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

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

DEFENDANT'S BRIEF ON THE APPLICATION OF *BRADY* AND RULE 16 TO A SUPPRESSION HEARING

Okello Chatrie, through counsel, respectfully submits this brief on the government's discovery obligations under *Brady v. Maryland*, 373 U.S. 83 (1963), and Federal Rule of Criminal Procedure 16 in the context of a pre-trial suppression hearing. For the reasons set forth below, Mr. Chatrie submits that he is entitled to discovery on all of the outstanding items in his discovery request, ECF No. 28. Documents responsive to requests 1, 3, 4(a), 4(b), 4(e), 8, 9, 11(c), and 11(e) are discoverable under both *Brady* and Rule 16, whereas requests 4(c), 4(d), 5, 10, 11(d), and 12 seek information discoverable under Rule 16 alone.

INTRODUCTION

On October 29, 2019, Mr. Chatrie filed a discovery motion concerning the search of Google location information obtained pursuant to a so-called "geofence" warrant. *See* ECF No. 28. Mr. Chatrie filed this motion in connection with his motion to suppress the evidence obtained from the geofence warrant, and all of the fruits thereof. *See* ECF No. 29. The government has provided discovery in response to paragraphs 2, 6, 7, 11(a), and 11(b) of ECF No. 28, but it has not provided information in response to the remainder of the items sought by Mr. Chatrie, which include:

1. The location/source of the WiFi/WiFi access points for individuals' location tracking data listed as "WiFi" in the "source" section of Prod01_142 and Prod_163, including all Media

Access Control (MAC) addresses, Service Set Identifier (SSID's) information, and MAC addresses for any data that could be associated with a Bluetooth beacon;

[. . .]

3. Details concerning Google's Sensorvault, including:
    a. how the location data is captured and collected;
    b. how often Google collects location data on Android phones, both through the operating system and through Google applications, services, or software;
    c. how often Google collects location data on non-Android phones using Google applications, services, or software;
    d. all manuals, policies, guidelines, presentations, and protocols relating to how the location data is captured and collected;
    e. all algorithms used in capturing and collecting the location data, including the algorithm version number(s) and year(s) developed;
    f. how Google stores the location data;
    g. all manuals, policies, guidelines, presentations, and protocols relating to how Google stores the data;
    h. all algorithms used in storing the location data, including the algorithm version number(s) and year(s) developed;
    i. how Google analyzes and sorts the location data to respond to law enforcement requests;
    j. all manuals, policies, guidelines, presentations, and protocols relating to how Google analyzes and sorts the location data to respond to law enforcement requests;

k. all algorithms used in analyzing and sorting the location data, including the algorithm version number(s) and year(s) developed;

l. all information about the accuracy of the location data, including any tests, validation studies, error rates and how the error rates were calculated (including whether they reflect test or operational conditions);

4. Parameters of Google's Sensorvault data, including:

a. how many individuals' tracking information is in the Sensorvault;

b. how often, if ever, information in the Sensorvault is purged;

c. who has access to the Sensorvault;

d. how the Sensorvault is maintained;

e. all privacy policies relating to the Sensorvault.

5. The name(s) and training, certifications, and qualifications of the individual(s) at Google who gathered and turned over the location data in this case to law enforcement officials;

[. . .]

8. All information about how law enforcement officials manipulated and analyzed the Sensorvault data to identify accounts for which Google provided additional information in the second and third rounds of the search process, including;

a. how law enforcement officials made determinations about which accounts to investigate further;

b. how law enforcement officials made determinations about which accounts to not investigate further;

c. what data law enforcement officials relied on to make these determinations;

9. Any and all Sensorvault data that Google initially determined to be potentially responsive to the warrant and subsequent law enforcement requests but excluded from the Sensorvault data ultimately Google provided to law enforcement officials in this case, including the reason(s) for the exclusion;
10. The name(s) and training, certifications, and qualifications of the analyst(s) who used the Sensorvault data to identify particular accounts to seek additional information from Google about;
11. For all law enforcement agencies and officers involved in this case, copies of any and all:

    [. . .]

    c. training materials in the possession of law enforcement agencies for obtaining and using Sensorvault data;

    d. contracts, memorandums of understanding and agreements, including but not limited to nondisclosure agreements, concerning the use of Sensorvault data, or that bind the law enforcement agencies;

    e. internal policies, guidelines, training manuals, or presentations concerning use of Sensorvault data;

12. All records produced as a result of the requests described above.

ECF No. 28 at 1-5. For the reasons set forth below, Mr. Chatrie is entitled to discovery on all of these requests under *Brady*, Rule 16, or both.

ARGUMENT

1. *Brady* (Due Process)

A. Legal Standard

For nearly sixty years, the Supreme Court has made clear that the Fifth Amendment's guarantee of due process requires the government to disclose to the defense in a criminal prosecution all evidence "favorable to an accused" and "material either to guilt or to punishment," *Brady*, 373 U.S. at 87. Evidence is material if there is a "reasonable probability that, had the evidence been disclosed to the defense, the result of the proceeding would have been different. A 'reasonable probability' is a probability sufficient to undermine confidence in the outcome." *United States v. Bagley*, 473 U.S. 667, 682 (1985).

Evidence that undermines confidence in the outcome of a case includes evidence that could affect the integrity of the government's investigation, impact the veracity or reliability of witness statements or testimony, conflict with or diminish the value of other evidence in the government's case, and support a case against a different suspect. *See Kyles v. Whitley*, 514 U.S. 419, 441-54 (1995); *Bagley*, 473 U.S. at 678; *Giglio v. United States*, 405 U.S. 150, 153-54 (1972). "The question is not whether the defendant would more likely than not have received a different verdict with the evidence, but whether in its absence he received a fair trial . . . ." *Kyles*, 514 U.S. at 434; *see also Smith v. Cain*, 565 U.S. 73, 75 (2012) (finding material evidence that undercut the only link between the defendant and the alleged crime, and rephrasing *Kyles*' definition of reasonable probability as "[a] reasonable probability does not mean that the defendant 'would more likely than not have received a different verdict with the evidence,' only that the likelihood of a different result is great enough to 'undermine[ ] confidence in the outcome of the trial.'").

In this case, the discovery requested relates to the potential suppression of the identification of Mr. Chatrie as a suspect. The only way that the government identified Mr. Chatrie as a suspect

was through the data it obtained from the geofence warrant. Thus, under the fruit of the poisonous tree doctrine, *see Wong Sun v. United States*, 371 U.S. 471 (1963), but for the unconstitutional search that led to the identification of Mr. Chatrie as a suspect, the government would not have been able to collect any other evidence against Mr. Chatrie and that evidence likewise must be suppressed. If the Court finds that the geofence warrant was an unreasonable search under the Fourth Amendment, then there is no case that the government can present against Mr. Chatrie because all of the evidence against him will have been suppressed. *See Wong Sun*, 371 U.S. at 488 (finding that the question of whether evidence is a "fruit" of illegal police activity is "whether, granting establishment of the primary illegality, the evidence to which instant objection is made has been come at by exploitation of that illegality or instead by means sufficiently distinguishable to be purged of the primary taint.") (internal quotation marks omitted). The question in this case, then, as to materiality, is had the evidence requested been disclosed to the defense, whether a probability sufficient to undermine confidence in the outcome of the Court's anticipated suppression ruling exists.

Every circuit that has decided the question of whether *Brady* applies in the suppression context has held that it does. *See United States v. Gamez-Orduno*, 235 F.3d 453, 461 (9th Cir. 2000) ("The suppression of material evidence helpful to the accused, whether at trial or on a motion to suppress, violates due process if there is a reasonable probability that, had the evidence been disclosed, the result of the proceeding would have been different."); *Smith v. Black*, 904 F.2d 950, 965-66 (5th Cir. 1990) ("The appropriate assessment for *Brady* purposes, of course, is whether nondisclosure affected the outcome of the suppression hearing."), *rev'd on other grounds*, 503 U.S. 930 (1992) (vacating judgment in light of *Stringer v. Black*, 503 U.S. 222 (1992), which addressed procedural aspects of habeas petition). In *Nuckols v. Gibson*, 233 F.3d 1261, 1266-67

(10th Cir. 2000), the Tenth Circuit found that *Brady*'s disclosure obligations applied to impeachment evidence material to a pretrial hearing regarding the admissibility of the defendant's confession, which was the only evidence tying the defendant to the crime. The Second Circuit has not yet decided the question of whether Brady applies in the suppression context, but in *United States v. Nelson*, 193 F. App'x 47, 50 (2d Cir. 2006), the court remanded the case for an evidentiary hearing on the suppression issue and noted that the *Brady* question would "be mooted if the Government, in advance of the hearing, turns over any material not already given to the defense in advance of the trial that may bear on the outcome of the suppression hearing." No circuit[1] has held that *Brady* does not apply in the suppression context.

