google to search all user accounts and provide "anonymized information" about any

devices in the area during the 30 minutes on either side of the robbery. In response, Google searched every user with "Location History" enabled and estimated that 19 devices were within 150 meters of the bank during that one-hour timeframe. Next, in "Step Two," investigators were to cull the list from Step One, after which Google would produce additional, "anonymized" location information about devices of interest for one hour on either side of the robbery (*i.e.*, two hours total), without geographic restriction. But instead of culling the list, investigators demanded additional information on all 19 devices—multiple times. Google did not comply until investigators identified a subset of nine users for further scrutiny. Finally, at "Step Three," investigators narrowed the list to three devices of interest and obtained de-anonymized information about those Google users. One of the three devices belonged to Mr. Chatrie, who became the government's primary suspect. As the government agrees, *see* 1/21/20 Tr. at 172-73, all of the evidence implicating Mr. Chatrie in this crime emanates from this Google geofence search.

From the beginning, Mr. Chatrie has urged this Court to find that such a warrant is unconstitutional, both categorically and on the facts of this case, because it is fatally overbroad and lacks the particularity required by the Fourth Amendment. *See* ECF No. 29 at 3. Since Mr. Chatrie made his initial motion to suppress, however, Google has filed an *amicus* brief and two affidavits that clarify and magnify the scope of the privacy intrusion worked by the government in this case. *See* ECF Nos. 59-1 & 96. The Court also heard testimony from a digital forensics expert, Spencer McInvaille. *See* 1/21/20 Tr. Mr. Chatrie sought leave to file a supplemental motion and present these new facts to the Court in advance of further testimony and argument, and in support of his motion to suppress all evidence obtained from the geofence warrant, as well as all fruits thereof. The Court granted Mr. Chatrie's request and subsequently extended the filing deadline to May 22, 2020. *See* ECF Nos. 101 & 103.

Mr. Chatrie had a reasonable expectation of privacy in his Google Location History records. As the Supreme Court recently recognized in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), such data is capable of revealing the "privacies of life" and is therefore constitutionally protected. *Id.* at 2214. It can reveal who is inside a home, church, or hotel—all of which are implicated here. The ability to access this Google data grants the government unprecedented surveillance powers, enabling investigators to locate individuals quickly, cheaply, and retroactively. This may be a boon to law enforcement, but it is also a Fourth Amendment search, just as it was in *Carpenter*. *Id* at 2230.

The so-called "third-party doctrine" does not apply to Location History records, and therefore a *valid* warrant—*i.e.*, one that is properly particularized and supported by probable cause—should be required in order for law enforcement to access it.

Location History records are qualitatively different than the "business records" that have fallen into the traditional third-party exception, such as bank deposit slips or telephone numbers dialed. *See United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979); *see also Carpenter*, 138 S. Ct. at 2216–17. As the Supreme Court has recently and repeatedly articulated, digital is different. *See id.* at 2214; *Riley v. California*, 573 U.S. 373, 393 (2014) (comparing a physical search to the search of a cell phone is like "saying a ride on horseback is materially indistinguishable from a flight to the moon"); *United States v. Jones*, 132 S. Ct. 945, 957 (2012) (the third-party doctrine is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks") (Sotomayor, J., concurring). As a result, any extension of old rules to digital data "has to rest on its own bottom." *Riley*, 134 S. Ct. at 2489.

In this case, Mr. Chatrie did not "voluntarily" convey his cell phone location data to Google in any meaningful way. Like many Google users, he did not knowingly or intentionally "opt-in" to Google's Location History service. And like the cell site location information in *Carpenter*, his Location History data is not subject to the third-party doctrine.

While the government obtained a warrant in this case, it did not obtain one for Mr. Chatrie's Location History data. In fact, it did not seek anyone's data in particular. Rather, the government compelled Google to search *everyone's* data in order to develop an investigative lead. This warrant was unconstitutional. It was both overbroad and lacking in particularly, a forbidden general warrant purporting to authorize a dragnet search of Google users. It did not—and could not—satisfy the Fourth Amendment's probable cause and particularity requirements, rendering it wholly impermissible and void from the beginning. Indeed, it was so deficient that no objectively reasonable officer could rely on it, and as a result, Mr. Chatrie asks this Court to suppress all evidence obtained as a result, as well as all fruits of the poisonous tree.

NEW FACTS

Mr. Chatrie initially characterized the geofence warrant in this case as "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." ECF No. 29 at 3. At the time, Mr. Chatrie understood this search to encompass "a trove of private location information belonging to 19 unknown Google users" who were within 150 meters of the bank. *Id.* But that, it turns out, was just the tip of a gargantuan iceberg. As Google now explains, the geofence search involved not just 19 users near the bank, but "roughly one-third of active Google users (i.e., numerous tens of millions of Google users)." ECF No. 96-1 at 3.

Geofence warrants differ from other types of law enforcement requests, entailing a uniquely broad search of all Google users who have "Location History" enabled on their devices. *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*; *see also* 1/21/20 Tr. at 21. Here, the warrant did not identify Mr. Chatrie in any way. Nor did it identify any of the users whose personal information was searched and turned over to law enforcement. Instead, the warrant operated in reverse: it required Google to identify users with Location History records and then allowed police full discretion to cull through this private information for devices of interest.

Geofence warrants require Google to produce data regarding all Google users who were within a geographic area during a given window of time. But, as Google explains, there is "no way to know ex ante which users may have [Location History] data indicating their potential presence in particular areas at particular times." *Id.* at 12. Thus, in order to comply with the request, Google must "search across all [Location History] journal entries to identify users with potentially responsive 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." *Id.* at 12-13.

Location History records are one of three types of user location information maintained by Google. If a user has the Google Location History service enabled, then Google estimates the user's device location using GPS signals, signals from nearby Wi-Fi networks, Bluetooth beacons, or cell phone towers. *See* ECF 96-1 at 4. Google saves this information on a map in each user's "Timeline," *id.* at 2, which Google describes as a "digital journal" of a user's locations and travels. *See* ECF No. 59-1 at 16. Google considers this information to be communications "content" for

purposes of the Stored Communications Act, 18 U.S.C. § 2703, requiring the government to obtain a warrant supported by probable cause in order to access it. *See id*.

In addition to Location History records, Google maintains separate databases for user location information derived from two other Google services: "Web & App Activity" and "Google Location Accuracy." Web & App Activity is on by default and it saves location information generated from activities like running a Google Search or using a Google application such as Google Maps, Gmail, or YouTube. *See* ECF No. 96-1 at 5; 1/21/20 Tr. at 23; *In Re Google Location History Litigation*, No. 5:18-cv-05062-EJD (N.D. Cal. Dec. 19, 2019). Google uses this data to provide "a more personalized experience" through "faster searches and more helpful app and content recommendations." ECF No. 96-1 at 5. Google asserts that it did not search the Web & App Activity database in this case because that database does "not store a user's location at a level of detail precise enough to be responsive to a geofence warrant."[1]

Google Location Accuracy, formerly known as "Google Location Services," works on Android devices and is also enabled by default. It estimates a device's location using GPS data, Wi-Fi access points, Bluetooth sensors, and mobile network information. *See* ECF No. 96-1 at 6; 1/21/20 Tr. at 23. Google uses this information to improve location accuracy by estimating the physical location of Wi-Fi access points, Bluetooth beacons, and cell phone towers based on the GPS coordinates transmitted by devices that interact with those networks. *See* ECF No. 96-1 at 6-7; 1/21/20 Tr. at 64-65. "In other words," explains Google, "[Google Location Accuracy] data might be used by the device to calculate a location data point that is stored in [Location History.]"

[1] Google states that Web & App Activity data "reflects a device's location to an approximate area of at least one square kilometer" and is "therefore too coarse to be responsive to the warrant," which initially entailed a search area with a 150-meter radius. ECF No. 96-1 at 8.

Id. at 6.[2] Google asserts, however, that it did not directly search the Google Location Accuracy database in response to the geofence warrant because the data is "not stored with user identifiers" and is "used in an anonymous way." *Id.*

Thus, even though the geofence warrant required Google to produce location data for "each type" of Google account inside the geofence, *see* ECF No. 54-1 at 4, 9, Google did not do so. Instead, Google says that it only searched the Location History database, not the Web & App Activity or Google Location Accuracy databases. *See* ECF No. 59-1 at 12; ECF No. 96-1 at 7-8. According to Google, Location History is the only form of data that is "sufficiently granular" and searchable to be responsive to a geofence request. ECF No. 96-1 at 7.

Consequently, Google did not search the contents of every Google user in order to respond to the warrant. Instead, it searched those users with Location History enabled on their accounts—*i.e.,* the "Sensorvault." But this is no small number. It amounts to "roughly one-third of active Google users." *Id.* at 4. Not even Google, however, knows precisely how many users it searched in this case. *Id.* Rather, Google estimates that "numerous tens of millions of Google users" had Location History enabled in 2019, all of whom had their accounts searched in order to identify 19 users who were, perhaps, roughly within 150 meters of the bank. *Id.*[3]

Of critical importance is that, in practice, the effective range of the geofence was more than double 150 meters. As a result, at least some of the 19 users identified by Google were likely never within the 150-meter geofence at all. As Google states, "it is possible that when Google is

[2] When estimating a user's location through the Location History service, Google appears to use historical location data from other users, stored in the Google Location Accuracy database, to estimate a device's likely GPS coordinates based on the presence and strength of known nearby Wi-Fi, Bluetooth, and cell phone tower signals. For example, if many devices transmit a similar set of GPS coordinates when they "see" a particular Wi-Fi network, then Google may attribute those GPS coordinates to a device that later "sees" the same Wi-Fi network if GPS is unavailable for that device.

