UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

information that is stored at premises controlled by Google, 1600 Amphitheatre Parkway, Mountain View, California 94043

Case No. 18-M-191 (DEJ)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A1 and A2

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim P. 41(c) is:

- ■ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: Title 18, United States Code, Sections 2113(a) and 924(c)

The application is based on these facts: See attached affidavit.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days:_____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

TFO Matthew Gibson, FBI
Printed Name and Title

Sworn to before me and signed in my presence:

Date: Nov. 20, 2018

Judge's signature

City and State: Milwaukee, Wisconsin

Honorable David E. Jones, U.S. Magistrate Judge
Printed Name and Title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Matthew Gibson, being first duly sworn on oath, on information and belief state:

I. INTRODUCTION, BACKGROUND, TRAINING, AND EXPERIENCE:

1. I make this affidavit in support of an application for a search warrant for information that is stored at premises controlled by Google, a provider of electronic communications service and remote computing service headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. § 2703(c)(1)(A) to require Google to disclose to the government copies of the information further described in Attachment B.

2. I have over 26 years of experience as a law enforcement officer and am currently assigned to the Milwaukee FBI Violent Crime Task Force as a Deputized Federal Task Force Officer. I was a Special Agent with the Federal Bureau of Investigation for over 23 years and have been an Investigator with the Milwaukee County District Attorney's Office since May, 2015. I have participated in numerous complex narcotics, money laundering, violent crime, armed bank robbery, and armed commercial robbery investigations in violation of Title 21, United States Code, Sections 841(a)(1), 843(b) and 846, and Title 18, United States Code, Sections 924(c), 1951, 1956, 1957, 2113, and other related offenses. I have employed a wide variety of investigative techniques in these and other investigations, including but not limited to, the use of informants, wiretaps, cooperating defendants, recorded communications, search warrants, surveillance, interrogations, public records, DNA collection, and traffic stops. I have also received formal training regarding the same. As a Federal Task Force Officer, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

3. Based on the facts set forth in this affidavit, there is probable cause to search the information described in Attachment A for evidence of a violation of in violation of 18 U.S.C. § 2113(a) (Bank Robbery) and 18 U.S.C. § 924(c) (Brandishing a Firearm During a Crime of Violence).

4. This affidavit is based upon my training and experience, my personal knowledge and information reported to me by other federal, state, and local law enforcement officers during the course of their official duties, all of whom I believe to be truthful and reliable. This affidavit is also based upon police reports, surveillance videos, and witness statements, that I consider to be reliable as set forth herein.

5. Because this affidavit is submitted for the limited purpose of a obtaining a search warrant, I have not included each and every fact known to me concerning this investigation.

II. JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense investigated." 18 U.S.C. § 2711(3)(A)(i).

III. BACKGROUND RELATING TO GOOGLE AND RELEVANT TECHNOLOGY

7. A cellular telephone or mobile telephone is a handheld wireless device used primarily for voice communication through radio signals. Cellular telephones send signals through networks of transmitter/receivers called "cells," enabling communication with other cellular telephones or traditional "landline" telephones. Cellular telephones rely on cellular towers, the location of which may provide information on the location of the subject telephone. Cellular telephones may also include global positioning system ("GPS") technology for determining the location of the device.

8. Google is an Internet company which, among other things, provides electronic communication services to subscribers. Google allows subscribers to obtain email accounts at the domain name gmail.com. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

9. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, I know that this information often provide clues to their identity, location or illicit activities.

10. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of login (i.e., session) times and durations, the types of service utilized, the status of the account (including

whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

11. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. Further, information maintained by the email provider can show how, where, and when the account was accessed or used. Based on my training and experience, I have learned that Google also maintains records that may reveal other Google accounts accessed from the same electronic device, such as the same computer or mobile device, including accounts that are linked by Hypertext Transfer Protocol (HTTP) cookies, which are small pieces of data sent from a website and stored in a user's Internet browser.

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

13. According to https://www.idc.com/promo/smartphone-market-share/os in 2017 Google's Android operating system was used in slightly more than 85% of the world's smartphones with Apple's OIS system being used in slightly less than 15%. In a 3 month period ending September 2018, Kantar Worldpanel, which collected data on the U.S. smartphone market share, indicated Google's Android operating systems accounted for 60.1 % of the U.S. market while Apple's OIS operating system accounted for 39.7%. This data was obtained from the website https://www.kantarworldpanel.com/global/smartphone-os-market-share/.

14. In addition, over the past 15 years the majority of subjects I have arrested and investigated have had cellular telephones and utilized them in some capacity in furtherance of their criminal activity, such as but not limited to; arranging meetings with co-conspirators; taking photographs of bank proceeds, firearms, and vehicles used in robberies; using Instant Messaging and Facebook posts to sell pills stolen from pharmacies; purchasing firearms which were used in robberies; using web searches to find pharmacies and cellular phone stores they later robbed; and sending text messages concerning robberies. Also, in numerous police reports I have reviewed as part of these criminal investigations the subjects almost always have a cellular telephone mentioned in the report or seized as evidence.

15. Based on my training and experience, I have learned that Google collects and retains location data from Android-enabled mobile devices when a Google account user has enabled Google location services. The company uses this information for location-based advertising and location-based search results. This information is derived from GPS data, cell site/cell tower information, and Wi-Fi access points.

16. Location data can assist investigators in understanding the chronological and geographic context of the email account access and use relating to the crime under investigation.

This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email).

IV. PROBABLE CAUSE

17. On 10/13/2018, two unidentified male subjects ("UNSUB #1" and "UNSUB #2") committed an armed robbery of the Great Midwest Bank ("GMB"), which is located at 600 Hartbrook Drive, #117 in Hartland, WI. The UNSUBs entered the bank at approximately 9:02 a.m. through the front door of the GMB. UNSUB #1 approached the teller counter and engaged the two bank employees while UNSUB #2 loitered behind UNSUB #1. Shortly thereafter, UNSUB #2 leapt over the counter, displayed a handgun and ordered both employees to the floor. UNSUB #2 removed a plastic garbage bag, opened it up and the UNSUBs began taking money from the teller drawers and placing it into the plastic bag. The UNSUBs asked one of the bank employees for the keys to the vault which the employee provided to the UNSUBs. The UNSUBs entered the vault and removed three drawers of cash from the vault. The UNSUBs were very calm and very polite during the robbery despite the fact they had difficulty opening the vault and despite the fact the UNSUBs were in the GMB for approximately 7 minutes. The UNSUBs fled through the north facing rear door of the GMB at approximately 9:09 a.m. with the stolen U.S. currency, one teller drawer, two vault drawers, and the set of keys used to open the vault. External surveillance cameras from a neighboring business showed the UNSUBS walking north from the bank towards a path through a tree line located behind the GMB which abutted a residential neighborhood.

18. According to interviews with the two bank employees, there were no customers in the bank at the time UNSUB #1 and UNSUB #2 entered the bank. No one else entered the bank during the duration of the robbery.

19. Hartland, Wisconsin is a town with a population of approximately 9,110 according to the 2010 census.

20. From a review of surveillance videos and witness descriptions UNSUB #1 was described as an African-American male, approximately 40 to 48 years of age, bearded or unshaved face, subject wearing a light green zip up hooded jacket, blue jeans, black shoes, sunglasses, and a green stocking cap. UNSUB #2 was described as a male subject wearing a black hooded sweatshirt, blue jeans, black shoes, and gloves. UNSUB #2 had the hood up over his head and his face covered with some type of cloth in order to conceal his identity.

21. Google Maps identified the Great Midwest Bank, 600 Hartbrook Drive, #117, Hartland, WI, location using latitude/longitude data as 43.110877, -88.337330.

