

# EXHIBIT A

(Docket Entry No. 1)

UNITED STATES DISTRICT COURT

for the  
District of Columbia

In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)

INFORMATION ASSOCIATED WITH

AND  
WHICH ARE  
STORED AT PREMISES CONTROLLED BY GOOG

Case No: 1:17-mj-619

Assigned To: Magistrate Judge Harvey, Michael G.

Date Assigned: 8/21/17

Description: Search and Seizure Warrant

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 (identify the person or describe the property to be searched and give its location):

See Attachment A incorporated herein and included as part of the Affidavit in Support of this Application for a Search Warrant

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B incorporated herein and included as part of the Affidavit in Support of this Application for a Search Warrant

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

- ☒ 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 a violation of:

Code Section	Offense Description
18 U.S.C. § 371	Conspiracy to Defraud the United States; Compensation to Members of Congress,
18 U.S.C. § 203, 18 U.S.C. § 1001	officers, others in matters affecting the Government; Providing Material False Statements,

The application is based on these facts:  
See Attached Affidavit

- ☒ Continued on the attached sheet.
- ☐ 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

Harry Lidsky, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 08/21/2017

City and state: Washington, D.C.

Judge's signature

U.S. Magistrate Judge G. Michael Harvey

Printed name and title

**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with [REDACTED]@gmail.com and [REDACTED]@gmail.com that are stored at premises owned, maintained, controlled, or operated by Google, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

**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 e-mails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on August 1, 2017, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all e-mails associated with the account, from January 1, 2017 to the present, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider shall deliver the information set forth above via United States mail, courier, or e-mail to: Zia Faruqui, 4<sup>th</sup> Floor, 555 4<sup>th</sup> St NW, Washington, DC 20001.

**II. Information to be seized by the government**

All information described above in Section I that constitutes fruits and evidence of violations of Title 18 United States Code Sections 371, and 203, those violations involving George HIGGINBOTHAM and Prakazrel Samuel MICHEL, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) Anicorn, LLC, its parent company or subsidiaries;
- (b) The relationship between HIGGINBOTHAM and MICHEL, including any consulting work performed by HIGGINBOTHAM for MICHEL and any consulting agreement or contract between HIGGINBOTHAM and MICHEL;
- (c) The individuals identified in the contract discussed above, as well as any law enforcement investigations of those individuals;
- (d) Any financial transactions involving HIGGINBOTHAM, MICHEL, or Anicorn;
- (e) Any payments to/from MICHEL, Anicorn, and HIGGINBOTHAM, and any bank accounts or companies that could be used by HIGGINBOTHAM or by MICHEL to conduct financial transactions;
- (f) Any information about the source, nature, and origin of funds being transferred into or out of the United States;
- (g) HIGGINBOTHAM's meeting with the Chinese Ambassador on July 17, 2017, as well as the source of the message communicated by HIGGINBOTHAM to the Chinese Ambassador;
- (h) Evidence indicating how and when the e-mail accounts were accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the e-mail account owners;

- (i) Evidence indicating the e-mail account owners' state of mind as it relates to the crimes under investigation;
- (j) The identity of the person(s) who created or used the user IDs, including records that help reveal the whereabouts of such person(s);
- (k) The identity of the person(s) who communicated with the user IDs about matters relating to the concealment or facilitating of funds, including records that help reveal their whereabouts.

### **III. GOVERNMENT PROCEDURES FOR WARRANT EXECUTION**

The United States government will conduct a search of the information produced by the Provider and determine which information is within the scope of the information to be seized specified in Section II. The information that is within the scope of Section II may be copied and retained by the United States.

Law enforcement personnel will then seal any information from the Provider that does not fall within the scope of Section II and will not further review the information absent an order of the Court.



AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the  
District of Columbia

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

INFORMATION ASSOCIATED WITH

AND

WHICH ARE STORED AT

Case No: 1:17-mj-619

Assigned To: Magistrate Judge Harvey, Michael G.