[3] Thus, assuming Google has two billion active users, a third of which is 660 million (*i.e.*, twice the population of the United States), then 19 users represent a hit rate of 0.0000029%.

compelled to return data in response to a geofence request, some of the users whose locations are estimated to be within the radius described in the warrant (and whose data is therefore induced in a data production) were in fact located outside the radius." *Id.* at 9; *see also* ECF No. 59-1 at 20 n.12 (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."); 1/21/20 Tr. at 65. This phenomenon is a product of how Google calculates a user's location based on "multiple inputs," including the strength of nearby Wi-Fi signals. ECF No. 96-1 at 8; *see also supra* n.2. According to Google, the latitude/longitude coordinates saved in Location History records do not necessarily reflect a user's actual location, *id.*, but are "probabilistic estimates," each with a different "margin of error." ECF No. 59-1 at 10 n.7. Google presents that margin of error as a "Map Display Radius," which is often depicted on a map as a shaded blue circle extending outwards from the "blue dot" indicating the user's estimated location. ECF No. 96-1 at 9. Importantly, there is only an "estimated 68% chance that the user is actually within the shaded circle surrounding that blue dot." *Id.* Or in other words, chances are better than 1-in-5 that the user is outside of the shaded circle altogether.[4]

Google has provided numerical values for the margins of error in this case, the largest of which is 387 meters from coordinates near the center of the 150-meter geofence. *See* ECF No. 68 Ex. A at 6-12, 17-37. Figure 1, below, depicts the 150-meter geofence in red and the 387-meter margin of error in yellow. That margin of error indicates that at least one user[5] could have been more than 387 meters away from the bank—and more than 237 meters outside the geofence—but

[4] The size of the margin of error depends on the user location data available to Google. For example, coordinates obtained from GPS signals are more accurate than coordinates derived from Wi-Fi signals. *See* 1/21/20 Tr. at 64. In this case, 88% of the coordinates at issue were derived from Wi-Fi signals, as opposed to GPS. *Id.* None were derived from Bluetooth or cell phone tower data.
[5] "Device ID" number 702354289.

was nonetheless swept into the dragnet. In fact, Google is only 68% confident that the user was not even farther away than 387 meters. Put it another way, the yellow line indicates the minimum effective range of the geofence in this case, which is more than twice what the warrant authorized.

Figure 1

The true reach of the geofence, therefore, included not only a major thoroughfare (U.S. Route 360), the bank, and the Journey Christian Church, but also another road next to the church, a Ruby Tuesday restaurant, a Hampton Inn hotel, a mini storage facility, an apartment complex for seniors, and another residential apartment complex. *See* Tr. 1/21/20 at 66-67. Numerically, the 150-meter radius covered an area of 78,000 square meters, or about 17 acres, whereas the effective range was 470,000 square meters, or about 116 acres—an increase of more than 500 percent.

ARGUMENT

Execution of the geofence warrant was an unconstitutional search that intruded upon Mr. Chatrie's reasonable expectation of privacy in his Google location data. As Mr. Chatrie contends, the warrant was invalid because it was a general warrant, fatally overbroad and devoid of particularity, and therefore impermissible under the Fourth Amendment. *See* ECF No. 29 at 7, 16-24. Moreover, the warrant was *void ab initio*—so obviously deficient from the beginning that the search must be regarded as warrantless. As a result, the good-faith doctrine does not apply and the results of the search, including all of its fruits, should be suppressed.

I. The Geofence Warrant Intruded on Mr. Chatrie's Reasonable Expectation of Privacy in His Location History Records.

As Mr. Chatrie argues in his initial motion to suppress, the Supreme Court's recent decision in *Carpenter* applies to mobile location data obtained from Google just as much as similar data obtained from a cellular service provider. *See* 138 S. Ct. 22; ECF No. 29 at 7-11. Narrowly construed, *Carpenter* found a reasonable expectation of privacy in seven days of historical cell-site location information ("CSLI"), *id*. at 2217, because seven days was the shortest amount of time on the record before the Court. *See* ECF No. 48 at 2-4. Nonetheless, *Carpenter's* reasoning applies with at least equal force here. As Justice Gorsuch noted in dissent, presciently: "[W]hat distinguishes historical data from real-time data, or seven days of a single person's data from a download of *everyone*'s data over some indefinite period of time? . . . On what possible basis could such mass data collection survive the Court's test while collecting a single person's data does not?" *Id.* at 2267 (emphasis in original). The government struggles to argue that technical differences compel a different conclusion here, but Justice Gorsuch is correct. There are no principled distinctions to be had.

The government's primary objection centers on the length of the search, which covered two hours during rush hour on a Monday evening in Richmond, as opposed to the seven days at issue in *Carpenter*. But by "declin[ing] to determine whether there is a 'limited period' for which the government can acquire cell phone location information without implicating the Fourth Amendment," ECF No. 41 at 7, the Supreme Court did not give the government a free pass to obtain less than seven days of location data without a warrant. (In fact, the government's demand for seven days of data in *Carpenter* netted only two days of data. *See* 138 S. Ct. at 2212.)

On the contrary, the Supreme Court has repeatedly expressed concern that even short-term location tracking may constitute a search. *See Jones*, 565 U.S. at 415 (Sotomayor, J., concurring); *accord Carpenter*, 138 S. Ct. at 2215. Indeed, there are significant privacy implications involved in just 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." *Jones,* 565 U.S. at 415 (Sotomayor, J., concurring) (quoting *People v. Weaver*, 12 N.Y.3d 433, 441-442 (2009)). And this is especially true where the search reveals information about the interior of a constitutionally-protected space, such as a home. *See United States v. Karo*, 468 U.S. 705, 716 (1984) (finding that the use of a beeper to track a drum of chemicals into a private residence was a search); *see also Kyllo v. United States*, 533 U.S. 27, 37 ("The Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained."). Such intrusions are "presumptively unreasonable in the absence of a search warrant." *Katz v. United States,* 389 U.S. 347, 361 (1967); *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)).

In this case, the geofence search revealed Google users who were not only inside the bank, but also in nearby homes, apartment complexes, and, it would seem, the Journey Christian Church. *See* 1/21/20 Tr. at 80-82 (describing the data for "Mr. Green," which begins at a hospital, ends at a private residence, and incorrectly indicates he went into church); *id.* at 83-85 (describing the data for "Mr. Blue," which shows a trip to a private residence with start and end points in an apartment complex); *id.* at 88-90 (describing the data for "Ms. Yellow," which shows a trip from a single-family residence to Manchester High School, followed by two local businesses, and then a return trip home). While this data was supposedly "anonymized" by Google, the defense was able to ascertain the likely identities of Mr. Green, Mr. Blue, and Ms. Yellow based upon the addresses of the residences involved, their travel history, and other publicly available information. *See id.* at 83, 87-88, 90-91.

Google's handling of the data at issue lends further credence to the notion that any slice of Location History data is private, no matter how small. Google considers Location History to be communications "contents" for purposes of the Stored Communications Act, 18 U.S.C. § 2703, meaning that from a privacy perspective, it is on par with the contents of an email or personal documents stored remotely on Google Drive. *See* ECF No. 59-1 at 9, 17; ECF No. 72 at 3. Far from an ordinary "business record," Google considers Location History to be a "digital journal" of users' movements and travels. ECF No. 59-1 at 16. As a result, Google requires the government to obtain a warrant supported by probable cause in order to access Location History records. *Id.* at 15-18. There is no exception for two hours of private, invasive data.

Finally, Location History records are at least as accurate as the cell site location information ("CSLI") in *Carpenter*, and equally capable of revealing the "privacies of life." 138 S. Ct. at 2217. Initially, Mr. Chatrie argued that all of the records in this case were "more precise than the cell site

location at issue in *Carpenter*." ECF No. 29 at 12. But as Google's *amicus* brief makes clear, Google derives Location History coordinates from "multiple inputs," some of which are more accurate than CSLI and some of which are not. ECF 96-1 at 4. These "inputs" include GPS signals, which are highly accurate and can estimate a device's location within "approximately twenty meters or less." *Id*. But they may also include Wi-Fi, Bluetooth, and CSLI data, which is generally less accurate than GPS. *Id*. Google explains that "[c]ombined, these inputs . . . can be capable of estimating a device's location to a higher degree of accuracy and precision than is typical of CSLI." *Id*.[6]

Nonetheless, Location History is at least as accurate as CSLI, *i.e.*, the least accurate "input" that Google uses. Furthermore, the *Carpenter* Court equated CSLI and GPS for purposes of Fourth Amendment analysis. *See* 138 S. Ct. at 2217 ("As with GPS information, the time-stamped [CSLI] data provides an intimate window into a person's life, revealing . . . his particular movements") (internal citation omitted). And as *Carpenter* instructs, courts should anticipate advances in the accuracy of such technologies in order to "'assure [ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" 138 S. Ct. at 2214 (quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001)) (alteration in original); *accord United States v. Jones*, 565 U.S. 400, 406 (2012). When new technologies "encroach upon areas normally guarded from inquisitive eyes," *id.*, courts must remain vigilant "to ensure that the 'progress of science' does not erode Fourth Amendment protections." *Id.* at 2223. Indeed, not even the government finds a meaningful difference between CSLI and GPS, conceding that *Carpenter* "t[ook] account of

[6] At the same time, however, because Location History was developed for the purpose of targeting customer advertisements and not for impeccable surveillance, estimates based on CSLI or Wi-Fi signals may be far less accurate than estimates based on GPS tracking. Consequently, a geofence search may mistakenly identify some users as being within the radius who were in fact located outside of it. *Id.* at 9. In the case, Google appears to have identified at least one user inside the Journey Christian Church who was likely never in the church at all, and may in fact have been more than 387 meters away. *See supra* at 9-10.

more sophisticated systems" and recognized that CSLI "is rapidly approaching GPS-level precision." ECF No. 41 at 8.

In this case, the Location History records produced by Google involve a mix of GPS and Wi-Fi inputs, with approximately 12% coming from GPS and 88% coming from Wi-Fi signals. *See* 1/21/20 Tr. at 64. But the government did not and could not—because of the nature of the colossal search Google conducts in these types of cases—know in advance which sources of location data would ultimately be at issue. Rather, because GPS and CSLI are among the potential sources, the analytical assumption has to be that Location History records may be least as precise as the GPS or cell site signals in *Jones* and *Carpenter*.

II. The Third-Party Doctrine Does Not Diminish Mr. Chatrie's Expectation of Privacy in His Google Location Data.

The third-party doctrine does not apply to Location History records or diminish Mr. Chatrie's privacy interest in them. The doctrine generally holds that individuals do not have a reasonable expectation of privacy in information "voluntarily" conveyed to a third-party, but the *Carpenter* Court was clear that the rule is not to be "mechanically" applied in the digital age. 138 S. Ct. at 2219; *see also* ECF No. 29 at 9-11. Instead, *Carpenter* teaches that mobile location information is a "qualitatively different category" of data, distinct from the telephone numbers and bank records in *Miller*, 425 U.S. 435, or *Smith*, 442 U.S. 735. *See* 138 S. Ct. at 2216–17. The same reasoning applies here.