22. A neighborhood canvass was conducted by law enforcement following the GMB robbery which included the stores in the strip mall where GMB is located. An employee of Design Xchange ("DX"), which is located at 600 Hartbrook Drive, #114 in Hartland, WI, adjoining Great Midwest Bank, advised law enforcement of suspicious activity between 2:30 p.m. and 3:30 p.m. on 10/12/2018. The DX employee advised that an unidentified African-American male subject entered the DX, looked around the DX for a short period of time, and left. The DX store is a consignment store that sells home decor products. The DX employee thought the activity was suspicious based on the expression on the subject's face and his interaction with the employee. As the subject entered the store it appeared to the DX employee that the subject did not expect DX to be a home decor store. The subject also appeared to be confused when the DX employee

approached him and asked if he needed any assistance. The subject did not stay inside of the DX for very long and did not appear to be interested in any of the products inside of the store. The employee described this individual as an African-American male, approximately 38 to 48 years of age, 5'6" to 5'8" tall, unshaved, with a stocky build.

23. Based on my training and experience I know that robbery suspects often use utilize mobile cellular devices as tools in furtherance of their robbery conspiracies. For example, I know that robbery suspects often use accomplices as lookouts or getaway drivers and communicate with these accomplices through cell phones. Oftentimes, suspects conduct pre-robbery surveillance to determine the number of people inside of the store or the presence of law enforcement. In this instance it is probable that that the UNSUBs had a getaway driver waiting for them in a vehicle in the neighborhood north of the GMB. The UNSUBs entered the GMB through the front door of the bank. In addition, the UNSUBs were not seen on neighboring surveillance video approaching the building from the rear of the GMB before the robbery, but they fled out the rear of the GMB after the robbery. This indicates that the UNSUBs were dropped off in front of the GMB and picked up in the neighborhood north of the GMB. Witnesses stated the UNSUBs were extremely calm during the robbery despite the fact they spent approximately 7 minutes inside of the GMB and had difficulty unlocking the door to the vault. Investigators, who are familiar with the case, believe that the UNSUBs conducted surveillance on the GMB during the afternoon of 10/12/2018 based on the observation of the DX employee and the physical description of the subject seen by the DX employee being similar to UNSUB#1. Also, the UNSUBs actions in entering the front of GMB and fleeing out the rear door indicated a level of planning which would have required some familiarity with the area around GMB.

V. CONCLUSION

24. Based on the forgoing, it is probable that the unknown subjects of this investigation had cellular telephones which utilized either Google's Android or Apple OIS operating systems. I request that the Court issue the proposed search warrant. Because the warrant will be served on Google who will then compile the requested records at a time convenient to it, reasonable probable cause exists to permit the execution of the requested warrant at any time in the day or night.

VI. REQUEST FOR SEALING

25. It is further requested that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

ATTACHMENT A1

BANK ROBBERY LOCATION

Property To Be Searched

This warrant applies to information associated with all Google accounts that, during the **time period** described below, were accessed from a mobile device located in the **geographic region** described below.

1. **Date**: October 13, 2018
   Bank Robbery Location: 43.110877, -88.337330 (Latitude/Longitude)
   Time Period: 08:50 a.m. CST to 09:20 a.m. CST
   Radius: 30 meters around location coordinate

This warrant calls for information that is stored at premises controlled by Google, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043.

ATTACHMENT A2

BANK ROBBERY LOCATION

BANK ROBBERY LOCATION

Latitude/Longitude: 43.110877, -88.337330

Great Midwest Bank, 600 Hartbrook Drive #117, Hartland, WI.

Radius: 30 meters

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider shall provide responsive data (as described in Attachments A1 and A2) pursuant to the following process:

1. Google shall query location history data based on the Initial Search Parameters (as described in Attachments A1 and A2).

2. For each location point recorded within the Initial Search Parameters, Google shall produce anonymized information specifying the corresponding unique device ID, timestamp, coordinates, display radius, and data source, if available (the "Anonymized List").

3. Law enforcement shall review the Anonymized List to remove devices that are not relevant to the investigation, for example, devices 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.

4. For those device IDs identified as relevant pursuant to the process described above, law enforcement may request that Google Provide subscriber information for the Google Account associated with each identified device ID.