Rather than squarely address the issue, the Fourth Circuit has assumed without deciding that *Brady* applies in the suppression context. *See United States v. Williams*, 10 F.3d 1070, 1077 (4th Cir. 1993) ("we assume *arguendo* but decline to address definitively on the merits the issue of whether *Brady* should call for disclosure of material evidence at pre-trial suppression hearings")[2]. But, the Fourth Circuit has long-required that evidence be disclosed at a time when it will be of value to the defense. "If it is incumbent on the State to disclose evidence favorable to an accused, manifestly, that disclosure to be effective must be made at a time when the disclosure would be of value to the accused." *Hamric v. Bailey*, 386 F.2d 390, 393 (4th Cir. 1967); *accord*

[1] In *United States v. Jones*, 725 F. App'x 763, 765-66 (11th Cir. 2018) (finding evidence government failed to disclose not material), the Eleventh Circuit analyzed an alleged *Brady* violation as if *Brady*'s disclosure obligations applied in the suppression context. *See also United States v. Sigillito*, 759 F.3d 913, 929-30 (8th Cir. 2014) (analyzing an alleged *Brady* violation as if *Brady*'s disclosure obligations applied in the suppression context); *Murray v. United States*, 704 F.3d 23, 30-32 (1st Cir. 2013) (analyzing an alleged *Brady* violation as if *Brady*'s disclosure obligations applied in the suppression context).

[2] Four other circuits have also not squarely addressed the issue. *See United States v. Thomas*, 835 F.3d 730, 734 (7th Cir. 2016) (observing that Seventh Circuit has not yet taken a position on whether *Brady* applies in the suppression context); *United States v. Taylor*, 471 F. App'x 499, 520 (6th Cir. 2012) (assuming without deciding that *Brady* applies in the suppression context); *United States v. Donahue*, 460 F. App'x 141, 143-44 (3d Cir. 2012) (assuming without deciding that *Brady* applies in the suppression context); *United States v. Bowie*, 198 F.3d 905, 912 (D.C. Cir. 1999) (declining to decide whether *Brady* applies in the suppression context).

United States v. Elmore, 423 F.2d 775, 779 (4th Cir. 1970). Even though suppression of incriminating evidence may be unrelated to the actual culpability of an accused person, the rationale behind *Brady* "applies with equal force" to evidence that is necessary to challenge the constitutionality of a search. *United States v. Barton*, 995 F.2d 931, 935 (9th Cir. 1993). That is particularly so when the ruling at issue is case dispositive. *See Nuckols*, 233 F.3d at 1266-67. To hold that *Brady* did not apply to case dispositive suppression rulings, "would effectively deprive a criminal defendant of his Fourth Amendment right to challenge the validity of a search []." *Id.*

B. Materiality

The information requested is material to Mr. Chatrie's argument that the geofence general warrant violated his Fourth Amendment rights. Requests 1, 3, 4(a), 4(b), 4(e), 8, and 9 relate to at least one of three issues that are central to the success of his suppression motion: overbreadth, lack of particularity, and lack of voluntariness. Requests 11(c) and 11(e) seek potential impeachment evidence. Without access to this information, there is a likelihood of a different result in the suppression proceeding great enough to undermine confidence in the outcome. *Smith*, 565 U.S. at 75; *Bagley*, 473 U.S. at 682.[3]

1. Wi-Fi Access Points

Request 1 concerns information about the location of the Wi-Fi access points that Google used to estimate the location of users identified as responsive to the first step of the geofence warrant. *See* ECF No. 28 at 1-2. This information bears directly on the warrant's overbreadth and lack of particularity. According to the expert testimony of Mr. Spencer McInvaille, 88% of the location points initially produced by Google came from Wi-Fi data, which is not as accurate as

[3] Furthermore, this Court "may consider directly any adverse effect that the prosecutor's failure to respond [to the discovery request] might have had on the preparation or presentation of the defendant's case." *Bagley*, 473 U.S. at 683.

GPS, and depends on Google's assumptions about where nearby Wi-Fi access points (e.g., routers) are physically located. 1/21/20 Tr. at 64-70. Because Wi-Fi networks can extend up to 150 feet from the access point, an access point that was close to the edge of the 150-meter geofence would have been "seen" by devices well outside the geofence radius. *Id.* at 65. As Mr. McInvaille explained, this appears to have caused Google to include users in the initial warrant return who were never inside the geofence at all. *Id*. at 65, 69. Thus, for example, Mr. McInvaille demonstrated that "Mr. Green" was probably never inside the geofence, but was simply driving down a road next to the Journey Christian Church on his way home from a nearby hospital. *Id.* at 82.

Access to information about the location of the relevant Wi-Fi access points will permit Mr. Chatrie to determine how many devices Google may have falsely placed within the 150-meter geofence. *Id.* at 68. The government presented no information to the issuing magistrate about this possibility or the likelihood of ensnaring people outside the scope of the warrant. These facts, however, go directly to Mr. Chatrie's overbreadth and particularity arguments, as he maintains that the scope of the search was impermissibly broad and afforded too much discretion to law enforcement to determine whose data would be produced and ultimately de-anonymized. Without this information, neither the parties nor the Court would have a complete understanding of the nature of the search and seizure that occurred in this case. Such a deficient factual record would undermine confidence in the outcome of Mr. Chatrie's suppression motion and impair his likelihood of success.

2. "Sensorvault" Details

Request 3 asks for details concerning Google's "Sensorvault," the cache of location information collected from users. *See* ECF No. 28 at 2-3. Subparts (a)-(e) seek to establish how Google *captures and collects* this information from users, including the frequency of collection,

policies and procedures for collection, and the algorithms involved in the collection process. *Id.* at 2. Subparts (f)-(h) relate to how Google *stores* this location information, also seeking policies and procedures as well as the relevant algorithm. *Id.* at 2. Likewise, subparts (i)-(k) ask for the policies and procedures as well as the algorithm involved in *analyzing and sorting* location data in response to law enforcement requests. *Id.* at 2-3. And subpart (l) seeks information about the accuracy of the location data, including any tests and validation studies. *Id.* at 3.

All of the items in Request 3 bear on the breadth and particularity of the geofence warrant in this case, as well as the degree of voluntariness involved in conveying location information to Google. The warrant, for example, required Google to produce location data for "each type" of Google account inside the 150-meter geofence, *see* ECF No. 54-1 at 4, 9. As Mr. McInvaille testified, Google classifies the location information it collects into three categories: "Location History," "Google Location Services," and "Web & App Activity." *See* 1/21/20 Tr. at 23. But as Google proffered in its *amicus* brief, its response to the geofence warrant was limited to a search of "Location History" data only—meaning that it did not search data generated as a result of Google Location Services or Web & App Activity. *See* ECF No. 59-1 at 12. Google, however, provides no support for this assertion and does not explain why it would restrict the search in a manner contrary to the plain language of the warrant. In other cases, involving requests for account-specific data, Google typically indicates in the raw warrant return which category of location data is at issue (e.g., "Location History" or "Web & App Activity"). *See* 1/21/20 Tr. at 29-31. But in this case, Google did not do so, raising further questions about what data was actually searched and produced to law enforcement.

What data Google searched and why are fundamental facts in Mr. Chatrie's suppression claim. If Google did search Location History data only, then Google's rationale is likely to

strengthen Mr. Chatrie's argument that the warrant gave too much discretion to non-judicial officers. *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 v. United States*, 389 U.S. 347, 356 (1967)). If Google searched more than Location History, such as Google Location Services or Web & App Activity, then it would bolster Mr. Chatrie's argument that he did not voluntarily convey his location information to Google. Google maintains that users must "opt-in" to Location History tracking through a multi-step process, *see* ECF No. 59-1 at 7-8, whereas Google Location Services and Web & App Activity are enabled by default. Thus, if the geofence search did include data from either Google Location Services or Web & App Activity, then the lack of voluntariness involved in transmitting this information to Google would be even more apparent to the Court.[4]

Additionally, information about how Google responds to geofence warrants and provides ostensibly "anonymized" data to law enforcement is directly relevant to the warrant's overbreadth and lack of particularity. Mr. Chatrie maintains that the warrant application misrepresented the intrusiveness of the initial two steps of the search process by repeatedly describing the data produced to law enforcement as "anonymized." *See* ECF No. 54-1 at 2-3. As Mr. McInvaille demonstrated, Google's use of pseudonyms in place of user IDs did little to actually mask the identities of the individuals whose data was produced to law enforcement. 1/21/20 Tr. at 73-92. Instead, the location coordinates provided by Google may be sufficient to ascertain the likely identities of users. *Id.*; *see also* ECF No. 68 at 3-5. Furthermore, it appears that there may be a direct and predictable relationship between the pseudonyms assigned by Google and the true

[4] Mr. Chatrie does not concede that the "opt-in" procedure that Google has devised for Location History is in fact truly knowing and voluntary for the vast majority of users. *See* 1/21/20 Tr. at 57-58.

device IDs that have been supposedly anonymized. Information about this process and the anonymization algorithm employed by Google is likely to confirm this suspicion. If true, such a misrepresentation would undermine the government's argument that the search does not raise significant privacy concerns. It would also further establish the warrant's overbreadth and lack of particularity because, in practice, it effectively granted law enforcement access to more identifiable information than the warrant appears to authorize.