As Mr. Chatrie argues, "Google location records are qualitatively different from the business records to which the third-party doctrine traditionally applies." ECF No. 29 at 9. Unlike the numbers dialed in *Smith* or the bank deposit slips in *Miller*, Location History records are "detailed, encyclopedic, and effortlessly compiled," *Carpenter*, 138 S. Ct. at 2216, as well as deeply revealing. *See* ECF No. 29 at 12-13. Granting the government access to this information is

an unprecedented new surveillance power, akin to handing it a time machine capable of locating Google users in the past, all without expending finite physical resources like manpower or unmarked cars. *See id*. at 13-14. In short, it "gives police access to a category of information otherwise unknowable." *Carpenter*, 138 S. Ct. at 2218; *see also Prince Jones v. United States*, 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).

The government counters that Mr. Chatrie has "voluntarily" shared this data with Google because Location History is an "opt-in service." *See* ECF No. 41 at 10-12. Google also describes "several steps" that a user must take in order for Location History to function and save information. ECF 96-1 at 2-3; ECF 59-1 at 12. But a closer look at this "opt-in" process reveals that it is not nearly as informed or voluntary as Google and the government suggest. On the contrary, users may unknowingly enable the function without ever seeing the phrase "Location History" or being informed of the privacy implications of turning it on. *See* ECF No. 72 at 6-9; 1/21/20 Tr. at 56-57.

Following the standard setup of an Android phone like the one used by Mr. Chatrie, a user encounters a pop-up screen, reproduced in *Figure 2*, when opening the Google Maps application for the first time. *See* ECF No. 72 at 7; 1/21/20 Tr. at 56. It says, "Get the most from Google Maps" and then it gives the user two options: "YES I'M IN" or "SKIP." *Id.* There is also a statement that reads "Google needs to periodically store your location to improve route recommendations, search suggestions, and more" and a button to "LEARN MORE." ECF No. 72 at 7. The pop-up does not use the phase "Location History," but clicking on "YES I'M IN" enables the function. Clicking on "LEARN MORE" takes the user to a webpage with Google's complete Privacy Policy and Terms

of Service; it does not direct the user to any specific language concerning location data or Location History specifically. *See* 1/21/20 Tr. at 57.

In fact, Google's Terms of Service do not mention Location History at all. *See* Google, Terms of Service (Oct. 25, 2017).[7] And Google's Privacy Policy, which is 27 pages long, mentions Location History only twice. *See* Google, Privacy Policy at 4, 8 (Jan. 22, 2019).[8] In the first

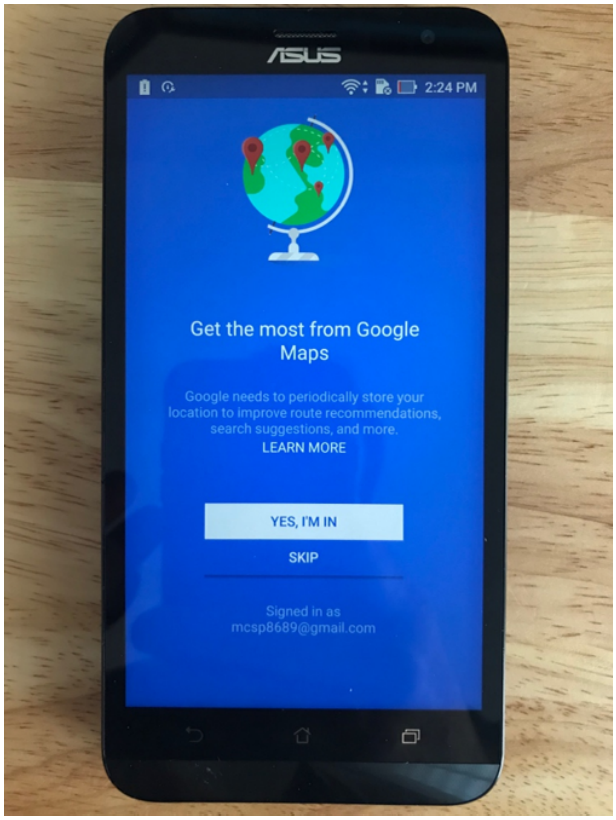

Figure 2

instance, it says, in full: "You can also turn on Location History if you want to create a private map of where you go with your signed-in devices." *Id.* at 4.[9] If anything, the phrase "private map"

[7] *Available at* https://policies.google.com/terms/archive/20171025.
[8] *Available at* https://www.gstatic.com/policies/privacy/pdf/20190122/f3294e95/google_privacy_policy_en.pdf.
[9] The Privacy Policy links to a current webpage with instructions on how to "Manage your Location History." The only date on the webpage is 2020 and it is not clear whether or what version of this page existed at the time Mr. Chatrie set up his phone.

is misleading and suggests that Google does not have access to the data. In the second instance, the policy says, in full: "Decide what types of activity you'd like saved in your account. For example, you can turn on Location History if you want traffic predictions for your daily commute, or you can save your YouTube Watch History to get better video suggestions." *Id*. at 8. Of course, "traffic predictions" do not begin to suggest that Google will keep a 24/7 "journal" of a user's whereabouts. But even if it did, a user would have no way of knowing that the pop-up "opt-in" screen relates to the Location History feature.

The pop-up does not reference "Location History" by name. As a result, a typical user would not know to scour Google's policies for references to Location History, much less understand the implications of the choice Google is asking them to make. In short, it is strikingly easy for a user to "opt-in" to Location History without ever being aware of doing so.

Consumer groups across Europe have filed complaints against Google over its location data practices, citing the deceptive design of the Location History "opt-in" process. *See Groups Across Europe File Complaints Against Google for Breach of GDPR*, The European Consumer Organisation (Nov. 27, 2018).[10] A complaint from Norway, for example, alleges that user consent to Location History tracking is not valid because it is not "freely given," "specific and informed," or "unambiguous." *Complaint to the Datatilsynet Under Article 77(1) of the European General Data Protection Regulation* at 8-12, Forbrukerrådet (Nov. 27, 2018).[11] Specifically, it argues that Location History can "be easily turned on involuntarily" and that the "relevant information regarding what Location History actually entails is hidden behind extra clicks and submenus, and the information about what the data is used for is ambiguous and unclear." *Id*. at 3, 11. It also

[10] *Available at* https://www.beuc.eu/publications/consumer-groups-across-europe-file-complaints-against-google-breach-gdpr/html.
[11] *Available at* https://fil.forbrukerradet.no/wp-content/uploads/2018/11/complaint-google-27-november-2018-final.pdf.

alleges that Google uses pop-up consent screens for Location History, similar to the one in Google Maps, in conjunction with other Google applications such as Google Assistant, the Google Search app, and Google Photos. *Id.* at 9. The cumulative effect is that a "user is repeatedly compelled to give consent using design patterns and biased notices," thereby increasing the likelihood that the user will "opt-in" by accident, out of frustration, or because of a belief that the services will not work otherwise. *Id*. In sum, "due to the deceptive design used by Google, it is not entirely clear for the user that she is actually giving consent to something, and even it was, it is not exactly clear to what she is consenting." *Id*. at 12; *see also Every Step You Take* at 16-23, Forbrukerrådet (Nov. 27, 2018) (the report on which the European complaints were based).[12]

On this side of the Atlantic, courts have been skeptical of so-called "clickwrap" contracts of adhesion. *See, e.g., Nguyen v. Barnes & Noble*, 763 F.3d 1171, 1175-76 (9th Cir. 2014) (categorizing "[c]ontracts formed on the Internet" as "clickwrap" or "browsewrap" depending on how they provide notice and seek assent); *Berkson v. Gogo*, 97 F. Supp. 3d 359, 395-401 (E.D.N.Y. 2015) (discussing "browsewrap," "clickwrap," "scrollwrap," and "sign-in-wrap"). Although the Fourth Circuit has not yet weighed in,[13] a recent opinion from this district is instructive. *See Melo v. Zumper*, No. 3:19-cv-621 (DJN), 2020 WL 465033, at *8-11 (E.D. Va. Jan. 28, 2020).

Like this case, *Zumper* involved a pop-up consent screen, but that is where the similarities end. The crucial question for the court in *Zumper* was "whether the website presented the terms

[12] *Available at* https://fil.forbrukerradet.no/wp-content/uploads/2018/11/27-11-18-every-step-you-take.pdf. The study's tests were performed "using a Samsung Galaxy S7 Android device running Android version 8.0.0" and then reproduced on a "Google Pixel device running Android 9." *Id.* at 6. While the "settings and device setup process may vary somewhat between devices," the results were "representative of a typical user experience." *Id*.; *see also* 1/21/20 Tr. at 36-37, 45-48 (discussing similarities in Location History prompts between Android versions).

[13] The Fourth Circuit in *A.V. ex rel. Vanderhye v. iParadigms*, LLC, 562 F.3d 630, 645 n.8 (4th Cir. 2009), "decline[d] to address the question of whether the terms of the Clickwrap Agreement created an enforceable contract."

and conditions in a hyperlink, and whether that hyperlink appeared clearly to the user." *Id.* at *9. In making this determination, the court considered the "placement of the terms and conditions hyperlink in relation to the button that grants a user access," "whether the terms and conditions hyperlink appeared to the user on multiple occasions," and "the overall design elements of the website, including font size and color, and other visual components that might hinder a user's reasonable notice." *Id.* at *9-10. In *Zumper*, the court concluded that the interface did provide sufficient notice of the company's terms and conditions because the company included a warning that "clearly stated that 'by creating a Zumper Account you indicate your acceptance of our Terms and Conditions and Privacy Policy," which were accessible through a conspicuous hyperlink directly below the "Create Account" button. *Id.* at *10-11.

In this case, by contrast, the "design and content" of Google's interface objectively obfuscates and discourages users from understanding what they are agreeing to. *See Berkson*, 97 F. Supp. 3d at 401. The pop-up here focused the user's attention on "get[ting] the most out of Google Maps" and did not mention Location History at all, let alone explain what clicking "YES, I'M IN" would entail. *See* Figure 2, *supra*; 1/21/20 Tr. at 56.