Date Assigned: 8/21/17

Description: Search and Seizure Warrant

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search  
of the following person or property located in the Northern District of California

(Identify the person or describe the property to be searched and give its location):

See Attachment A incorporated herein and included as part of the Affidavit in Support of this Application for a Search  
Warrant

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property  
described above, and that such search will reveal (Identify the person or describe the property to be seized):

See Attachment B incorporated herein and included as part of the Affidavit in Support of this Application for a Search  
Warrant

**YOU ARE COMMANDED** to execute this warrant on or before September 3, 2017 (not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the  
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the  
property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory  
as required by law and promptly return this warrant and inventory to U.S. Magistrate Judge G. Michael Harvey  
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.  
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose  
property, will be searched or seized (check the appropriate box)

☐ for \_\_\_\_\_ days (not to exceed 30) ☐ until the facts justifying the later specific date of \_\_\_\_\_

Date and time issued:

AUG 21 2017

3:45pm

Judge's signature

City and state:

Washington, D.C.

U.S. Magistrate Judge G. Michael Harvey

Printed name and title



Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:		

## Printed name and title

**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with [REDACTED] and

[REDACTED] that are stored at premises owned, maintained, controlled, or operated by Google, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

**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 e-mails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on August 1, 2017, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all e-mails associated with the account, from January 1, 2017 to the present, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider shall deliver the information set forth above via United States mail, courier, or e-mail to: Zia Faruqui, 4<sup>th</sup> Floor, 555 4<sup>th</sup> St NW, Washington, DC 20001.

**II. Information to be seized by the government**

All information described above in Section I that constitutes fruits and evidence of violations of Title 18 United States Code Sections 371, and 203, those violations involving George HIGGINBOTHAM and Prakazrel Samuel MICHEL, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) Anicorn, LLC, its parent company or subsidiaries;
- (b) The relationship between HIGGINBOTHAM and MICHEL, including any consulting work performed by HIGGINBOTHAM for MICHEL and any consulting agreement or contract between HIGGINBOTHAM and MICHEL;
- (c) The individuals identified in the contract discussed above, as well as any law enforcement investigations of those individuals;
- (d) Any financial transactions involving HIGGINBOTHAM, MICHEL, or Anicorn;
- (e) Any payments to/from MICHEL, Anicorn, and HIGGINBOTHAM, and any bank accounts or companies that could be used by HIGGINBOTHAM or by MICHEL to conduct financial transactions;
- (f) Any information about the source, nature, and origin of funds being transferred into or out of the United States;
- (g) HIGGINBOTHAM's meeting with the Chinese Ambassador on July 17, 2017, as well as the source of the message communicated by HIGGINBOTHAM to the Chinese Ambassador;
- (h) Evidence indicating how and when the e-mail accounts were accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the e-mail account owners;

- (i) Evidence indicating the e-mail account owners' state of mind as it relates to the crimes under investigation;
- (j) The identity of the person(s) who created or used the user IDs, including records that help reveal the whereabouts of such person(s);
- (k) The identity of the person(s) who communicated with the user IDs about matters relating to the concealment or facilitating of funds, including records that help reveal their whereabouts.



### **III. GOVERNMENT PROCEDURES FOR WARRANT EXECUTION**

The United States government will conduct a search of the information produced by the Provider and determine which information is within the scope of the information to be seized specified in Section II. The information that is within the scope of Section II may be copied and retained by the United States.

Law enforcement personnel will then seal any information from the Provider that does not fall within the scope of Section II and will not further review the information absent an order of the Court.

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH  
[REDACTED] AND  
[REDACTED], WHICH ARE  
STORED AT PREMISES CONTROLLED  
BY GOOGLE

Case No: 1:17-mj-619  
Assigned To: Magistrate Judge Harvey, Michael G.  
Date Assigned: 8/21/17  
Description: Search and Seizure Warrant

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Harry A. Lidsky, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with certain email accounts that are stored at premises controlled by Google, an e-mail provider headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 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(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B, using the procedures described in Section III of Attachment B.