Finally, information about the accuracy of the location data provided by Google bears on the breadth and particularity of the warrant. As was the case with "Mr. Green," the way Google estimates the location of users can have the effect of falsely including people inside the geofence. *See* 1/21/20 Tr. at 65, 69, 82. Or in other words, it effectively extends the reach of the geofence well beyond 150 meters. *Id*. at 66. Indeed, Mr. McInvaille testified that as a result, the initial search might have extended the reach of the geofence by as much as 50 meters, which would encompass nearby businesses as well as a hotel, a self-storage facility, apartment buildings, and a large road. *Id.* at 66-67. Information about the accuracy of Google's process for determining user location would likely confirm that the geofence captured users outside the 150-meter radius and demonstrate that Google was aware of this phenomenon. Similarly, access to the algorithmic process Google uses to collect and analyze user location data would likely assist Mr. Chatrie in assessing the accuracy of the geofence warrant returns and, consequently, the true breadth of the search. *Id.* at 70-71. It would allow the defense to determine how many devices may have been falsely identified as having been within the 150-meter geofence. It would also allow the defense to verify the error rates and confidence values that Google provides in the raw warrant returns. Like Mr. Chatrie's request for information about the Wi-Fi access points, the algorithms Google uses relate directly to Mr. Chatrie's overbreadth and particularity arguments. If Google provided

the government with "estimates" instead of "facts," *see* ECF No. 59-1 at 10, *id*. n.7, 13 n.8, 20 n.12, then the defense deserves to know how Google came up with those estimates, especially if Google's process effectively expands the scope of the search in a way unknown to the magistrate who signed the warrant.

The information Mr. Chatrie seeks in request 3 is essential to understanding the nature of the search and seizure that occurred in this case. It is also likely to further strengthen his arguments that the collection of his location data was not truly voluntary and that the geofence warrant used to search it was unconstitutionally broad and lacked particularity. Without these facts, neither Mr. Chatrie nor the Court will have a true understanding of what occurred in this case, thereby undermining confidence in the outcome of the Court's suppression hearing.

3. Sensorvault Parameters

Request 4 also concerns Sensorvault, and subparts (a), (b), and (e) are likewise discoverable under *Brady*. *See* ECF No. 28 at 3. Request 4(a) seeks the total number of users with location information in Sensorvault, the purpose of which is to determine how many users had their location data searched by Google in step one of the geofence warrant process. As Google explains in its *amicus* brief, conducting a geofence search requires a uniquely broad search of "all" Google users' timelines. *See* ECF No. 59-1 at 11. The defense, which crafted its discovery request prior to Google's *amicus* brief, understood the warrant to require a search of each category of location data in the Sensorvault, i.e., Location History, Google Location Services, and Web & App Activity. Therefore, the defense asked for the total number of users with location data in the Sensorvault. Google, however, stated that it searched Location History data only. ECF No. 59-1 at 12-13. But in either event, Mr. Chatrie seeks to determine the number of users who were searched at step one of the geofence warrant process, be it every user in the Sensorvault, or every user with Location History enabled. Mr. Chatrie is confident that this will be an extraordinarily

large number of users, likely in the millions or billions. *See* 1/21/20 Tr. at 168. Such information is undoubtedly helpful to Mr. Chatrie's overbreadth and particularity arguments, as the assuredly unprecedented scope of this search was not supported by probable cause and was not presented to the issuing magistrate.

Request 4(b) asks for information about how often, if ever, Google purges location information from the Sensorvault. *See* ECF No. 28 at 3. This would tell Mr. Chatrie how far back in time law enforcement can search. As in *Carpenter v. United States*, access to historical location cell phone location data gives the government "access to a category of information otherwise unknowable" by allowing it to "travel back in time to retrace a person's whereabouts, subject only to the retention policies of the wireless carriers." 138 S. Ct. 2206, 2218 (2018). Such surveillance "runs against everyone" and gives law enforcement access to "each carrier's deep repository of historical location information at practically no expense." *Id*. Mr. Chatrie seeks to know how deep that repository goes here. Mr. Chatrie believes that some location information may be retained indefinitely and never be purged, a fact which would support Mr. Chatrie's voluntariness argument under *Carpenter*.

Similarly, request 4(e) seeks all privacy policies relating to the Sensorvault in effect from the date of the robbery through the time of the search, as Mr. Chatrie believes these policies will further support his voluntariness argument. *See* ECF No. 28 at 3. While Google has a public privacy policy available online, it does not mention Sensorvault and only references Location History twice.[5] Mr. Chatrie therefore seeks any additional policies related to the privacy of his Sensorvault data that are not publicly available. This information is material because it would go

[5] *See* Google, Privacy Policy (January 22, 2019), https://policies.google.com/privacy/archive/20190122?hl=en-US.

to show the lack of control Mr. Chatrie had over the collection and retention of his Google location information, similar to the defendant in *Carpenter*. *See* 138 S. Ct. at 2220 (finding that a cell phone user does not voluntarily assume the risk of turning over a comprehensive dossier of his physical movements in any meaningful sense).

4. The "Narrowing" Process

Request 8 concerns what investigators did with the location information they received from Google in steps one and two of the geofence warrant process. *See* ECF No. 28 at 3-4. Step one of the warrant required Google to provide information on all Google users within 150 meters of the bank between 4:20 and 5:20 p.m. *See* ECF No. 54-1 at 4. It then required law enforcement to "attempt to narrow down the list" based on known information "specific to this crime" before returning that list to Google. *Id.* Step two required Google to produce additional data for each user identified on the narrowed list, including any travel outside the 150-meter geofence between 3:50 and 5:50 p.m. Once again, the warrant required law enforcement to "attempt to narrow down the list" with information that is "specific to this crime" before returning a final short list to Google. *Id.* at 5. Step three required Google to provide "identifying account information" for each user on that short list. *Id.* Mr. Chatrie seeks all information about how law enforcement manipulated and analyzed the data in order to comply with the terms of the warrant and "narrow down the list" before requesting additional information from Google in steps two and three.

While a request for "all" information about this narrowing process might be too broad under some circumstances, Mr. Chatrie does not believe that this request is too broad here and will not unduly burden the government. Rather, it appears as if law enforcement attempted to obtain the maximum amount of data possible and did not narrow down the list in step one, at least initially. In an email to Google following Google's step one production, the government asked for expanded

location information on every single user Google initially identified. *See* ECF No. 48-1 at 1.When Google did not respond, the government sent the same request again, asking once more for information on every user identified in step one. *See* ECF No. 48-2 at 1. Although law enforcement stated in both emails that "device numbers 1-9 may fit the more likely profile of the parties involved," investigators did not provide Google with a narrowed-down list until their third try, when they requested additional data on only those nine devices. *See* ECF No. 48-3 at 1. The information requested relates to potential impeachment by the law enforcement officials who testify about the government's attempts to "narrow down the list."

Mr. Chatrie submits that law enforcement attempted to obtain the maximum amount of data possible despite having already determined that half of the accounts they planned to search further did not fit the profile of parties involved in the crime. Information about how and when law enforcement determined which accounts to investigate further and which to abandon will demonstrate that Google, not a judicial officer, was responsible for determining whether law enforcement had complied with the terms of the warrant. Indeed, law enforcement recognizes that its initial requests for additional data on all users may "seem[] unreasonable," *see* ECF No. 48-1 at 1; ECF No. 48-2 at 1, leaving it up to Google to determine what data it ought to produce. Google, however, must not be the arbiter of what is "reasonable" under the Fourth Amendment. Rather, such negotiations between law enforcement and the recipient of a warrant are indicative of a profound lack of particularity and a delegation of the judicial function. Mr. Chatrie therefore believes that information about how law enforcement determined which accounts to search further will directly support his arguments that geofence warrants like this one are constitutionally impermissible.

5. Responsive Data Not Provided to Law Enforcement

Request 9 asks for information about the paths not taken, *i.e.*, "Sensorvault data that Google initially determined to be potentially responsive . . . but [did not provide] to law enforcement officials." ECF No. 28 at 4. It is at least possible that Google identified additional users within the geofence but then excluded them from the data it produced to law enforcement in step one. Indeed, such a scenario is likely if Google initially searched all data in the Sensorvault, including Google Location Services or Web & App Activity categories, and then later filtered the results to show Location History results only. If so, then Google would have records showing that other individuals were in the vicinity of the bank at the time of the robbery. Such records would be quintessential *Brady* evidence and highly probative of the unprecedented breadth and lack of particularity inherent in this geofence warrant. At the very least, these records would demonstrate that the pool of users subject to search by Google was larger than Google has acknowledged, supporting Mr. Chatrie's overbreadth and particularity arguments. Without such basic information about the scope of Google's initial search, it is difficult to place confidence in the result of any suppression hearing, making this data material.