Mr. Chatrie would have had to agree to Google's terms and conditions during the initial setup process of his phone. *See* 1/21/20 Tr. at 50. But unlike the pop-up in *Zumper*, he did not have to view or assent to the terms again when he encountered the pop-up "opt-in" screen. He was not required to click through the text of Google's terms before Location History collection began; a renewed reference to the terms was not displayed, prominently or otherwise. *Cf. Tradecomet.com v. Google*, 693 F. Supp. 2d 370, 377-78 (S.D.N.Y. Mar. 5, 2010) (clickwrap agreement was reasonably communicated where the user "had to click through the text of that agreement" in order to agree"); *Moore v. Microsoft Corp.*, 293 A.D.2d 587, 587 (N.Y. 2002) (finding assent where the

terms were "prominently displayed on the program user's computer screen before the software could be installed" and the user was required to "click[] on the 'I agree' icon before proceeding with the download of the software."); *Feldman v. Google, Inc.*, 513 F. Supp. 2d 229, 237 (E.D. Pa. 2007) (finding notice and assent where "the user had to visit a webpage which displayed the Agreement in a scrollable text box," there was a "prominent admonition in boldface to read the terms and conditions carefully," and the terms were "only seven paragraphs long—not so long so as to render scrolling down to view all of the terms inconvenient or impossible"). The prompt did not even use the words "I Agree" or "Terms and Conditions," which may have at least implied that users were giving up something. *See* 1/21/20 Tr. at 56-57.

A "LEARN MORE" button is no substitute for a clear statement that users are agreeing to something drastically new. After all, the initial setup process—the point at which Mr. Chatrie did have to accept Google's terms—indicates that Location History is *not enabled* by default. *See* 1/21/20 Tr. at 53. Nothing about the pop-up screen indicates that users would be reasonably informed that they are changing this default setting or opting-in to the Location History service. Providing a link to all of Google's policies and terms of service is meaningless without a clear indication of what is changing and where to look.

III. The Geofence Warrant Infringed on Mr. Chatrie's Property Interests in His Location History Records and Was Therefore a Fourth Amendment Search.

Mr. Chatrie reiterates that he has a property interest in his Location History records, which constitute his private "papers and effects." *See* ECF No. 29 at 14-16; ECF No. 48 at 8-10. Google is a mere bailee of these records and the government can only search and seize them with a valid warrant. *See* ECF No. 29 at 15-16. The government has yet to address the substance of this argument, dismissing it as a theory "rooted in Justice Gorsuch's solo dissent in *Carpenter*," ECF No. 41 at 12. The government simply does not engage with centuries of Supreme Court

jurisprudence that embraces—and continues to validate—a property-based understanding of the Fourth Amendment. *See* ECF No. 48 at 8-10; *Carpenter*, 138 S. Ct. at 2213-2214 ("[N]o single rubric definitively resolves which expectations of privacy are entitled to protection"); *Jones*, 565 U.S. at 406-07 ("For most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates. *Katz* did not repudiate that understanding."); *id.* at414 ("*Katz*'s reasonable-expectation-of-privacy test augmented, but did not displace or diminish, the common-law trespassory test that preceded it.") (Sotomayor, J., concurring); *Kyllo*, 533 U.S. at 40 ("well into the 20th century, our Fourth Amendment jurisprudence was tied to common-law trespass").

Mr. Chatrie fully adopts, incorporates, and re-asserts his property-based arguments here. *See* ECF No. 29 at 14-16; ECF No. 48 at 8-10. If anything, Google's repeated insistence that Location History data is a personal "journal" only solidifies this claim, even if it is not a journal that users know they are keeping. *See* ECF No. 59-1 at 16; ECF No. 96-1 at 9. Regardless of whether the Court analyzes Mr. Chatrie's claim under a property-based theory or the reasonable expectation of privacy framework set forth in *Katz*, the result is the same. The search of Mr. Chatrie's Google Location History records was a Fourth Amendment search.

IV. The Geofence Warrant Was an Unconstitutional General Warrant, Fatally Overbroad and Lacking Particularity.

Mr. Chatrie also renews his argument that geofence warrants are inherently unconstitutional. They are the epitome of the indiscriminate, "dragnet"-style searches that the Supreme Court has repeatedly warned against—and that the Framers fought a revolution to prevent. *See* ECF No. 29 at 16-23. Indeed, the Supreme Court has never upheld anything remotely approaching the search of "numerous tens of millions" of people. *See* ECF No. 96-1 at 4. The new facts presented by Google in its *amicus* brief and affidavits only confirm that the warrant in this

case was uniquely overbroad and so lacking in particularity that it can only be described as the digital equivalent of an impermissible general warrant.

A. Overbreadth

The geofence warrant here did not—and could not—meet the probable cause or particularity requirements demanded by the Fourth Amendment. It did not identify any individuals or accounts to be searched because investigators did not know who they were searching for, or even if Google would have relevant data. *See* ECF No. 29 at 23. Nothing in the warrant application indicates that the bank robber was a Google user or had Location History enabled at the time of the robbery. *Id*. Instead, the application rested on broad conjecture based on the popularity of Google and cell phones generally. *See* ECF No. 29 at 23; ECF No. 48 at 19.

From the outset, the government enlisted Google to search untold *millions* of unknown accounts in one of the largest fishing expeditions in Fourth Amendment history. The number of individuals affected by this case dwarfs the number of people searched in any other reported criminal opinion. Even controversial "tower dumps," which are exceedingly broad in their own right, tend to impact hundreds or thousands of people at most. *See, e.g., United States v. James*, No. 18-CR-216, 2019 WL 325231, at *3 (D. Minn. Jan. 25, 2019) ("hundreds if not thousands" of cell phone users); *In re Cell Tower Records Under 18 U.S.C. 2703(D)*, 90 F. Supp. 3d 673, 676 (S.D. Tex. 2015) ("several thousand phone numbers"); *United States v. Pembrook*, 119 F. Supp. 3d 577, 586 (E.D. Mich. 2015) ("potentially hundreds"); *In re Application of the U.S.A. for an Order Pursuant to 18 U.S.C. 2703(c), 2703(d)*, 42 F. Supp. 3d 511, 513 (S.D.N.Y. 2014) ("hundreds or thousands"); *In re Search of Cellular Tel. Towers*, 945 F. Supp. 2d 769, 770 (S.D. Tex. 2013) (**"**hundreds, or even thousands").

A tower dump requires cell phone service providers to produce the records of every device connected to a particular cell tower or towers during a particular time. *See* ECF 59-1 at 14. But as a practical matter, the number of people affected is limited by the number of cell phone users who were present at the time—*i.e.*, hundreds or thousands, depending on the area and the time. The difference with geofence searches is that there is no such practical upper limit. Rather, Google asserts that it 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*. Consequently, the number of users searched using a geofence warrant is bound only by the number of Google users with Location History enabled, which Google estimates to be in the "numerous tens of millions." ECF No. 96-1 at 4.

The government cites to the "Playpen" cases as a justification for the breadth of the search here. *See* ECF No. 41 at 19-20. Those cases arose from a warrant that searched users who logged into a child pornography website temporarily run by the FBI. The scheme was one of the largest sting operations in history, but it still only involved "approximately nine thousand" computers globally. *See* Order on Defendants' Motion to Dismiss Indictment at 5, 12, *United States v. Tippens*, No. 16-05110-RJB (W.D. Wash. Nov. 30, 2016) (ECF No. 106). Moreover, users had to take numerous affirmative steps to access and log into the website, making it "extremely unlikely for someone to stumble innocently upon Playpen." *United States v. Matish*, 193 F. Supp. 3d 585, 603 (E.D. Va. 2016); *see also United States v. McLamb*, 880 F.3d 685, 688 (4th Cir. 2018) (noting that in order to access Playpen, a user must download special software 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). By contrast, there was no government honeypot in this case, and there is

no argument that using Location History or being near the Call Federal Credit Union is inherently suspicious. *See* ECF No. 48 at 13.

The fact that Google produced the records belonging to 19 of these users does not diminish the scope of the initial search conducted at the government's behest. Unlike scenarios where a company must search defined records to identify responsive data, the search here did not identify any specific users or accounts to be searched. Instead, the warrant forced Google to act as an adjunct detective, scouring the accounts of numerous tens of millions of users with Location History enabled in order to generate a lead for the government. That the intimate, private data of numerous tens of millions of users were searched is the heart of the overbreadth analysis in this case. That records belonging to 19 people were ultimately produced does not lessen the massive, and illegal, search conducted in this case.

B. Particularity

A geofence warrant is overbroad by design, but it is also severely lacking in particularity. Apart from probable cause, the Fourth Amendment requires that warrants "particularly describ[e]" the place to be searched and the things to be seized. U.S. Const. amend. IV. The idea is to leave nothing to the discretion of the officers executing a warrant that a court has properly authorized. *See Marron v. United States*, 275 U.S. 192, 196 (1927). This is especially critical where, as here, a search implicates First Amendment concerns. *See* ECF No. 29 at 13, 22; ECF No. 48 at 3 n.3. If particularized, it should be obvious to all what officers can search and what they can seize. The exact opposite occurred here.

The geofence warrant left it up to Google and the government to negotiate which users would have their account information searched and further revealed to investigators—the hallmark of an unparticularized warrant. *See Steagald v. United States*, 451 U.S. 204, 220 (1981); *Stanford*

v. Texas, 379 U.S. 476, 482-83 (1965) (describing the "battle for individual liberty and privacy" as finally won when British courts stopped the "roving commissions" given authority to "search where they pleased"). As Mr. Chatrie contends, "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." ECF No. 29 at 23. At each step along the way, Google and the government—not the issuing magistrate—decided what data to search and what data to produce. Even the government now appears to agree that there was some "lack of clarity about what this search warrants asks for." 1/21/20 Tr. at 171.

At Step One, Google made critical decisions that would ordinarily be made by a judge, not the recipient of the warrant. First, Google decided to search only a portion of its records, specifically "Location History" records kept in the "Sensorvault." *See* ECF No 96-1 at 3. Google then decided to ignore the margins of error generated by its own calculations and "estimate" that 19 Google users were within the 150-meter geofence. In reality, at least five of those 19 users were never within the geofence at all.[14] Instead, Google guessed—inaccurately. One device could have been more than 387 meters away from the bank, and yet Google still identified its user as a potential suspect subject to additional search in Step Two.