2. I am a Senior Special Agent with the United States Department of Justice (DOJ), Office of the Inspector General (OIG), and have been since March 2010. Since mid-2013, I have been assigned to the Cyber Investigations Office. From October 1999 to September 2005, I was

employed as a Special Agent with the Drug Enforcement Administration (DEA). I graduated from the DEA Basic Agent Training Academy program in February 1999. I have received training in traditional investigative subject areas, and extensive training in the areas of computer and mobile device forensics. My past duties have involved the investigation of narcotics distribution, money laundering, bribery, fraud, and other crimes, including those committed by government employees. I have participated in numerous investigations of criminal activity, including investigations involving electronic communications that are relevant to criminal cases. My current duties with the DOJ-OIG include supporting investigations of criminal and administrative misconduct through forensic analysis of computers and mobile devices.

3. I have successfully completed more than ten training courses related to computer and mobile device forensic examination, including successful completion of the Federal Law Enforcement Training Center Seized Computer Evidence Recovery Specialist (SCERS) program and the Guidance Software EnCE Certified Examiner program. I have examined more than 289 mobile devices and computers in my career to date.

4. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18 United States Code Sections 371, 203, and 1001, have been committed by George HIGGINBOTHAM, Prakazrel Samuel MICHEL, and others. There is also probable cause to search the information described in Attachment A for evidence or fruits of these crimes further described in Attachment B.

### **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 being investigated.” 18 U.S.C. § 2711(3)(A)(i). As discussed more fully below, acts or omissions in furtherance of the offenses under investigation occurred within Washington, D.C. *See* 18 U.S.C. § 3237. Finally, the offenses under investigation are the subject of a grand jury investigation in the District of Columbia.

### **PROBABLE CAUSE**

7. On Saturday, July 15, 2017, two members of the DOJ Office of International Affairs (OIA), received separate calls from counterparts at the Embassy of the People’s Republic of China to the United States (Embassy), located in Washington, District of Columbia. The two callers are known to the DOJ and their positions at the Embassy are confirmed.

8. The two callers each inquired about the position HIGGINBOTHAM held at the DOJ, and about whether or not he should be meeting with the Chinese Ambassador to the United States. The Embassy callers were described as surprised to have learned that HIGGINBOTHAM would be meeting with the Ambassador.

9. The OIA employees informed their Chinese counterparts that they were unaware of HIGGINBOTHAM’s position at DOJ or of his planned meeting, and could not opine as to whether or not he should be allowed to see the Ambassador. The OIA employees were able to tentatively confirm HIGGINBOTHAM’s employment with DOJ. One of the OIA employees sent HIGGINBOTHAM an e-mail to his DOJ account and attempted to contact him via phone to obtain an explanation for the call from the Chinese. The OIA employees also contacted the DOJ

Office of Legislative Affairs (OLA), to which HIGGINBOTHAM is currently assigned, on detail from the Office of Justice Programs (OJP).

10. On July 20, 2017, I interviewed HIGGINBOTHAM about his contacts with the Chinese Embassy. In that interview, HIGGINBOTHAM acknowledged that he met with the Chinese Ambassador at the Chinese Embassy on Sunday, July 16, 2017. HIGGINBOTHAM stated that the meeting was arranged by MICHEL and that the purpose of the meeting was to deliver a message to the Chinese Ambassador on behalf of MICHEL. HIGGINBOTHAM further stated that the message concerned a particular matter relating to the foreign policy of the United States and China. HIGGINBOTHAM further stated that he occasionally does consulting work for MICHEL, and HIGGINBOTHAM claimed that he attended the meeting with the Chinese Ambassador in that capacity and not in his official capacity as a DOJ attorney.

11. On July 26, 2017, HIGGINBOTHAM voluntarily met with and was interviewed by Special Agents from the Federal Bureau of Investigation (FBI), along with your affiant. During that interview, HIGGINBOTHAM reiterated that the message he provided to the Chinese Ambassador, on behalf of MICHEL, dealt with a matter between the United States and China. HIGGINBOTHAM surmised that a person or entity might profit as a result of the information that he provided to the Chinese, but claimed not to have specific knowledge of, or direct involvement with, such profiteering.