6. Law Enforcement Procedures for Geofence Warrants

Finally, requests 11(c) and (e) concern law enforcement's procedures for obtaining Google location data from the Sensorvault. Request 11(c) seeks training materials on the subject and request 11(e) seeks the corresponding policies and procedures. *See* ECF No. 28 at 4-5. These documents are material for *Brady* purposes because they constitute potential impeachment evidence pursuant to *Kyles*, 514 U.S. at 433 (equating exculpatory and impeachment evidence for *Brady* purposes); *see also Bagley*, 473 U.S. at 682. In the suppression context, impeachment

evidence relates to the government's lack of good faith in obtaining and executing the geofence warrant at issue here.

The defense strongly suspects that the warrant in this case was produced using a template provided by a private company, namely "CellHawk."[6] A CellHawk geofence warrant template is available to law enforcement officials who attend CellHawk trainings, as well as select outsiders, such as Mr. McInvaille. Mr. McInvaille obtained the template from CellHawk's website, a copy of which is attached as Exhibit A.[7] The template is strikingly similar to the warrant in this case—indeed, it is mostly verbatim. *Compare* ECF No. 54-1 at 1-2 *with* Ex. A at 1-2. If the defense is correct, then law enforcement's reliance on CellHawk's template would be highly probative for purposes of determining good faith under *United States v. Leon* and its progeny. *See* 468 U.S. 897, 918-19 (1984). *Leon* cannot excuse systemic negligence directed by government-sponsored trainings and search warrant templates that a private industry created.

Mr. Chatrie therefore seeks access to all training materials, policies, and procedures that address Google geofence warrants, especially if those documents originate from private companies such as CellHawk. On the other hand, if the government has no geofence policies and procedures of its own, then it should disclose that fact as well. In either case, such disclosure would strengthen Mr. Chatrie's argument that the government did not act in good faith when seeking the geofence warrant in this case. Consequently, such information is discoverable under *Brady* and *Giglio v. United States*, 405 U.S. 150 (1972), because it is likely to show that the government did not make an honest mistake. Instead, the government appears to have outsourced its operating procedures,

[6] *See, e.g.*, Hawk Analytics, http://www.hawkanalytics.com (last visited Feb. 18, 2020); *Features of CellHawk*, Hawk Analytics, http://www.hawkanalytics.com/features-of-cellhawk (last visited Feb. 18, 2020).

[7] This document is not available to the general public, but Mr. McInvaille was able to access it through his CellHawk account.

relying on training materials and templates offered by a private company that also happens to sell the analytic software used to interpret geofence data.[8] In this light, Mr. Chatrie ought to have access to all of the training materials and procedures provided to and utilized by law enforcement, as this information is likely to impeach the government's argument that it acted in good faith.

C. Google Is Part of the Prosecution Team

Mr. Chatrie has consistently argued that Google is "a part of the government's investigative team as it relates to the use of Google's location data in this case." ECF No. 49 at 2. Therefore, it is of no consequence if the information Mr. Chatrie requests from the government lies "in the possession, custody, and control of Google." *See* ECF No. 38 at 8. "*Brady*'s commands do not stop at the prosecutor's door; the knowledge of some of those who are part of the investigative team is imputed to prosecutors regardless of prosecutors' actual awareness." *United States v. Robinson*, 627 F.3d 941, 951 (4th Cir. 2010); *see also United States v. Harry*, Cr. No. 10-1915, at *9 (D.N.M. Oct. 10, 2014) ("United States prosecutors are 'encouraged to err on the side of inclusiveness when identifying the members of the prosecution team for discovery purposes.'"); *id.* at *4 (quoting Department of Justice Memorandum Regarding Guidance for Prosecutors Regarding Criminal Discovery ("Ogden memo"), authored by former Deputy Attorney General David W. Ogden, dated January 4, 2010). Here, Google is part of the "prosecution team" for *Brady* purposes. *See Kyles*, 514 U.S. at 437.

As the Supreme Court clarified in *Kyles*, the scope of required disclosure under *Brady* includes not just information known to the "individual prosecutor," but also "others acting on the government's behalf in the case." 514 U.S. at 437. The *Kyles* Court focused on the agency-principal relationship (*i.e.* who is "acting on . . . *behalf*" of the government) when determining

[8] *See, e.g., CellHawk Overview*, Hawk Analytics, http://www.hawkanalytics.com/cellhawk-overview (last visited Feb. 18, 2020).

Brady's reach. *See* 514 U.S. at 437-38 (emphasis added). Thus, following *Kyles*, courts have found third parties to be a part of the prosecution team where they serve as the government's agents in particular cases. In *United States v. Ackerman*, then-Judge Gorsuch found that the National Center for Missing and Exploited Children (NCMEC) was a government agent for Fourth Amendment purposes where NCMEC reviewed an email for suspected child pornography and alerted law enforcement, as required by statute. 831 F.3d 1292, 1301-1302 (10th Cir. 2016). The question is "simply whether the agent acts with the principal's consent and (in some way) to further the principal's purpose." *Ackerman*, 831 F.3d at 1301. Similarly, in *United States v. Rosenschein*, the court held that NCMEC was a part of the prosecution team for discovery purposes because it was "*involved in the investigation of the case*" and "*provided information to the government* in aid of the prosecution," No. CR 16-4571 JCH, 2019 WL 2298810, at *7 (D.N.M. May 30, 2019) (emphasis in original).

The critical point is to make an agency determination based on the facts of the particular case. It is not sufficient, for example, to infer an agency-principal relationship based on the structure of government agencies. *Compare United States v. Taylor*, 942 F.3d 205, 224-25 (4th Cir. 2019) (finding that officers with the Bureau of Alcohol, Tobacco, Firearms, and Explosives were not part of the FBI prosecution team because they "were looking into an *entirely separate* case.") (emphasis added), *and Horton v. United States*, 983 F. Supp. 650, 655, n.10 (E.D. Va. 1997) (finding that a prison was not "part of the [United States Attorney's] investigatory team" where there was "no suggestion that [prison] officials participated in the federal investigation of [the] murder."), *with McCormick v. Parker*, 821 F.3d 1240, 1247–48 (10th Cir. 2016) (finding that a nurse who conducted a sexual-assault examination of the victim was part of the prosecution team because she "acted at the request of law enforcement in the pre-arrest investigation of a crime");

Bracamontes v. Superior Court of San Diego County, 2019 WL 6044552, at *6-10 (Cal. Ct. App. Nov. 15, 2019) (finding that private companies providing DNA testing services on behalf of the prosecutor are also considered a part of the prosecution team). Rather, the question turns on the "level of interaction between the prosecutor and the agency or individual." *See United States v. Meregildo*, 920 F. Supp. 2d 434, 440 (S.D.N.Y. 2013); *United States v. Locascio*, 6 F.3d 924, 949 (2d Cir. 1993); *Pina v. Henderson*, 752 F.2d 47, 49 (2d Cir. 1985). Where the government "knew of and acquiesced in the intrusive conduct" and the "party performing the search intended to assist law enforcement," then courts have generally found an agency-principal relationship. *See Ackerman*, 831 F.3d at 1301.

In this case, Google repeatedly "act[ed] on the government's behalf," *see Kyles*, 514 U.S. at 437, "to further the [government's] purpose" of finding a suspect in the bank robbery, *see Ackerman*, 831 F.3d 1301. It makes no difference that Google is not actually a governmental entity. *See Ackerman*, 831 F.3d at 1300; *Taylor*, 942 F.3d at 224-25. Google's investigative actions are comparable to NCMEC's in *Ackerman* and *Rosenchein*. First, as in *Ackerman*, Google had a statutory requirement to assist the government. *See* 831 F.3d at 1296 (finding it probative that 18 U.S.C. § 2258A and 42 U.S.C. § 5773(b) "mandate [NCMEC's] collaboration" with law enforcement). Here, the geofence warrant invokes section 19.2-70.3 of the Code of Virginia, which requires service providers like Google to disclose certain business records pertaining to their customers. ECF No. 54-1 at 3. And federally, as Google explains in its *amicus* brief, the Stored Communications Act requires "service providers such as Google to disclose data relating to a user's stored electronic communications."[9] ECF No. 73 at 20 (citing 18 U.S.C. § 2703). The

[9] While the Stored Communications Act is relevant to Google's relationship with the prosecution team, the defense maintains that neither it nor any statute can constitutionally authorize a geofence warrant.

contents of electronic communications must be disclosed in response to a warrant. 18 U.S.C. § 2703(a), (b)(1)(A).