During Step Two, the warrant said the government would "attempt" to narrow the Step One returns and then obtain additional location information on a subset of devices of interest. *See* ECF No. 54-1, Attach. I at 1-2; Attach. II at 2-3. The government did not try very hard. Instead, the government approached Google multiple times to press for expanded data on all 19 of the devices identified in Step One. First, Detective Hylton emailed Google on or about July 2, 2019, to request "additional location data (*i.e.*, step 2) and subscriber information (*i.e.*, step 3) for all 19

[14] Device IDs 702354289, -965610516, 907512662, 1135979718, and 2021066118.

device numbers produced in step 1." ECF No. 96-2 at 5; *see also* ECF No. 48 at 14, Ex. A at 1. On July 8, Det. Hylton called Google twice, and left two voicemails, presumably requesting the same. *Id*. A Google representative called Det. Hylton back and "explained the issues in the Detective's email as the request did not appear to follow the three sequential steps or the narrowing required by the search warrant." *Id*. Google also "explained the importance of step 2 in narrowing" to Det. Hylton. *Id.* At some point, the government emailed Google once again to ask for "additional location data and subscriber info" on all 19 devices identified in Step One. *See* ECF No. 48, Ex. B at 1.[15] In each email, Det. Hylton wrote to Google that, "If this request seems unreasonable, please keep in mind that device numbers 1-9 may fit the more likely profile of parties involved," but proceeded to request additional information on all 19 users anyway. *See* ECF No. 48, Ex. A at 1; *id.*, Ex. B at 1. Eventually, Det. Hylton acquiesced and emailed Google a third time to request additional information on 9 of the 19 users. *Id.*, Ex. C at 1. The third time around, Google complied.

The haggling between Google and Det. Hylton is emblematic of the absence of particularity in the geofence warrant. The Fourth Amendment demands that a neutral and detached magistrate make decisions about what to search and what to seize. This constitutional function cannot be outsourced to Google or to the police. As well-intentioned as Google may be, it is not up to Silicon Valley to determine what is "reasonable." *Cf.* ECF No. 48, Ex. A at 1; *id.*, Ex. B at 1 ("If this request seems unreasonable…"). That decision belongs to the judicial branch, and the judicial branch only. *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).

[15] The government has not provided the dates for either of the emails to Google.

Furthermore, a basic premise of the warrant was that the data returns in Step One and Step Two would be "anonymized." But as Mr. Chatrie has consistently argued, "[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; ECF No. 72 at 10; 1/21/20 Tr. at 83, 87-88, 90-91. On the contrary, every person takes a "unique path through life" that is "inherently identifiable." ECF No. 68 at 3; *see also* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701, 1716 (2010). And as Mr. Chatrie demonstrated, the impossibility of anonymizing location data holds true in this case as well. *See* 1/21/20 Tr. at 83, 87-88, 90-91. It is trivial to plot "anonymized" coordinates on a map, connect the dots, and determine which house belongs to whom. *See* ECF No. 68 at 3; 1/21/20 Tr. at 74-75. Indeed, the Step One returns may be enough, without anything more from Google, for law enforcement to determine the identity of "anonymized" users. *See* 1/21/20 Tr. at 86-87.[16] Consequently, this Court "should not discount the intrusiveness of the initial data returns disclosed by Google." ECF No. 72 at 10.

In Step Three, the government selected three Google users for even further scrutiny. At least one of these users[17] was likely never inside the geofence at all, something which should have been apparent to investigators reviewing the Step Two returns. Nonetheless, the government decided to have Google de-anonymize this user's records and turn over additional subscriber information associated with the account.

[16] For this reason, Mr. Chatrie does not believe it is appropriate, as the government suggests, to sever the warrant and consider Step One separately from Step Two. *See* ECF No. 41 at 20. Furthermore, doing so would "condone the digital equivalent of a general warrant that lacked particularity from the outset." ECF No. 48 at 14 n.5; *see also 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").

[17] Device ID: 907512662.

At no point during this three-step process did the government return to the magistrate to seek further authorization. *See* ECF No. 29 at 23-24. Instead, it was up to Google to determine what was "reasonable," beginning with the scope of the initial search, and including the returns provided in Steps Two and Three. ECF No. 48, Ex. A at 1; *id.*, Ex. B at 1. The point is not that Google should have searched the Location Accuracy or Web & App Activity databases, or that Google should have produced more or less records. The point is that this is not how warrants are supposed to work. What the government can search and seize is a question that the Constitution reserves for the judiciary, not for Google or the police. *See Groh*, 540 U.S. at 561 ("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); ECF No. 48 at 15-16. The delegation of this authority to Google only demonstrates the profound lack of particularity in the geofence warrant. *See* ECF No. 48 at 16.

V. The Good Faith Exception Does Not Apply.

Mr. Chatrie fully adopts, incorporates, and re-asserts in this supplement that the *Leon* good faith exception to the exclusionary rule does not apply to evidence obtained from a warrant that was *void ab initio*. *See* ECF No. 48 at 17-20. As set forth above and in the original geofence warrant briefing, this geofence warrant is void from its inception and thus, 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*, 540 U.S. at 558 ("[T]he warrant was so obviously deficient that we must regard the search as 'warrantless' within the meaning of our case law.").

Of critical importance here is the omission of key facts in the warrant affidavit that should have flagged the unique overbreadth of the search for the reviewing magistrate—namely, the true scope of the number of people to be searched and the true boundaries of the "geofence." Had the

magistrate known that the warrant he signed authorized Google to search the private daily journals of numerous tens of millions of people, surely he would have refused to sign such a warrant. Had the magistrate known that the warrant he signed simultaneously authorized a search of a church, a hotel, a restaurant, a mini storage facility, and two apartment complexes, surely he would have laid his pen on his desk and sent the affiant away empty-handed. To not include those facts demonstrates at least recklessness with regard to the true nature of the search the affiant proposed.

The unprecedented search of numerous tens of millions of private diaries at once also renders the warrant so overbroad that no reasonably objective officer would have thought it a valid warrant. *See, e.g.*, *United States v. Winn*, 79 F. Supp. 3d 904, 923-24 (S.D. Ill. 2015) (refusing to find good faith where two officers had fifteen years of experience between them and obtained a warrant that "gave them unbridled discretion to search for and seize whatever they wished"). In *Winn*, officers used a template affidavit that received only a "quick and cursory" review by the State's Attorney to obtain "any or all files" on an individual's cell phone. *Id*. at 919, 923-24. While consultation with counsel was "prima facie evidence" of good faith, the court found that *Leon* did not apply because of the government's "recklessness" as to particularity. *Id*. at 923. The court also found that the judge "did the same . . . abandon[ing] his judicial role to some extent" by authorizing "a warrant to rummage through every conceivable bit of data." *Id*. at 923-24. Such disregard for the particularity requirement negated the government's claim of good faith in *Winn*, *id.* at 924, and it should have the same result here.

In this case the government used a warrant template (the provenance of which is still unclear to Mr. Chatrie) that was fundamentally overbroad and lacking in particularity. It substituted generalized assumptions about cell phone use for probable cause and sought to authorize the unbridled search of numerous tens of millions of Google users. It did not even attempt

to exclude devices associated with the Journey Christian Church any step along the way. The government then presented this application to a state magistrate who approved it without any information or, presumably, understanding of the scope of the search or the level of discretion being afforded to investigators. As in *Winn*, such reckless disregard for the probable cause and particularity requirements should negate the government's argument that it acted in good faith. *See also United States v. Doyle*, 650 F.3d 460, 476 (4th Cir. 2011) ("[W]here a reasonable officer would know that a probable cause determination could not be rendered without information conspicuously absent from his application for a warrant, reliance on the resulting warrant is not objectively reasonable.").

CONCLUSION

The geofence warrant here was the epitome of a general warrant, a search of numerous tens of millions of Google users in an attempt to develop a single lead. Its overbreadth and absence of particularity are so unprecedented that no officer would reasonably rely on it. As a result, this Court should suppress all evidence and fruits that the government obtained from it.

Respectfully submitted,
OKELLO T. CHATRIE

By: _____/s/_____
Michael W. Price
NY Bar No. 4771697 (*pro hac vice*)
NACDL, 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
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.	)	

UNITED STATES' 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 supplemental motion to suppress evidence obtained from Google, LLC ("Google") pursuant to a search warrant for GeoFence location information (the "GeoFence warrant"). ECF No. 104. This Court should deny the defendant's motion for three reasons. First, investigators did not infringe the defendant's reasonable expectation of privacy 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. INTRODUCTION

Agents investigating the armed robbery of the Midlothian Call Federal Credit Union had good reason to believe that Google was a witness and had evidence of the crime: surveillance video showed the robber with a cell phone, and investigators knew that there was therefore a fair probability that Google had stored the robber's cell phone location information. They also knew that Google likely had other location information that would provide them with a fuller understanding of the time and place of the events of the robbery, as well as help them identify

other witnesses and suspects. Federal Bureau of Investigation Task Force Officer Josh Hylton put these facts in an affidavit, and he obtained a GeoFence search warrant for a narrowly focused set of evidence: a two-hour interval of Google location information (and associated identity information) for devices that Google's records placed within 150 meters of a point near the bank during the hour of the robbery. *See* ECF No. 54-1.

The investigators were correct: Google had been a witness to the robbery. Pursuant to the warrant, Google produced to the United States a small set of records: 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. This information was sufficient for investigators to recognize that the defendant's Google account likely belonged to the robber, and subsequent investigation led to his indictment.

The defendant argues that the Fourth Amendment bars Google from being a witness in an investigation like this one: that even where a judge finds probable cause to believe that Google has evidence concerning unidentified individuals present at the scene of a serious crime, the Fourth Amendment bars issuance of a warrant to obtain that evidence. Fortunately, the defendant is wrong, and his arguments that the United States violated the Fourth Amendment by obtaining his location information are without merit.

II. BACKGROUND

The United States' initial Response in Opposition to Defendant's Motion for Suppression sets forth the basic facts of the bank robbery, the GeoFence Affidavit, the GeoFence Warrant, and the warrant's execution. *See* ECF No. 41 at 1-5. In addition, Google has now submitted two affidavits relevant to the defendant's motion. *See* ECF No. 96. The United States and the defendant have agreed to stipulate to the accuracy of these affidavits. One, by Google Location

History Product Manager Marlo McGriff, describes the Google Location History service, including steps the defendant took to opt in to Google's storage of his location information. *See* ECF No. 96-1. The other, by Google Team Lead for Legal Investigations Support Sarah Rodriguez, provides further information about the execution of the GeoFence warrant. *See* ECF No. 96-2. The United States will not repeat these facts here, but will reference them below in explaining why the GeoFence warrant was consistent with the Fourth Amendment. In addition, the arguments made now by the defendant remain similar to his initial suppression arguments. The United States therefore incorporates by reference the arguments made in its initial opposition to the defendant's suppression motion and in its response to the Google amicus brief. *See* ECF No 41 at 6-24; ECF No. 71 at 1-9.

III. ARGUMENT

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

It is a fundamental Fourth Amendment 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 government. This principle has deep roots: when an individual discloses information to a third party, the third party becomes a witness, and 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 repeatedly rejected Fourth Amendment arguments contrary to this principle in cases ranging from private conversations to business records. *See, e.g.*, *Hoffa v. United States*, 385 U.S. 293, 302 (1966) (statements made in the presence of an informant); *Couch v. United States*, 409 U.S. 322, 335-36 (1973) (information disclosed to an accountant); *United States v. Miller*, 425 U.S. 435, 443 (1976) (bank records); *Smith v. Maryland*, 442 U.S. 735, 742-44

(1979) (dialed telephone numbers); *SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984) (financial records).

Based on this fundamental principle, the defendant had no reasonable expectation of privacy in the location information he disclosed to Google. As discussed below, the multiple steps that the defendant took to opt in to Google's receipt and storage of his location information confirm this result. But even without the defendant's explicit agreement to disclose his location information to Google, the defendant's voluntary disclosure of his location would be evident from the nature of the services Google provides to customers. Courts often infer that information is voluntarily disclosed to a third party based on the nature of the relationship between the third party and the one making the disclosure. For example, in *Miller*, the Supreme Court did not need to consider Miller's explicit agreements with his bank in order to conclude that he had voluntarily disclosed his financial information. Instead, the Court's conclusion was based on "examin[ing] the nature of the particular documents sought" and concluding that they were "not confidential communications but negotiable instruments to be used in commercial transactions." *Miller*, 425 U.S. at 442. Similarly, the Supreme Court's analysis of the disclosure of dialed phone numbers in *Smith v. Maryland* began by observing that 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." *Smith v. Maryland*, 442 U.S. at 742.

Here, similar analysis demonstrates that the defendant voluntarily disclosed his location information to Google. Google does far more than provide a storage service for its customers' location information. Instead, Google customers disclose their location to Google to obtain location-based services such as mapping, traffic updates, and help finding their phones. *See* ECF No. 96-1 at 2. For example, customers who use Google's mapping services to assist them with

driving from one place to another realize that they must convey their location to Google. Thus, because the defendant provided his location to Google to obtain its location-based services, the United States did not infringe his reasonable expectation of privacy when Google conveyed that information to the United States.

The fact that the defendant voluntarily disclosed his location information to Google is confirmed and reinforced by the multiple steps he took to enable Google to obtain and store his location. The McGriff affidavit establishes that Google users "must explicitly opt in to the [Location History] service." ECF No. 96-1 at 2. McGriff sets forth the multiple steps that a user must take before Google stores the user's Location History: Location History "functions and saves a record of the user's travels only when the user opts into [Location History] as a setting on her Google account, enables the 'Location Reporting' feature for at least one mobile device, enables the device-location setting on that mobile device (and for iOS devices provides the required device-level application location permission), powers on and signs into her Google account on that device, and then travels with it." ECF No. 96-1 at 3.

The McGriff affidavit further explains both that Google users may delete their location information and that users are informed of this fact in the Google Privacy Policy. *See* ECF No. 96-1 at 5. Google's Privacy Policy also explains to users that Google has access to their location information for purposes ranging from providing them with targeted advertising or driving directions to Google's development of new services. *See* Google Privacy Policy (available at https://policies.google.com/privacy/archive/20190122). The defendant concedes that he "agree[d] to Google's terms and conditions during the initial setup process of his phone." ECF No. 104 at 19. As part of these terms and conditions, he agreed that Google could use his data "data in accordance with our privacy policies." *See* October 25, 2017, Google Terms of Service (available

at https://policies.google.com/terms/archive/20171025).

These facts confirm that the defendant voluntarily conveyed his location information to Google. Significantly, they also distinguish with respect to voluntary disclosure the location information here from the cell-site records of *Carpenter v. United States*, 138 S. Ct. 2206 (2018). *Carpenter* held that cell phone users do not voluntarily disclose their cell-site records to the phone company because cell-site information is collected "without any affirmative act on the part of the user beyond powering up," because "there is no way to avoid leaving behind a trail of location data," and because carrying a cell phone "is indispensable to participation in modern society." *Carpenter*, 138 S. Ct. at 2220. These factors are not present here. Google could not obtain and store the defendant's location without his undertaking multiple affirmative acts. He had to opt in to Location History in his account settings, and he had to enable Location Reporting for his phone. *See* ECF No. 96-1 at 3. The defendant had discretion regarding whether Google stored his location information, and he retained the ability to delete it. *See* ECF No. 96-1 at 5. And none of the services associated with Google's storage of location information are indispensable to participation in modern society. The defendant thus voluntarily disclosed his location information to Google, and Google's conveyance of that information to the United States did not infringe his reasonable expectation of privacy.

The defendant makes multiple arguments in support of his claim that he had a reasonable expectation of privacy in the location information he disclosed to Google. All of them lack merit.

First, the defendant argues that *Carpenter* protects even the brief period of his location information obtained by investigators. *See* ECF No. 104 at 10-11. But this argument ignores both *Carpenter*'s explicit limitations and its reasoning. As an initial matter, the Court in *Carpenter* did not abolish the third-party doctrine or "disturb the application of *Smith* and *Miller*." *Carpenter*,

138 S. Ct. at 2220. Thus, because the defendant voluntarily disclosed his location to Google under the reasoning of *Carpenter*, the government did not conduct a search when it obtained his location information.

Even absent the third-party doctrine, *Carpenter* does not support the defendant's claim that obtaining two hours of his location information was a search. *Carpenter* protects only a privacy interest in long-term, comprehensive location information. The Court explicitly limited its holding to its conclusion "that accessing seven days of [cell-site location information] constitutes a Fourth Amendment search." *Carpenter*, 138 U.S. at 2217 n.3. The Court emphasized that *Carpenter* was "not about 'using a phone' or a person's movement at a particular time." *Carpenter*, 138 U.S. at 2220. Instead, it was "about a detailed chronicle of a person's physical presence compiled every day, every moment, over several years." *Id.* The government conducted a search in *Carpenter* because the cell-site records the government obtained created a "comprehensive record of the person's movements" that was "detailed" and "encyclopedic." *Id.* at 2216–17. By this standard, the government did not conduct a search when it obtained only two hours of the defendant's location information pursuant to the GeoFence warrant.

Significantly, although the Supreme Court decided *Carpenter* nearly two years ago, the defendant fails to cite a single case interpreting *Carpenter* broadly to protect a brief period of location information. Instead, courts have agreed that *Carpenter* protects only long-term, comprehensive location information. *See, e.g.*, *United States v. Adkinson*, 916 F.3d 605, 611 (7th Cir. 2019) (stating that *Carpenter* "did not invalidate warrantless tower dumps (which identified phones near *one location* (the victim stores) at *one time* (during the robberies))" (emphasis in original)); *Commonwealth v. McCarthy*, 484 Mass. 493, 494 (2020) ("[W]hile the defendant has a constitutionally protected expectation of privacy in the whole of his public movements, an interest

which potentially could be implicated by the widespread use of [automatic license plate readers], that interest is not invaded by the limited extent and use of ALPR data in this case."); *United States v. Yang*, 958 F.3d 851, 862 (9th Cir. 2020) (Bea, J., concurring) (stating that a query of a large automatic license plate recognition database that revealed only a single location point for Yang was not a search under *Carpenter* because "the information in the database did not reveal 'the whole of [Yang's] physical movements.'").[1]

Second, the defendant continues to cite the fact that the United States obtained location information regarding other Google users, *see* ECF No. 104 at 12, but he still provides no explanation of how this fact supports his claim that he had a reasonable expectation of privacy in his location information. Such an argument would be foreclosed by Supreme Court precedent. The Supreme Court has squarely held that Fourth Amendment rights "may not be vicariously asserted." *Rakas v. Illinois*, 439 U.S. 128, 133-34 (1978) (quoting *Alderman v. United States*, 394 U.S. 165, 174 (1969)). Courts have agreed that defendants lack standing to challenge the government obtaining others' cell phone location information. *See, e.g.*, *United States v. Patrick*, 842 F.3d 540, 545 (7th Cir. 2016); *United States v. Forest*, 355 F.3d 942, 948 (6th Cir. 2004), *vacated on other grounds by* 543 U.S. 1100 (2005) (vacating in light of *United States v. Booker*, 543 U.S. 220 (2005)).

[1] The defendant also cites *United States v. Karo*, 468 U.S. 705 (1984), for the proposition that the government conducts a search when it obtains "information about the interior of a constitutionally-protected space, such as a home." ECF No. 104 at 11. However, both *Smith v. Maryland* and *Hoffa* demonstrate that the government does not conduct a search when it obtains information voluntarily disclosed to another from within a protected space and then conveyed by that party to the government. *Smith v. Maryland*, 442 U.S. at 743; *Hoffa*, 385 U.S. at 301. Moreover, the defendant does not claim that the GeoFence warrant revealed any such information about him.

Third, the defendant argues that he has a reasonable expectation of privacy in the location information he disclosed to Google because Google considers it to be "'contents' for purposes of the Stored Communications Act." ECF No. 104 at 12. As the United States previously explained, Google's analysis of how the Stored Communications Act applies to location information may be incorrect. *See* ECF No. 71 at 8. But regardless, the statutory classification of Google's location information does not affect whether a user has a reasonable expectation of privacy in it. As *Hoffa* demonstrates, one has no reasonable expectation of privacy in the contents of communications disclosed to a third party when the third party conveys that information to the government. *See Hoffa*, 385 U.S. at 302. Here, because the defendant conveyed his location information to Google to obtain location-based services, his Fourth Amendment rights were not infringed when Google conveyed that information to the United States.

Fourth, the defendant argues that his Google location information should be protected because "it is at least as accurate" as the cell-site information in *Carpenter* and thus "capable of revealing the 'privacies of life.'" ECF No. 104 at 13. The United States agrees that the Google information here was at least as accurate as the cell-site information in *Carpenter*, but *Carpenter* nevertheless does not protect it both because of its short duration and because the defendant disclosed it to Google.