12. A review of the contents of HIGGINBOTHAM's work email and his personal phone, which was searched with HIGGINBOTHAM's consent, revealed the following relevant evidence:

13. HIGGINBOTHAM's personal cell phone contained a photograph of what appears to be the second page of a contract. The contract states that a company called "Anicorn" will be

paid for “work done and/or efforts taken” to persuade “[t]he US Department of Justice (“USDOJ”), US Federal Bureau of Investigations [sic] (“FBI”), and any other relevant US Government agencies...to drop all civil and/or criminal cases and/or cease investigations and/or removal of any INTERPOL Red Notice...by 31 September 2017...against” four specified foreign individuals and their families. The contract further states that the cases and investigations will be dropped “with (a) no wrongdoing [sic] whatsoever; (b) no admission of guilt; (c) no forfeiture of any further assets other than” certain assets “that have already been seized in Switzerland.” The contract further states that the “Client” shall pay Anicorn a non-refundable retainer fee of 19,000,000 Euros, with the first payment of 2,000,000 Euros due on May 9, 2017. The contract further states that the “Client” shall pay Anicorn a “success fee” of 280,000,000 Euros when the “[m]atters...are achieved.”

14. Further inquiry with the FBI revealed that at least two of the four individuals identified in the contract are the subjects of an ongoing federal money-laundering investigation. (It should be noted that in the FBI interview, HIGGINBOTHAM identified the individual who was the subject of HIGGINBOTHAM’s conversation with the Chinese Ambassador, and that individual was not one of the individuals identified in the contract page.)

15. HIGGINBOTHAM’s personal cell phone also contained a photograph of a computer screen showing a wire transfer from a bank in Honk Kong, to a bank in Los Angeles. HIGGINBOTHAM photographed the computer screenshot on May 8, 2017. The wire transfer was dated May 8, 2017, the day before the due date of the first retainer payment specified in the contract, and was in the amount of €2,751,890.00 (approximately \$3,219,711.00). Law enforcement has corroborated via information from the bank that this transaction occurred, as well as other high value transactions.

16. Based on information observed in Higginbotham's personal cell phone, the bank account that received the May 8, 2017 wire transfer belongs to a company called Anicorn, LLC. Subsequent information received from the bank identified a secondary company which was responsible for the establishment of Anicorn. Contact information for the owner of that company was found in HIGGINBOTHAM's personal phone. The search of HIGGINBOTHAM's personal phone yielded several text messages between HIGGINBOTHAM's personal phone and the phone number associated with the owner of Anicorn's parent company, discussing various financial topics and mentioning MICHEL.

17. The information received from the bank revealed that on May 10, 2017, two days after the wire transfer from Hong Kong to the Anicorn bank account in Los Angeles, \$20,000 was wired from the Anicorn bank account to an account belonging to HIGGINBOTHAM. On May 11, 2017, at approximately 1:10 AM, Higginbotham called the bank, ostensibly to check the payment status.

18. On the day of that \$20,000 wire transfer, HIGGINBOTHAM received a message from MICHEL via the application "Wickr." Wickr is a messaging application that ensures secure communication through encryption services and via a message "self-destruction" feature, by which messages are automatically erased after they have been sent. (This particular message was recoverable from HIGGINBOTHAM's phone because HIGGINBOTHAM took a screen shot of the message.) MICHEL's message to HIGGINBOTHAM read, "Good," and was followed by the address of an apartment in Los Angeles.

19. On May 18, 2017, MICHEL made a withdrawal from the Anicorn, LLC account in the amount of \$33,000 in cash.

20. On June 26, 2017, approximately five weeks after MICHEL made the withdrawal from the Anicorn, LLC bank account, HIGGINBOTHAM used his personal cell phone to send a text message to MICHEL stating, "Check your email – sent you wiring instructions."

21. On June 29, 2017, HIGGINBOTHAM used his personal cell phone to send a text message stating, "Gotta see how the money flows with Sidehustle." Based on your affiant's training and experience, your affiant believes that this text message by HIGGINBOTHAM reflects his anticipation about profiting from a fraudulent (i.e. hustle) side job.

22. In his interviews with your affiant and with the FBI on July 20 and 26, 2017, HIGGINBOTHAM did not mention Anicorn, LLC or the contract discussed above. When questioned about his consulting work for MICHEL, HIGGINBOTHAM specifically denied any involvement with the Chinese and claimed that he was unaware of MICHEL having ever visited China, and did not know what role, if any, China played in any of MICHEL's business ventures.