Of course, mere compliance with a warrant does not transform its recipient into a government agent. But Google, like NCMEC, did not merely turn over existing evidence; it functioned instead as a critical part of the investigative team. Just as NCMEC reviewed files to determine if they contain child pornography, *see Ackerman*, 831 F.3d at 1301-1302; *Rosenchein*, 2019 WL 2298810, at *7, so too did Google review user location data to determine devices that matched the geofence criteria. Unlike warrants seeking data from a particular user or account, Google did not simply produce specific records; instead, Google was responsible for identifying them Indeed, Google functioned as part of the investigative team in this case by searching *all* of its users at the government's behest and creating multiple spreadsheets of data based on the government's evolving requests. *See* ECF No. 73 at 12-13. Moreover, Google was responsible for developing the entire three-step process prescribed in the geofence warrant. *See* ECF No. 73 at 12 (stating that Google "developed a multi-step . . . protocol" for responding to geofence warrants). It was also Google that determined when the list of users had been sufficiently "narrowed" to proceed with the second step of the warrant. *See* ECF No. 48-1 at 1 (deferring to Google with respect to the reasonableness of the request); ECF No. 48-2 at 1 (same); ECF No. 48-3 at 1 (same). Google was no mere witness. It was deeply "involved in the investigation of the case," *see Rosenschein*, 2019 WL 2298810, at *7, and hewed closely to the specifics of the government's requests, just as an agent would act to "further the principal's purpose," *see Ackerman*, 831 F.3d at 1301.

In sum, the government obtained a warrant using a tiered disclosure process that Google itself designed, for a search that Google conducted at the behest of law enforcement officers

working on this case. Consequently, Google's role here was as a private actor participating in a specific criminal investigation at the behest of the government, just like the hospital nurse in *McCormick*, 821 F.3d at 1247–48, or the DNA testing company in *Bracamontes*, 2019 WL 6044552, at *6-10. Thus, this Court should find that Google was a part of the prosecution team in this case. As a matter of fundamental fairness and due process, Mr. Chatrie is entitled to information demonstrating the unconstitutionality of the investigative techniques used against him. As a key member of the government's investigative team, Google "has the means to discharge the government's *Brady* responsibility," and opposition to doing so "boils down to a plea to substitute [Google] for the prosecutor, and even for the courts themselves, as the final arbiter[] of the government's obligation to ensure fair trials." *See Kyles*, 514 U.S. at 438.

2. Rule 16

A. Legal Standard

Federal Rule of Criminal Procedure 16(a)(1)(E) requires disclosure of evidence that "is material to preparing the defense " if "the item is within the government's possession, custody, or control." Rule 16 requires much broader disclosure than the government's disclosure obligations under the due process demands of *Brady*. *See United States v. Caro*, 597 F.3d 608, 620 (4th Cir. 2010) (citing *United States v. Baker*, 453 F.3d 419, 424 (7th Cir. 2006) (recognizing that Rule 16 requires disclosure of both inculpatory and exculpatory evidence that "might assist in preparation of a defense")). There must be some indication that disclosure of the requested evidence will enable the defendant to "significantly alter the quantum of proof in his favor." *Caro*, 597 F.3d at 621 (internal quotation marks omitted). "'[E]vidence is material as long as there is a strong indication that it will play an important role in uncovering admissible evidence, aiding witness preparation, corroborating testimony, or assisting impeachment or rebuttal.'" *Caro*, 597 F.3d at

621 (quoting *United States v. Lloyd*, 992 F.2d 348, 351 (D.C. Cir. 1993) (observing that this materiality standard "normally is not a heavy burden")).

Rule 16 applies pretrial and the federal rules specifically contemplate its connection to suppression hearings. Federal Rule of Criminal Procedure 12(b)(4) governs discovery for pretrial hearings, including suppression hearings. Federal Rule of Criminal Procedure 12(b)(4)(B) provides that "[a]t the arraignment or as soon afterward as practicable, the defendant may, in order to have an opportunity to move to suppress evidence under Rule 12(b)(3)(C), request notice of the government's intent to use (in its evidence-in-chief at trial) any evidence that the defendant may be entitled to discover under Rule 16." (emphasis added); *see also* 1A Charles A. Wright & Andrew D. Leipold, *Federal Practice & Procedure: Criminal* § 195, at 451 (4th ed. 2008) (stating that Rule 12(b)(4)(B) is "intended to facilitate the making of a pretrial motion for the suppression of evidence"). One of the primary purposes of Rule 16's pretrial disclosure obligation is to protect a defendant's constitutional right to a fair trial, in part by allowing the defendant to challenge the constitutionality of admitting specific pieces of evidence. *See United States v. McElroy*, 697 F.2d 459, 464 (2d Cir. 1982) ("Pretrial discovery prevents the defendant from being unfairly surprised with his statements at trial and enhances the ability of defense counsel to suppress inadmissible statements."). That application is directly on point here.

B. Materiality

All of the information discoverable under *Brady* and its progeny is also discoverable under Rule 16. For the reasons described above, requests 1, 3, 4(a), 4(b), 4(e), 8, 9, 11(c), and 11(e) are likely to significantly alter the quantum of proof in Mr. Chatrie's favor. All of this information is material because it will help the defense uncover admissible evidence, prepare expert witnesses, corroborate testimony, and assist impeachment or rebuttal. *See Caro*, 597 F.3d at 621. Moreover,

courts have repeatedly held that "[a] party seeking to impeach the reliability of computer evidence should have sufficient opportunity to ascertain by pretrial discovery whether both the machine and those who supply it with data input and information have performed their tasks accurately." *United States v. Budziak*, 697 F.3d 1105, 1112 (9th Cir. 2012) (quoting *United States v. Leibert*, 519 F.2d 542, 547–48 (3rd Cir. 1975)); *see also Supplemental Order Regarding C-3 Motion to Compel Discovery and Production of Evidence: Torrential Downpour Software* at 4, *United States v. Schwier*, No. 3:17-cr-0095, (D. AK, Nov. 18, 2019) (Ex. B) (finding the functionality, reliability, and accuracy of third-party software were material to the defense); *United States v. Gonzales*, No. CR1701311001PHXDGC, 2019 WL 669813, at *5 (D. Ariz. Feb. 19, 2019) (granting access to third-party software where the defense presented evidence that called into question the government's version of events, and finding that "the functions of the [program] constitute[] a 'very important issue' for [Gonzales's] defense.")).

Additionally, the remainder of Mr. Chatrie's discovery requests—4(c), 4(d), 5, 10, 11(d), and 12—are material under Rule 16 for the reasons below.

1. Sensorvault Parameters

Request 4(c) seeks records of who has access to the Sensorvault. This information is material under Rule 16 because it will aid the defense in identifying witnesses with knowledge of the Sensorvault and its operations. There are significant unanswered questions about the types of location information Google stores in Sensorvault and the types of data subject to search pursuant to a geofence warrant. Identifying the individuals with access to Sensorvault will therefore assist the defense in identifying potential witnesses who can answer these questions and corroborate (or challenge) Google's assertion that it searched only users with Location History enabled. *See* ECF No. 59-1 at 12.

Request 4(d) seeks records regarding how Google maintains the Sensorvault. This information is material under Rule 16 because it will aid the defense in understanding what data goes into the Sensorvault, how it is stored, and when, if ever, Google deletes it. Like request 4(b), this information will elucidate the historical reach of geofence warrants as well as the degree of voluntariness associated with Google's collection and storage of Mr. Chatrie's data. And like request 4(c), it will help Mr. Chatrie identify witnesses with knowledge of the Sensorvault and its operations. All of the information requested in 4(c) and 4(d) is therefore material and discoverable under Rule 16.

2. Names, Training, Certification, and Qualifications

Requests 5 and 10 ask for the names and qualifications of individuals who were involved in the geofence search process. Request 5 pertains to Google employees, whereas request 10 pertains to law enforcement. Mr. Chatrie seeks to learn the names of these individuals as well as their relevant training, certifications, and qualifications. This information is material under Rule 16 because it will aid Mr. Chatrie in identifying witnesses who can corroborate or discredit critical claims, such as Google's assertion that it searched only users with Location History enabled. *See* ECF No. 59-1 at 12. Additionally, the information constitutes potential impeachment evidence pursuant to *Kyles v. Whitley* with respect to any law enforcement or Google witnesses testifying about the geofence search process. Finally, it will assist the defense in preparing its own expert to testify at the geofence suppression hearing.

3. Contracts, Memoranda, & Agreements

Request 11(d) asks for contracts, memoranda of understanding, and agreements between Google and law enforcement relevant to the use of Sensorvault data for the geofence search in this case. *See* ECF No. 28 at 4. The defense does not seek all agreements between law enforcement

and Google, but only those concerning geofence searches in effect at the time of the search in this case. This information is material because it would go to show the close relationship between Google and law enforcement, similar to other third-party sources that courts have determined to be part of the prosecution team. *See, e.g., United States v. Rosenschein*, No. CR 16-4571 JCH, 2019 WL 2298810, at *9-10 (D.N.M. May 30, 2019) (finding that memoranda and agreements with Microsoft are material and discoverable where they show the nature of agency relationship); *see also Ackerman*, 831 F.3d at 1301 ("An agency relationship is usually said to 'result[ ] from the manifestation of consent by one person to another that the other shall act on his behalf and subject to his control, and consent by the other so to act.'") (quoting Restatement (Second) of Agency § 1 (1958)). Furthermore, the government denies that Google functioned as a part of the prosecution team, ECF No. 64 at 5-6. Mr. Chatrie therefore deserves to access contracts and agreements that would contradict the government's denial. For all of these reasons, request 11(d) is material under Rule 16.

4. Other Documents

Request 12 seeks all records produced as a result of the geofence warrant in this case, including notes or memoranda of conversations regarding the search or actions taken as part of the search process, as well as any written justification for such actions. This information is material under Rule 16 because it will help the defense in uncovering admissible evidence. For example, the government asserts that it acted in "good faith" because it "followed the approach endorsed by *McLamb*," *i.e.*, "consulted with prosecutors—both state and federal—about GeoFence warrants." ECF No. 41 at 22. As a result, the government is likely to have documents regarding this consultation that bear on the question of good faith. These documents would likely speak to the constitutionality of the warrant's breadth and lack of particularity. They may also show law

enforcement's rationale for seeking expanded location data on all 19 users in step two of the search. In any event, such documents constitute potential impeachment evidence pursuant to *Kyles v. Whitley* with respect to any law enforcement or Google witnesses testifying about the geofence search process. They will also assist the defense in preparing its own expert to testify at the geofence suppression hearing.

C. Google Is a Part of the Prosecution Team

Google is a part of the "government" under Rule 16 for the same reasons it is a part of the "prosecution team" under *Brady*—it "act[ed] on the government's behalf in the case." *See Kyles*, 514 U.S. at 437. Mr. Chatrie may therefore request items that are "within [Google's] possession, custody, or control" through Rule 16. *See* Fed. R. Crim. P. 16(a)(1)(E). The government's "disclosure obligation under Rule 16," just as under *Brady*, "turns on 'the extent to which the prosecutor has knowledge of and access to the documents sought.'" *See Horton*, 983 F. Supp. at 654 (citing *United States v. Bryan*, 868 F.2d 1032, 1036 (9th Cir. 1989)).The other courts that have defined "government" in Rule 16 have also generally equated it with the "prosecution team." *See Rosenschein*, 2019 WL 2298810, at *4 (collecting cases); *United States v. Brodnik*, 710 F. Supp. 2d 526, 544 (S.D.W. Va. 2010) (collecting cases); *Weems v. United States*, 191 A.3d 296, 300 (holding that the government's disclosure obligations under Rule 16 apply to "the entire 'prosecution team.'"). As argued above, Google's investigative actions pursuant to the general warrant in this case made it part of the "prosecution team." In turn, Google is part of the "government" under Rule 16 and is subject to Mr. Chatrie's discovery requests.

CONCLUSION

For the foregoing reasons, Mr. Chatrie respectfully submits that he is entitled to discovery on all of the outstanding requests in ECF No. 28. Each requested item is material to the defense

and discoverable under *Brady*, Rule 16, or both, regardless of whether it is in the possession of Google, which functioned as an agent of the prosecution team in this case.

Respectfully submitted,

OKELLO T. CHATRIE

By: _____/s/_____

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

_____/s/_____

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

CERTIFICATE OF SERVICE

I hereby certify that on February 18, 2020, I filed the foregoing with the Clerk of Court using the CM/ECF system, which will send a notification of such filing (NEF) to all counsel of record.

/s/

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

SUPERIOR COURT OF <Enter your state here>

County of <Enter your county here>

SEARCH WARRANT

<Enter your full name here> swears under oath that the facts expressed by him in the attached and incorporated **Statement of Probable Cause** are true and that based thereon he has probable cause to believe and does believe that the articles, property, electronic communications, and data described below are lawfully seized pursuant to <code> et seq., as indicated below, and are now located at the location(s) set forth below. Wherefore, Affiant requests that this Search Warrant be issued.

_____

(Signature of Affiant)

THE PEOPLE OF THE STATE OF <Enter your state here> **TO ANY PEACE OFFICER IN THE COUNTY OF** <Enter your county here>: proof by affidavit, having been this day made
before me by <Enter your full name here>, finds that there is probable cause to believe that the property and/or person described herein may be found at the locations set forth herein and is lawfully seized pursuant to <code> et seq., as indicated below by **X** (s) in that:

- When the property was stolen or embezzled;
- When the property or things were used as the means of committing a felony:
- When the property or things to be seized consist of an item or constitute evidence that tends to show that a felony has been committed, or tends to show that a particular person has committed a felony;
- When the property or things are in the possession of any person with the intent to use them as a means for committing a public offense, or in the possession of another to whom he or she may have delivered them for the purpose of concealing them or preventing their discovery;
- There is a warrant to arrest a person;
- When a provider of electronic communication service or remote computing service has records or evidence, as specified in <code>, showing that property was stolen or embezzled constituting a misdemeanor, or that property or things are in the possession of any person with the intent to use them as a means of committing a misdemeanor public offense, or in the possession of another to whom he or she may have delivered them for the purpose of concealing them or preventing their discovery;

PLACE TO BE SEARCHED:

See Attachment A

ITEMS TO BE SEIZED:

See Attachment B

Attachment "A"

YOU ARE THEREFORE COMMANDED TO SEARCH:

Google, LLC – An Electronic Communications Service Provider
Google Legal Investigations Support
1600 Amphitheatre Parkway
Mountain View, CA, 94043

Service via Google's Law Enforcement Request System (LERS) on-line
Service may be via email at uslawenforcement@google.com

Attachment "B"

ITEMS TO BE SEIZED AND SEARCHED:

This warrant is directed to Google, LLC, headquartered at 1600 Amphitheatre Parkway, Mountain View, California, and applies to:

Records pertaining to:

Identifying information according to the "**Production Protocol**" described below for Google accounts that reported a GPS, cellular, WiFi or Bluetooth sourced location history data generated from devices that reported a location within the geographic region bounded by the following coordinates dates and times ("**Initial Search Parameters**"):

Search 1:

Date and Time Period:
<Enter start date and time> to <Enter end date and time>

Target Location:
A radius of <enter radius> meters around Latitude <enter latitude>, Longitude <enter longitude>.The area is further described as the immediate area around <address, city and state> and is pictured in the following image:

Image 1:

Production Protocol:

1. Google shall query location history data based on the **Initial Search Parameters** (as described above).
2. For each location point recorded within the **Initial Search Parameters**, Google shall produce anonymized information specifying the corresponding unique device IDs of all location data, whether derived from Global Positioning System (GPS) data, cell site/cell tower triangulation/trilateration, Bluetooth beacons, precision measurement information such as timing advance or per call measurement data, and Wi-Fi location, including the GPS coordinates, estimated radius, and the dates and times of all location recordings (with captured time zone), data source and device type (platform), during the date and time period associated with specific device IDs; (the "**Anonymized List**").
3. Law enforcement shall review the **Anonymized List** to remove device IDs that are not relevant to the investigation, for example, device IDs that were not in the location for a relevant period of time, or device's that remained at the location after law enforcement arrival. Law enforcement will also shortlist the Anonymized List by reviewing the time stamped location coordinates for each device ID and compare that against the known time and location information that is specific to this crime. Law enforcement will also compare the Anonymized List for each location and attempt to locate device IDs located at two or more identified locations.
4. If additional location information for a given anonymized device ID is needed in order to determine whether that anonymized device ID is relevant to the investigation, law enforcement may request that Google provide additional location coordinates for the time period that fall outside of the **Initial Search Parameters**. These contextual location coordinates may assist law enforcement in identifying anonymized device IDs that were located outside the search locations, were not within the search locations for a long enough period of time, were moving through the search locations in a manner inconsistent with the facts of the underlying case, or otherwise are not relevant to the investigation.

<Special note: It is our recommendation to use a second legal demand when seeking subscriber data. If you proceed with subscriber data under one legal demand, you can leave PP #5. Be sure to remove PP #5 if using a second warrant as well as any language in the body of the warrant related to subscriber data. See instructions tab for details; special attention California agencies. Be sure to check with your prosecutors before moving forward>

5. For those anonymized device IDs identified as relevant pursuant to the ongoing investigation through an analysis of provided records, and upon demand by law enforcement, Google shall provide identifying information for the Google accounts associated with each identified anonymized device IDs, to include subscriber's name, street address, telephone number(s), email addresses, services subscribed to, last six (6) months of IP history, SMS account number, and registration IP, all information provided by the subscriber to the service provider to establish or maintain an account or communications channel.

Investigating officers and those agents acting under the direction of the investigating officers are authorized to access all data to determine if the data contains the items as described above. Those items that are within the scope of this warrant may be copied and retained by investigating officers.

Order for Production of Records

It is hereby ordered that any records produced in response to this search warrant may be provided via email or digital storage media to:

<Enter your full name here>
<Enter your address here>
<Enter your city here> ,
<Enter your state here>
<Enter your zip here>
<Enter your here>
<Enter your here>

Order to Delay Notice:

<Be sure to include a Non-Disclosure/Delay of Notice since Google's policy is to notify their users of law enforcement requests unless otherwise ordered to not disclose>
This matter having come before this Court pursuant to an affidavit and petition which requests the issuance of an order commanding Google, LLC to not disclose to or notify any person of the existence of the warrant ("criminal process") attached hereto, the Court finds that:

1. The criminal process is issued pursuant to 18 U.S.C. § 2703(b)(1) (search warrant for the content) or 18 U.S.C. § 2703(c)(2) (criminal process for non-content records), therefore the <Enter your agency here> is not requested to provide notice to the subscriber or customer;
2. The Petition is valid pursuant to 18 U.S.C. § 2703 (b); and
3. Per 18 U.S.C. § 2705(a), there is reason to believe that the notification to any person, other than as is necessary to provide the demanded records, documents, data, and/or content of the existence of the criminal process will result in:
    - Endangering the life or physical safety of an individual;
    - Flight from prosecution;
    - Destruction of or tampering with evidence;
    - Intimidation of potential witnesses; or
    - Otherwise seriously jeopardizing an investigation or unduly delaying a trial.