Fifth, despite the defendant's stipulation to the Google affidavits, he attempts to argue that he did not voluntarily disclose his location information to Google. *See* ECF No. 104 at 15-17. As an initial matter, the defendant's argument that he did not voluntarily disclose his location focuses entirely on the opt-in procedures for Google's storage of location information. He thus ignores that his voluntary disclosure of location information to Google is evident from the nature of the

location-based services (like mapping) that Google provided him.[2]

The defendant bases his argument that he did not voluntarily disclose his location information to Google in large part not on the McGriff affidavit, but instead on his own description of the setup process for an Android phone. *See* ECF No. 104 at 15-17. As an initial matter, the United States does not believe that the steps described by the defendant fully and accurately describe the steps he would have taken to create a Google account, set up the phone he used at the time of the robbery, and opt in to Google Location History. For example, the defendant does not address the steps involved in the initial creation of his Google account or signing into that account using his phone.

Nevertheless, assuming for the sake of argument that the defendant's description of his cell phone setup process is accurate, the defendant voluntarily disclosed his location information to Google. The defendant concedes that during setup, a screen on his phone informed him that "Google needs to periodically store your location to improve route recommendations, search suggestions, and more." ECF No. 104 at 15. He does not dispute that in response to this warning, he clicked "YES I'M IN." *See id*. He also concedes that this screen of his phone linked to a web page containing Google's Terms of Service and Privacy Policy, *see id*. At 15-16, which describe

[2] Although the defendant might object that a user of Google's location-based services cannot tell that Google will store her location information, the Supreme Court held in *Smith v. Maryland* that the third-party doctrine applies to information voluntarily disclosed to a third party regardless of any expectations regarding subsequent storage. In *Smith*, the defendant argued that the third-party doctrine should not apply to his dialed numbers because the phone company did not usually store information concerning local phone calls. The Supreme Court rejected his argument: "The fortuity of whether or not the phone company in fact elects to make a quasi-permanent record of a particular number dialed does not in our view, make any constitutional difference. Regardless of the phone company's election, petitioner voluntarily conveyed to it information that it had facilities for recording and that it was free to record." *Smith*, 442 U.S. at 745. Thus, the defendant would have no reasonable expectation of privacy in information he disclosed to Google even if he had not been informed that Google would store that information.

Google's use, storage, and deletion of location information. He further concedes that he "would have had to agree" to these terms and conditions. ECF No. 104 at 19.

These concessions are fatal to the defendant's argument that he did not voluntarily disclose his location information to Google. The defendant attempts to evade the consequences of his agreements through an argument worthy of Goldilocks: that the language on his phone screen was too short, and that the Terms of Service and Privacy Policy were too long. He complains that the language on his phone screen did not use the phrase "Location History" or inform him "of the privacy implications of turning it on," and he complains that the Privacy Policy was "27 pages long." *See* ECF No. 104 at 15-16. But the language on his phone screen was just right—in brief, clear language, it informed him of what Google would do: periodically store his location to provide him with services. Moreover, the Supreme Court has never limited voluntary disclosure under the third-party doctrine to circumstances where one is informed of the Fourth Amendment implications of disclosure. And the Privacy Policy was also just right, because it gave the defendant the opportunity to obtain a more detailed explanation of Google's use and storage of his location information.

Sixth and finally, the defendant cites cases addressing whether Internet Terms of Service create binding contacts, including a case within this district enforcing such a contract. *See* ECF No. 104 at 18-20 (citing *Melo v. Zumper*, No. 3:19-cv-621 (DJN), 2020 WL 465033 (E.D. Va. Jan. 28, 2020)). Although Google's Terms of Service likely creates a binding contract with customers, the defendant cites no cases holding that this contracts question plays any role in determining whether information is voluntarily disclosed to a third party for Fourth Amendment purposes. For example, the Supreme Court in *Smith v. Maryland* relied on statements in phone books to support its conclusion that "telephone users realize that they must 'convey' phone numbers to the telephone

company," *Smith v. Maryland*, 442 U.S. at 742-43, but phone book statements are not likely part of a contract between a phone company and its customers.

Moreover, courts rely on terms of service in evaluating whether a service provider's disclosure of information to the government violates the Fourth Amendment. *See, e.g.*, *Adkinson*, 916 F.3d at 610 (holding that that T-Mobile's disclosure of cell-site information to the government did not violate Adkinson's Fourth Amendment rights because Adkinson "agreed to T-Mobile's policy that T-Mobile could disclose information when reasonably necessary to protect its rights, interests, property, or safety"). Here, the defendant agreed that in order to obtain Google's location-based services, he would share his location with Google, and he chose for Google to store it. Google's conveyance of that information to investigators did not infringe his reasonable expectation of privacy.[3]

B. The Fourth Amendment's Protection of Property Does Not Restrict Google from Conveying to the United States Information Disclosed to it by the Defendant

The defendant continues to argue that obtaining location records from Google was a search under "a property based theory," *See* ECF No. 104 at 20, but his argument flies in the face of the fundamental principle that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities." *Miller*, 425 U.S. at 443. The Supreme Court has recognized that a physical trespass for purposes of obtaining

[3] The defendant also cites European complaints regarding Google's storage of location information. For example, the defendant cites a complaint by a Norwegian individual whose name is redacted in which that unknown person alleges that Google "uses different means to nudge the user into turning on" Location History. *See* ECF No. 104 at 17 (citing complaint available at https://fil.forbrukerradet.no/wp-content/uploads/2018/11/complaint-google-27-november-2018-final.pdf). Here, where this Court has the benefit of an expert from Google, as well as experts provided by the United States and the defense, this Court should not rely on unproven allegations from an anonymous person abroad.

information is a search. *See United States v. Jones*, 565 U.S. 400, 404-05 (2012). But the investigation in this case involved no physical trespass; instead, the GeoFence warrant directed Google to produce specified information that its customers had disclosed to it. The defendant cites no case—and the United States is aware of no case—in which a court has relied on a "property-based theory" to discard the third-party doctrine of *Smith* and *Miller* or prevent witnesses from providing evidence to the government. Justice Gorsuch's solo dissent in *Carpenter* did contemplate abandoning the third-party doctrine based on some sort of property rights theory of the Fourth Amendment, *see Carpenter*, 138 S. Ct. at 2262-72 (Gorsuch, J., dissenting), but a solo dissent is not the law, and the third-party doctrine of *Smith* and *Miller* remains binding law.

In addition, the defendant's assertion that Google is a "mere bailee" of location information ignores how Google uses location information to provide services to its customers. ECF No. 104 at 20. Google does not merely store its customers' locations; it uses that information to provide location-based services. *See* ECF No. 96-1 at 2. Under these circumstances, Google's disclosure of its customers' location information to investigators does not implicate the Fourth Amendment. For example, the owner of documents may retain a property interest in documents shared with an accountant, but the owner's Fourth Amendment rights are not infringed when the accountant conveys them to the government. *See Couch*, 409 U.S. at 335.

C. The GeoFence Search Warrant Satisfied the Fourth Amendment

The GeoFence warrant satisfied the Fourth Amendment because it was issued on a showing of probable cause and specified its object with particularity. The defendant's arguments that the search warrant did not "meet the probable cause or particularity requirements demanded by the Fourth Amendment" are without merit. ECF No. 104 at 22.

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)). Here, the affidavit in support of the Geofence warrant established an ample basis for the issuing magistrate's finding of probable cause. In particular, the affidavit established: (1) that an unknown subject committed an armed bank robbery at a particular place and time; (2) that prior to the robbery, the robber held a cell phone to his ear and appeared to be speaking with someone; (3) that the majority of cell phones were smartphones; (4) that "[n]early every" Android phone "has an associated Google account," and that Google "collects and retains location data" from such devices when the account owner enables Google location services; and (5) that Google can collect location information from non-Android smartphones if the devices are "registered to a Google account and the user has location services enabled." State GeoFence Warrant at 4-5. 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 argues that the warrant lacked probable cause because it "did not identify any individuals or accounts to be searched because investigators did not know who they were searching for, or even if Google would have relevant data." ECF No. 104 at 22. However, a warrant for evidence of crime need not identify specific individuals or establish with certainty that evidence will be found—all it must do is establish a fair probability that specified evidence will be found in the place to be searched. Indeed, the warrant here is similar in this respect to the search warrant approved by the Supreme Court in *Zurcher v. Stanford Daily*, 436 U.S. 547, 551 (1978), which authorized seizure from a newspaper of photographs of unidentified individuals who had

assaulted police officers.

The defendant also ignores the standard for probable cause when he argues that probable cause was lacking because "the application rested on broad conjecture based on the popularity of Google and cell phones generally." ECF No. 104 at 22. As an initial matter, the affidavit included specific facts supporting the finding of probable cause, including the robbery itself and that the armed robber had a cell phone. Moreover, it is entirely appropriate in the Fourth Amendment context to rely in part on probabilistic inferences. For example, *in United States v. James*, No. 18-cr-216, 2019 WL 325231, at *3 (D. Minn. Jan. 25, 2019), the court relied on inferences about cell phone use to conclude that a warrant for a cell tower dump was based on probable cause, even though it was "unknown whether a phone was used by the suspect before or after the robbery."[4] As required by the Fourth Amendment, the GeoFence affidavit established a fair probability that Google had evidence pertaining to the robbery.

2. The GeoFence Warrant Was Not Overbroad

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 Fourth Amendment 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.*

[4] The recent Supreme Court case *Kansas v. Glover*, 140 S. Ct. 1183 (2020), provides an example of the Court upholding probabilistic reasoning in the Fourth Amendment context. The Court held that a police officer had properly made a "commonsense inference" that the owner of a vehicle was likely its driver. *Id.* at 1188. *See also Illinois v. Gates*, 462 U.S at 240 (noting the authority of a magistrate issuing a search warrant "to draw such reasonable inferences as he will from the material supplied to him by applicants for a warrant").

Maryland, 427 U.S. 463, 480 (1976)). Moreover, the test "is a pragmatic one" that "may necessarily vary according to the circumstances and type of items involved." *United States v. Torch*, 609 F.2d 1088, 1090 (4th Cir. 1979) (quoting *United States v. Davis*, 542 F.2d 743, 745 (8th Cir. 1976)).