23. Your affiant believes that the aforementioned evidence establishes probable cause that HIGGINBOTHAM has violated 18 U.S.C. § 203. Section 203 makes it a crime for an employee of the Executive Branch to "demand[], seek[], receive[], accept[], or agree[] to receive or accept any compensation for representational services, as agent or attorney or otherwise" in relation to "any proceeding, application, request for a ruling or other determination, contract, claim, controversy, charge, accusation, arrest, or other particular matter in which the United States is a party or has a direct and substantial interest" that is before any "department" or "agency." In particular, the photographs of the contract and the wire transfer information in HIGGINBOTHAM's phone, the \$20,000 wire transfer from the Anicorn account to HIGGINBOTHAM's account, HIGGINBOTHAM's connections to Anicorn, LLC, and HIGGINBOTHAM's admission that he performed consulting work for MICHEL, establish



probable cause that HIGGINBOTHAM, a current Department of Justice attorney, agreed to accept, and did in fact accept, compensation for representational services related to the federal criminal investigations identified in the contract.

24. Your affiant further believes that the evidence discussed above also establishes probable cause that HIGGINBOTHAM has violated 18 U.S.C. § 1001 by making material false statements in his interviews with DOJ OIG and with the FBI. In those interviews, which focused on HIGGINBOTHAM's meeting with the Chinese Ambassador, HIGGINBOTHAM specifically denied any involvement with the Chinese and claimed that he was unaware of MICHEL having ever visited China, and did not know what role, if any, China played in any of MICHEL's business ventures. In fact, the evidence set forth above shows that HIGGINBOTHAM was aware of the Anicom business deal discussed in the contract page and the accompanying wire transfer.

25. Your affiant further believes that the review of HIGGINBOTHAM's personal phone establishes probable cause to believe that the personal email accounts of HIGGINBOTHAM and MICHEL will yield evidence of the above-describe offenses.<sup>1</sup>

26. The review of HIGGINBOTHAM's personal phone shows that HIGGINBOTHAM regularly used the email address [REDACTED] to communicate with MICHEL at the email address [REDACTED] regarding business and financial matters, including matters related to China. Some examples of those communications include:

---

<sup>1</sup> This application has received the requisite approval from the Department of Justice for the search of an attorney's email account. Accordingly, the government will undertake a taint review as part of the content review process.

- a. In an e-mail dated March 1, 2017, HIGGINBOTHAM sent a message from his official DOJ account to MICHEL at [REDACTED]. In the message, HIGGINBOTHAM wrote "...Once you get back from China, you and I could meet at my office, get breakfast...If this sounds good, let me know your schedule once you get back from Beijing and I will try to set this up."
- b. On June 19, 2017, one week before HIGGINBOTHAM texted MICHEL with the message, "Check your email – sent you wiring instructions." HIGGINBOTHAM sent an email from [REDACTED] to [REDACTED]. The content of this message was not recoverable from HIGGINBOTHAM's phone.
- c. In several emails from June and July 2017, HIGGINBOTHAM received communications at the email address [REDACTED] regarding the formation of a company based in Dubai, United Arab Emirates called "[REDACTED] [REDACTED]" a company whose partners include MICHEL.

27. Your affiant believes that additional communications among HIGGINBOTHAM and MICHEL, as well as others involved in the events described above, exist within the stored communication held by Google.

28. On August 1, 2017, a preservation request was sent to Google for the accounts [REDACTED] and [REDACTED]. In general, an e-mail that is sent to a Google subscriber is stored in the subscriber's "mail box" on Google servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Google servers indefinitely. Even if the subscriber deletes the e-mail, it may continue to be available on Google servers for a certain period of time.

**BACKGROUND CONCERNING E-MAIL**

29. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail ("e-mail") access, to the public. Google allows subscribers to obtain e-mail accounts at the domain name gmail.com, like the e-mail accounts listed in Attachment A. 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 un-retrieved e-mail for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, e-mail 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.

30. In my training and experience, e-mail providers generally ask their subscribers to provide certain personal identifying information when registering for an e-mail account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail 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 provides clues to their identity, location or illicit activities.