I further state that the other means of preventing the identified results of the aforementioned disclosure or notification are not readily employable because:

- I do not know the true identity of the suspect in this investigation;
- I do not know the current location of the suspect in this investigation;
- I do not know the location of or description of specific evidence the suspect may possess or to which the suspect may have access to;
- I believe the suspect is in the presence of or has access to a victim or vulnerable person (e.g., a child) who may be a victim of the aforementioned crimes being investigated; and/or,
- Other: <enter other>

It is hereby ordered that Google and the executing agency shall delay notification of the existence of this warrant, or the existence of the investigation, to the subscribers or to any other person:

- permanently; or,
- for a period of time not less than <##> days.

STATEMENT OF PROBABLE CAUSE

Summary:

<Briefly explain the purpose of the warrant. Example:
I am currently investigating a <crime> that occurred on <date>. There are no suspects and I have not yet located any witnesses. The purpose of this search warrant application is to authorize the examination of Google location history records from the time and place of the <crime> to identify potential suspects and witnesses.

Affiant's Experience:

I, <Enter your full name here>, being a duly sworn peace officer for the State of <Enter your state here>, have been employed by the <Enter your agency here> for <Enter years of employment> years.

<Insert affiant's law enforcement experience here>

Investigation:

This affidavit is made in support of a search warrant requesting the listed geo-location information as described in Attachment B, related to a criminal investigation of <code(s)> which began on <date> as described below.

<Insert case-specific reasons for choosing those times listed. Example: "Witness Jones reported hearing a single gunshot at 3:40 a.m. Officer Smith discovered the victim's body at 3:45 a.m. and saw no other people in the immediate area. Therefore, I am requesting records from approximately 10 minutes before the murder through the arrival of Officer Smith.">

Google Location History Data:

Based on my training and experience, I know most people in today's society possess cellular phones and other connected devices (e.g. tablets, watches, laptops) used to communicate electronically. I know these devices are capable of sending and receiving communications in many different forms. I know most people carry cellular phones on their person and will carry them whenever they leave their place of residence. I know that cellular phones may include global positioning systems (GPS) and other technology for determining a more precise location of the device.

I know a subject's physical cellular phone often times does not retain all the data relevant to a specific crime. Portions of this data may only be on the Electronic Communications Service Provider's server located in the subscriber's account. Google services are often interconnected with a log-in to a Google account allowing access to many of the other Google services.

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

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

I know nearly every Android powered device has an associated Google account. I also know that Apple iPhone's supports several Google applications, such as Google Search, Gmail, Google Maps, and Google Drive, all of which require a Google account. I also know Google continuously tracks devices with an associated Google account.

Based on my training, experience and conversations I've had with other law enforcement officers and/or from reviewing documentation, I know that Google collects and retains location data on their servers (also known as the "Sensorvault" database) from Android enabled mobile devices, as well as devices supporting Google applications such as Google Search, Gmail, Google Maps, and Google Drive, so long as the location services of the phone are enabled. The location data gathered is stored forever, unless it is deleted by the user. The company uses this information for location-based advertising and location-based search results. Per Google, this information is derived from Global Position System (GPS) data, cell site/cell tower information, Bluetooth beacons, and Wi-Fi access points. While the specific parameters of when this data is collected are not entirely clear, it appears that Google collects this data not only whenever one of their services is activated and/or whenever there is an event on the mobile device such as a phone call, text messages, internet access, or email access, but also when the user is not interacting with the device (e.g. applications running in the background).

Additionally, location information digitally integrated into images, videos, or other computer files sent via the cellular phone can further indicate the geographic location of the account's user at a particular time. Digital cameras, including cameras built into a cellular phone, frequently store GPS coordinates in the metadata of image files, indicating where a photo was taken. These image files may be stored in the account user's Google cloud storage.

Based on my training and experience, I know when a user activates a Google Account, Google will request an associated phone number for the user, to assist in password recovery if a password is forgotten or for security purposes.

Given that almost all cellular phones and connected devices are either supported by Google or support Google software and most people in today's society carry a cellular phone or other connected device on their person at nearly all times, I believe it is likely the suspect(s) involved in this criminal investigation were in possession of at least one cellular phone/device, which was either powered by Android OS or had a cellular phone with a Google application.

Based on my training and experience, suspects involved in criminal activity will typically use cellular phones to communicate when multiple suspects are involved. I am also aware Android based cellular phones report detailed location information to Google, where the geo-location and electronic data is then stored on their servers.

The timeframe of the Google request of <Date and Timeframe (e.g. 12/12/2018, 10pm PDT to 12/13/2018, 7:00am PDT)> will allow investigators to see which Google device IDs were present in the geographic area prior to, during, and after the crime. The information provided by the extended timeframe and times when entering and exiting the geographical area will allow investigators to determine which device IDs require further investigation and which ones do not.

The initial device IDs provided by Google do not include any subscriber information and is provided in an anonymized list.

I believe the information provided by Google will assist investigators in understanding a bigger geographic picture and timeline, which may tend to identify potential witnesses, as well as possibly inculpate or exculpate the account owners. I therefore believe that it is likely that a review of Google's location history will help law enforcement in developing suspect(s) in a felony crime, the crime of <code(s)> and provide possible witnesses to the crime.

As such, I am requesting a list of any Google anonymized device IDs in a geographic area around the <address of target location(s)> in particular, the geographical region(s) identified in Attachment B and the date(s) and time(s) specified. This Application seeks authority to collect certain location information related to Google device IDs that were located within the Target Location(s) during the Date and Time Period (Anonymized List).

The information sought from Google regarding the Anonymized List will potentially identify which cellular phones/devices were near the location where the crime occurred and may assist law enforcement in determining which persons were present or involved in the crime under investigation.

Law enforcement shall review the Anonymized List to remove device IDs that are not relevant to the investigation, such as device IDs that were not in the location for a sufficient period of time. If additional location information for a given device ID is needed in order to determine whether that device is relevant to the investigation, law enforcement may request that Google provide additional location coordinates for the time period that fall outside of the target location. These contextual location coordinates may assist law enforcement in identifying devices that were located outside the target location, were not within the target location for a long enough period of time, were moving through the target location in a manner inconsistent with the facts of the underlying case, or otherwise are not relevant to the investigation.

Google Legal Process Service Location:

On <date>, I confirmed the location where Google accepts service of search warrants by reviewing the www.search.org "ISP List." Based on my experience and discussion with other members of law enforcement, I know that SEARCH is a national non-profit organization dedicated to sharing information and training law enforcement. The "ISP List" is constantly updated and is commonly relied upon by law enforcement to determine the location to send search warrants to a wide range of communications service providers, financial institutions and other record holders.

According to the SEARCH ISP List, Google, LLC accepts search warrants at the following location:

Google Legal Investigations Support
Google LLC
1600 Amphitheatre Parkway
Mountain View, CA 94043
Service may be via email at uslawenforcement@google.com

Productions of Records

Based on my training and experience, I know that the requested records are maintained in electronic format. I also know that Google prefers to produce records in an electronic format and that electronic records are easier for investigators, prosecution and defense to use. Therefore, I request an order that any records be provided in electronic format to the following address:

<Enter your full name here>
<Enter your address here>
<Enter your city here> ,
<Enter your state here>
<Enter your zip here>
<Enter your here>
<Enter your here>

Conclusion:

The facts set forth in this affidavit are based upon my own personal observations, my training and experience, and information obtained during this investigation. Therefore, based on the above facts, I have probable cause to believe, and do believe, that evidence of the commissions of felonies, in violation(s) of <code(s)>, and property related to the commission of said felonies, will be located on the premises described above. I request that a search warrant be issued with respect to the above location for the seizure of said property.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

_____ _____
(Signature of Affiant / Date)

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA, Plaintiff, v. MATTHEW WILLIAM SCHWIER, Defendant.	Case No. 3:17-cr-00095-SLG

SUPPLEMENTAL ORDER REGARDING C-3 MOTION TO COMPEL DISCOVERY AND PRODUCTION OF EVIDENCE: TORRENTIAL DOWNPOUR SOFTWARE

On October 24, 2019, after an evidentiary hearing, the Court entered an order at Docket 231 that granted in part and denied in part Defendant Matthew William Schwier's C-3 Motion to Compel Discovery and Production of Evidence: Torrential Downpour Software at Docket 199. The Court directed the government to conduct certain validation testing of the Torrential Downpour software in the presence of the defense.[1] The October 24, 2019 order set out the factual background relevant to this issue and it is not repeated here.[2]

The Court's October 24, 2019 order allowed the defense to file a supplemental declaration of its expert to explain why it believed additional testing was necessary, and the Court notified the parties that it may amend its order as

[1] Docket 231 at 12–14.

[2] *See* Docket 231 at 1–12.

warranted in light of that declaration.[3] On October 31, 2019, the defense timely filed a supplemental ex parte declaration of Jeffrey M. Fischbach, offered as a computer forensics expert.[4] The defense filed a redacted copy of Mr. Fischbach's declaration on the same day, from which it had removed all information it claimed as privileged.[5]

On November 1, 2019, the government filed a motion responding to Mr. Fischbach's redacted declaration, asking the Court to either hold an immediate status hearing or issue an order finding that the defense had not shown that additional tests were material.[6]

The Court granted the government's motion and held a brief status conference on November 4, 2019,[7] after which the parties conducted validation testing of the Torrential Downpour software pursuant to the Court's October 24, 2019 order.[8] The Court held a second status conference after the completion of the validation process, on November 5, 2019, at which it notified the parties that it

[3] Docket 231 at 12, 14.

[4] Docket 233.

[5] Docket 234.

[6] Docket 235.

[7] Docket 240.

[8] *See* Docket 231 at 12–13 (ordering government to conduct "the validation process described at Docket 219-1").

would issue a written order that would address whether additional testing would be ordered in light of Mr. Fischbach's October 31, 2019 declaration.

DISCUSSION

Pursuant to Federal Rule of Criminal Procedure 16(a)(1)(E)(i), the government must disclose any "books, papers, documents, data . . . or copies or portions" thereof upon the defendant's request, provided that the item is in the government's control and is "material to preparing the defense." "A defendant must make a 'threshold showing of materiality' in order to compel discovery pursuant" to this rule.[9] "Neither a general description of the information sought nor conclusory allegations of materiality suffice; a defendant must present facts which would tend to show that the Government is in possession of information helpful to the defense."[10]

In *United States v. Budziak*, the Ninth Circuit held that a district court had erroneously denied the defense's request for discovery of EP2P, a piece of investigative software similar to Torrential Downpour.[11] The Circuit concluded that the defendant had demonstrated materiality by "identif[ying] specific defenses to

[9] *United States v. Budziak*, 697 F.3d 1105, 1111 (9th Cir. 2012) (citing *United States v. Santiago*, 46 F.3d 885, 894 (9th Cir. 1995)).

[10] *Id.* (quoting *United States v. Mandel*, 914 F.2d 1215, 1219 (9th Cir. 1990)).

[11] *Id.* at 1111–12.

the distribution charge that discovery on the EP2P program could potentially help him develop."[12] The Circuit cautioned:

> In cases where the defendant has demonstrated materiality, the district court should not merely defer to government assertions that discovery would be fruitless[,] . . . especially . . . where . . . a charge against the defendant is predicated largely on computer software functioning in the manner described by the government, and the government is the only party with access to that software.[13]

It explained that "[a] party seeking to impeach the reliability of computer evidence should have sufficient opportunity to ascertain by pretrial discovery whether both the machine and those who supply it with data input and information have performed their tasks accurately."[14] In its October 24, 2019 order, the Court found that the functionality, reliability, and accuracy of Torrential Downpour were material to Mr. Schwier's defense.[15]

However, the government asserted that production of the software was precluded by the law enforcement privilege recognized in *Roviaro v. United* States,

---

[12] *Id.* at 1112. The defendant in *Budziak* "presented evidence suggesting that the FBI may have only downloaded fragments of child pornography files from his 'incomplete' folder, making it 'more likely' that he did not knowingly distribute any complete child pornography files to [federal] [a]gents." *Id.* He also "submitted evidence suggesting that the FBI agents could have used the EP2P software to override his sharing settings." *Id.*

[13] *Id.* at 1112–13.

[14] *Id.* at 12 (quoting *United States v. Leibert*, 519 F.2d 542, 547–48 (3rd Cir. 1975).

[15] Docket 231 at 7–8.

353 U.S. 53 (1957).[16] Balancing the government's interest against the defendant's,[17] the Court found in its October 24, 2019 order that based on the record then before it, "the validation process proposed by the government [was] sufficient to meet the defense's needs."[18] The Court noted that Mr. Fischbach had spoken only in generalities at the evidentiary hearing about why production of the software for additional testing by him was necessary to the defense.[19] Mr. Fischbach claimed that the defense's proposed testing ideas were confidential attorney work product and subject to the attorney-client privilege.[20] The Court concluded that it could not "rule on the materiality of forensic tests that have not been disclosed to it."[21]

In the ex parte portion of his subsequent October 31, 2019 declaration, Mr. Fischbach described four additional tests of the Torrential Downpour software that

---

[16] Docket 214 at 8–11.

[17] *See Roviaro*, 353 U.S. at 62 (directing courts to balance public interest in protecting flow of information to government against defendant's right to prepare his case, "taking into consideration the crime charged, the possible defenses, the possible significance of the informer's testimony, and other relevant factors").

[18] Docket 231 at 10–11.

[19] Docket 231 at 11.

[20] *See, e.g.*, Docket 230 at 6:24–7:4 (Excerpt of October 18, 2019 Hearing Transcript) ("[T]he findings that we have, and again, I'm being careful as far as privilege goes, the findings that we have have demonstrated some oddities possibly, but, again, they have to be tested to see if they are associated, but they certainly cause concern.").

[21] Docket 231 at 12.

he seeks to conduct at the Regional Computer Forensics Lab ("RCFL") in Anaheim, California.[22] Mr. Fischbach explained that these four tests are necessary to either develop or rule out specific defense strategies related to Counts 1 and 2 of the Third Superseding Indictment, both of which are premised on the FBI's use of the Torrential Downpour software.[23]

In the redacted copy of Mr. Fischbach's declaration, the entire description of these four tests and their relevance to the defense are blacked out.[24] The government argues that "[b]y redacting the tests themselves, the defense has withheld from the government any opportunity to contest the tests, or to agree with them."[25] The Court acknowledges the government's concerns and recognizes that in *United States v. Gonzales*, the defense disclosed the actual tests it wanted to run on Torrential Downpour in a way that permitted the government to argue against the testing.[26] Nevertheless, the Court is prepared to balance the defense's need for the additional testing of Torrential Downpour against the government's interest in restricting further access to the software.

---

[22] Docket 233-1 at 7–10, ¶ 23; Docket 234-1 at 7–10, ¶ 23 (redacted).

[23] Docket 233-1 at 7–10, 11 ¶¶ 23, 28; Docket 234-1 at 7–10, 11 ¶¶ 23, 28 (redacted); *see also* Docket 231 at 4 (describing basis of counts in indictment).

[24] Docket 234-1 at 7–10, ¶¶ 23, 28.

[25] Docket 235 at 3.

[26] No. CR-17-01311-001-PHX-DGC, 2019 WL 4040531, at *4–7 (D. Ariz. Aug. 27, 2019) (describing six tests and government's objections to their materiality).

Upon review of Mr. Fischbach's October 31, 2019 declaration, the Court concludes that requiring the Torrential Downpour software to be accessible to Mr. Fischbach for the additional testing at the Anaheim RCFL is warranted. In reaching this conclusion, the Court has considered that the government's interest in prosecuting Mr. Schwier for child pornography is not eviscerated by ordering the software's production. The government may opt to dismiss Counts 1 and 2; if it does so, it is not required to further produce the Torrential Downpour software to the defense. In that event, the government may still proceed on Count 3.[27] The Court also notes that the government would have the opportunity to assert that the conduct alleged in Counts 1 and 2 constitutes relevant conduct for sentencing purposes in the event Mr. Schwier is adjudged guilty on Count 3.

CONCLUSION

In light of the foregoing, the Court supplements its order at Docket 231 as follows:

(1) **Within seven days of the date of this order**, the government shall make the Torrential Downpour software available to Mr. Fischbach and defense counsel at the Regional Computer Forensics Lab in Anaheim, California, for a

[27] *United States v. Gonzales*, No. CR-17-01311-001-PHX-DGC, 2019 WL 669813, at *8 (D. Ariz. Feb. 19, 2019) ("When the two interests come squarely into conflict, the defendant's right to a fair trial should prevail because the government can always choose to protect its investigative technique by dropping the prosecution and due process dictates that a citizen should never be convicted in an unfair trial." (citing *United States v. Turi*, 143 F. Supp. 3d 916, 921 (D. Ariz. 2015))).

period of 21 consecutive days for additional testing. This testing shall be limited to the four tests described in Mr. Fischbach's October 31, 2019 declaration.

(2) The government may propose additional terms to the protective order entered at Docket 231 as warranted.

DATED this 8th day of November, 2019, at Anchorage, Alaska.

/s/ Sharon L. Gleason
UNITED STATES DISTRICT JUDGE