Here, the GeoFence warrant was limited 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 an armed robbery during a one-hour interval. The warrant was appropriate for its investigatory purpose, which was to obtain evidence to help identify and convict the robber. The warrant's breadth is also supported by *James*, in which the district court held that a cell tower dump warrant was sufficiently limited because it was constrained geographically and temporally to robberies under investigation. *James*, 2019 WL 325231 at *3. The GeoFence warrant here is narrower than the warrant upheld in *James*: its geographical area was smaller than a cell site, and it produced information about only 19 individuals, as opposed to "hundreds if not thousands." *Id.*

The defendant argues that the GeoFence warrant was overbroad because Google reviewed a large body of data in order to comply with it, *see* ECF No. 104 at 22-24, but this argument is without merit. He cites no case law holding that a service provider may not review a large data set in order to produce a narrowly defined set of information. Such process is not new: for example, phone companies may review every call made by all their customers in order to find calls made to a specified phone number. *See Ameritech Corp. v. McCann*, 403 F.3d 908, 910 (7th Cir. 2005). GeoFence warrants are also similar to tower dump warrants: they determine who was present at a particular place and a particular time. If the cell tower is in a busy area, a large set of customers may have used the tower; the phone company in response to the warrant must search

within that data for those who used the tower at the specified time.

Google's review of a large set of data to comply with the GeoFence warrant is a result of Google's internal data storage practices, not an overbroad warrant. It would be possible for Google to create an additional Location History database indexed by location. This database would enable Google to comply with a GeoFence warrant—and produce the exact same data as Google currently produces—without reviewing the data of all customers. The constitutionality of a search warrant does not depend on a service provider's internal data storage practices which are invisible to customers and the government alike. Thus, the appropriate measure for the breadth of the GeoFence warrant is the limited data sought by the warrant, which resulted in the government obtaining location information for only 19 individuals, all of whom were near the bank at the time of the robbery.

3. The GeoFence Warrant Was Sufficiently Particular

The defendant next argues that the GeoFence warrant was insufficiently particular because of its three-step process, but the defendant's arguments are mistaken. First, the defendant complains that "Google decided to search only a portion of its records, specifically 'Location History' records." *See* ECF No. 104 at 25. As an initial matter, even if Google should have reviewed additional databases for responsive information, Google's failure to do so would not demonstrate any infirmity in the warrant or infringe the defendant's Fourth Amendment interests. No Stored Communications Act warrant has even been written that a service provider cannot botch, but a service provider's failure to produce a portion of the information sought pursuant to a warrant does not violate the Fourth Amendment. But as Google explains, it did nothing wrong: Location History was "the only form of location data Google maintains that Google believes to be responsive to a geofence request." McGriff Affidavit at 7. Google's review and production of the

information that it believed fell within the scope of the warrant does not make the warrant insufficiently particular. There was no reason for Google to review information it had concluded was nonresponsive to the warrant. [5]

Second, the defendant complains that Google's response to the warrant was not dependent on Google's estimates of the margins of error associated with its location calculations. *See* ECF No. 104 at 25. It is certainly true that no cell phone location measurement has perfect accuracy. However, a warrant that does not adopt a probabilistic approach to all location information is not insufficiently particular. Here, the warrant directed Google to disclose information for devices "inside the described geographical area" during the time of the robbery, and Google correctly interpreted this to mean it should disclose information concerning devices that its calculations placed within the circle specified by the warrant. Although there always remains a possibility of inaccuracy in Google's location information, and a defendant may certainly challenge at trial the weight given to this information, the possibility of inaccuracy does not make a warrant insufficiently particular.[6]

Third, the defendant argues that the warrant was insufficiently particular based on the correspondence between Google and FBI TFO Josh Hylton regarding step 2 of the warrant, but

[5] Elsewhere in his motion, the defendant states that the 'warrant required Google to produce location data for 'each type' of Google account," and he faults Google for not producing data from the Web & App Activity or Google Location Accuracy databases. ECF No. 104 at 7. The defendant has misinterpreted the GeoFence warrant: Web & App Activity and Google Location Accuracy are separate Google services, not separate types of Google accounts.

[6] The defendant does not dispute that his Google location information would have fallen within the scope of the warrant regardless of how the warrant addressed the uncertainty associated with it. Instead, the defendant highlights a single Google measurement of someone else's phone with a margin of error of 387 meters. *See* ECF No. 104 at 25. Another measurement associated with that person's device, however, had a margin of error of only 84 meters, placing the device within the GeoFence region.

this correspondence provides no evidence that the warrant lacked particularity. *See* ECF No. 104 at 25-26. The warrant was sufficiently particular because it specified the evidence law enforcement was authorized to obtain: two hours of location data (and associated identity information) for all individuals present at the site of the robbery during the hour of the robbery. The step 2 correspondence addresses an entirely separate issue: FBI TFO Hylton's decision to obtain less than the maximum amount of information authorized by the warrant. The Fourth Amendment requires that 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. Indeed, a contrary rule would be perverse: agents executing warrants would be required to engage in more invasive searches than they deemed necessary, simply because they had previously established probable cause for additional evidence.

Agents executing warrants often make choices about the intensity of their execution of a search warrant, and it is not a Fourth Amendment violation if they ultimately leave some evidence behind. The Playpen warrant explicitly included such a provision: it authorized a search of the computer of everyone who visited a specified child pornography web site, but it also stated 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). Courts uniformly agreed that this provision did not violate the Fourth Amendment's particularity requirement. *See, e.g.*, *United States v. Matish*, 193 F. Supp. 3d 585, 609 (E.D. Va. 2016) ("[T]he 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"). The defendant attempts to distinguish the Playpen warrant based on its breadth, *see* ECF No. 104 at 23-24, but the United

States cites the Playpen warrant for an entirely different proposition: that it is permissible for a warrant to authorize investigators to seize less than the maximum amount of evidence for which they have established probable cause and which the warrant describes with particularity. FBI TFO Hylton did not violate the Fourth Amendment when he executed the warrant in a manner that provided additional privacy protections for the majority of individuals present at the robbery. [7]

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

Finally, arguing that "every person takes a 'unique path through life,'" the defendant also faults the warrant for stating that the information produced by Google in step 1 and step 2 would be "anonymized." ECF No. 104 at 27. In the context of the GeoFence warrant, however, "anonymized information" refers to the fact that Google did not produce its subscriber identity information associated with the location information until step 3 of the warrant. The GeoFence warrant's use of the phrase "anonymized information" does nothing to make the warrant insufficiently particular.

[7] As argued in its initial opposition to the defendant's suppression motion, if the three-step process for the GeoFence warrant were insufficiently particular, the proper remedy would be to sever the second step. *See* ECF No. 41 at 20-21.

D. 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. In its response to the defendant's initial suppression motion, the United States explained that the good faith exception precluded suppression in this case both under the traditional good-faith analysis of *United States v. Leon*, 468 U.S. 897 (1984), and under the Fourth Circuit's standard in *United States v. McLamb*, 880 F.3d 685 (4th Cir. 2018), for good-faith reliance on a search warrant authorizing use of a novel investigative technique. *See* ECF No. 41 at 21-24. The United States will not repeat these arguments here, but they remain fully applicable to the defendant's supplemental motion.

The defendant now advances an additional argument against the good faith exception: he claims that the good-faith exception should not apply here because the GeoFence affidavit omitted "the true scope of the number of people to be searched and the true boundaries of the 'geofence.'" ECF No. 104 at 28. To challenge a search warrant on this basis, the defendant would be required to show "(1) that the officer deliberately or recklessly omitted the information at issue and (2) that the inclusion of this information would have defeated probable cause." *United States v. Andrews*, 577 F.3d 231, 238-39 (4th Cir. 2009). Here, the defendant's argument fails because he cannot satisfy either of these requirements.

To begin, the information that the defendant asserts should have been included in the warrant would not have defeated probable cause. First, information about Google's internal data structures and how it processes GeoFence warrants has nothing to do with either the probable cause that supported the warrant or the information that the warrant authorized to be seized. Instead, it relates to how the warrant was executed, and the Supreme Court has held that "[n]othing in the

language of the Constitution or in this Court's decisions interpreting that language suggests that, in addition to the three requirements discussed above [a neutral magistrate, probable cause, and particularity], search warrants also must include a specification of the precise manner in which they are to be executed." *Dalia v. United States*, 441 U.S. 238, 257 (1979). Regardless of how Google organized its databases or executed the warrant, the affidavit established a fair probability that Google had evidence of the location of the armed robber and others at the time of the robbery. Similarly, the fact that there is some margin of error in all service provider cell phone location information does not undermine probable cause or particularity: the affidavit still would have established a fair probability that Google stored location information of the robber and other nearby witnesses.[8]

Nor can the defendant establish that any omission by FBI TFO Hylton was deliberate or reckless. There was no reason for TFO Hylton even to know about the organization of Google's internal data structures. The defendant therefore cannot show that any omission regarding that information was deliberate or reckless. And the fact that there is some error in cell phone location measurements is common knowledge; there is no reason Officer Hylton would not have expected the issuing judge to be aware of that fact. In sum, the omissions cited by the defendant were not material to the issuance of the warrant, and in any event the defendant has not shown that any omissions were deliberate or reckless.

Finally, the defendant's argument against the good-faith exception relies heavily on a

[8] For example, the affidavit could have included the fact that many of Google's location points are based on GPS information, and that GPS coordinates are usually accurate to within a few feet. *See* https://www.gps.gov/systems/gps/performance/accuracy. This additional information would not have defeated the affidavit's probable cause. FBI TFO Hylton could not have known in advance Google's confidence radii for its WiFi-based location points. But even if he could have known that the step 1 WiFi location points would end up having a median confidence radius of 25 meters, that fact also would not have affected the existent of probable cause.

district court case from another circuit, *United States v. Winn*, 79 F. Supp. 3d 904 (S.D. Ill. 2015). But the warrant in *Winn* was nothing like the warrant here: it authorized seizure of "any or all files" contained on a cell phone. *Winn*, 79 F. Supp. 3d at 918. Here, in contrast, the warrant was remarkably targeted: despite the vast quantity of data stored by Google, it targeted only two hours of location data associated with devices near the bank at the time of the armed robbery, and Google produced data regarding only 19 accounts. Officers' reliance on the warrant was reasonable, and this Court should deny the defendant's motion to suppress.

IV. 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
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 12th day of June, 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 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