31. In my training and experience, e-mail 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 log-in (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, e-mail 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 e-mail account.

32. In my training and experience, in some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. 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.

33. As explained herein, information stored in connection with an e-mail 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 e-mail account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of

occupancy” while executing a search warrant at a residence. For example, e-mail communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the e-mail provider can show how and when the account was accessed or used. For example, as described below, e-mail providers typically log the IP addresses from which users access the e-mail account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the e-mail account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate 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 e-mail). Last, stored electronic data may provide relevant insight into the e-mail account owner’s state of mind as it relates to the offense under investigation. For example, information in the e-mail account may indicate the owner’s motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

34. Based on the forgoing, 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 cause exists to permit the execution of the requested warrant at any time in the day or night.

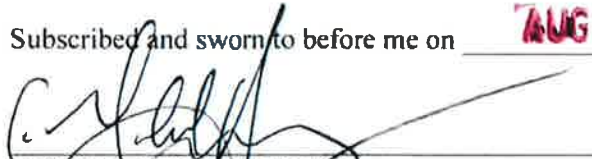
Respectfully submitted,



---

Harry A. Lidsky  
Senior Special Agent  
U.S. Department of Justice  
Office of the Inspector General

Subscribed and sworn to before me on AUG 21 2017, 2017



---

HONORABLE G. MICHAEL HARVEY  
UNITED STATES MAGISTRATE JUDGE

3 004

**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with [REDACTED] and [REDACTED] that are stored at premises owned, maintained, controlled, or operated by Google, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.



**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 e-mails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on August 1, 2017, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all e-mails associated with the account, from January 1, 2017 to the present, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider shall deliver the information set forth above via United States mail, courier, or e-mail to: Zia Faruqui, 4<sup>th</sup> Floor, 555 4<sup>th</sup> St NW, Washington, DC 20001.

**II. Information to be seized by the government**

All information described above in Section I that constitutes fruits and evidence of violations of Title 18 United States Code Sections 371, and 203, those violations involving George HIGGINBOTHAM and Prakazrel Samuel MICHEL, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) Anicorn, LLC, its parent company or subsidiaries;
- (b) The relationship between HIGGINBOTHAM and MICHEL, including any consulting work performed by HIGGINBOTHAM for MICHEL and any consulting agreement or contract between HIGGINBOTHAM and MICHEL;
- (c) The individuals identified in the contract discussed above, as well as any law enforcement investigations of those individuals;
- (d) Any financial transactions involving HIGGINBOTHAM, MICHEL, or Anicorn;
- (e) Any payments to/from MICHEL, Anicorn, and HIGGINBOTHAM, and any bank accounts or companies that could be used by HIGGINBOTHAM or by MICHEL to conduct financial transactions;
- (f) Any information about the source, nature, and origin of funds being transferred into or out of the United States;
- (g) HIGGINBOTHAM's meeting with the Chinese Ambassador on July 17, 2017, as well as the source of the message communicated by HIGGINBOTHAM to the Chinese Ambassador;
- (h) Evidence indicating how and when the e-mail accounts were accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the e-mail account owners;

- (i) Evidence indicating the e-mail account owners' state of mind as it relates to the crimes under investigation;
- (j) The identity of the person(s) who created or used the user IDs, including records that help reveal the whereabouts of such person(s);
- (k) The identity of the person(s) who communicated with the user IDs about matters relating to the concealment or facilitating of funds, including records that help reveal their whereabouts.

### **III. GOVERNMENT PROCEDURES FOR WARRANT EXECUTION**

The United States government will conduct a search of the information produced by the Provider and determine which information is within the scope of the information to be seized specified in Section II. The information that is within the scope of Section II may be copied and retained by the United States.

Law enforcement personnel will then seal any information from the Provider that does not fall within the scope of Section II and will not further review the information absent an order of the Court.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC  
BUSINESS RECORDS PURSUANT TO FEDERAL RULE  
OF EVIDENCE 902(11)**

I, \_\_\_\_\_, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Google and my official title is \_\_\_\_\_. I am a custodian of records for Google. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Google, and that I am the custodian of the attached records consisting of \_\_\_\_\_ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of Google; and
- c. such records were made by Google as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature