

UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

IN THE MATTER OF THE SEARCH
OF:

CASE NO. 8:23-mj-1544-SPF
FILED UNDER SEAL

Google Accts: [REDACTED]@gmail.com
associated with ID7607577673375;
[REDACTED]@burke-communications.com
associated with ID867030490921

ORDER

Before the Court is the *United States' Motion to Unseal Search Warrant Records* in the instant case, namely the (1) Search Warrant, (2) Application for Search warrant, (3) Motion to Seal Search Warrant and Related Records, (4) Order Regarding Motion to Seal Search Warrant Related Records (collectively, the "Search Warrant Records"), as well as the instant motion to unseal. Upon consideration, the Court grants the United States' motion and **ORDERS:**

1. The Search Warrant Records (with redactions) and the *United States' Motion to Unseal Search Warrant Records* are unsealed, and the Clerk is directed to file the documents in the public docket.
2. **IT IS FURTHER ORDERED** that the Search Warrant Records shall remain filed in their redacted format pending further order of the Court.

DONE AND ORDERED in chambers at Tampa, Florida, this 2nd day
of May 2024.



SEAN P. FLYNN
United States Magistrate Judge

Copies to: Jay G. Trezevant
Assistant United States Attorney

UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

MAY 2 2024 PM2:30
FILED - USDC - FLMD - TPA

IN THE MATTER OF THE SEARCH OF:

CASE NO. 8:23-mj-1544-SPF
FILED UNDER SEAL

Google Accts: [REDACTED]@gmail.com
associated with ID7607577673375;
[REDACTED]@burke-communications.com
associated with ID867030490921

**UNITED STATES' MOTION TO UNSEAL
SEARCH WARRANT RECORDS**

The United States of America, by Roger B. Handberg, United States Attorney for the Middle District of Florida, moves this court to unseal the search warrant records in this case, namely the (1) Search Warrant, (2) Application for Search warrant, (3) Motion to Seal Search Warrant and Related Records, (4) Order Regarding Motion to Seal Search Warrant Related Records (collectively, the "Search Warrant Records"), and (5) this motion. In support, the United States offers as follows:

1. On May 5, 2023, upon consideration of an application and supporting sworn affidavit, this Court found probable cause supported the United States' application for a warrant to search the above Google accounts for records and evidence relating to violations of 18 U.S.C. § 1030 (intentional unauthorized access of a computer), and 18 U.S.C. § 2511 (intentional interception and disclosure of wire, oral, or electronic communication), and issued the pertinent warrant.

2. The Search Warrant Records are presently maintained under seal pursuant to a Court Order, entered on November 30, 2023.

3. On February 15, 2024, a federal grand jury sitting in the Middle District of Florida returned a fourteen-count indictment against Timothy Burke, charging Burke in Count One with engaging in a conspiracy from in or around February 2022, and continuing through May 2023, in violation of 18 U.S.C. § 371; in Counts Two through Seven with intentionally accessing a protected computer without authorization, in violation of 18 U.S.C. § 1030(a)(2)(C); in Counts Eight through Twelve with intentional interception of a wire, oral, or electronic communication, in violation of 18 U.S.C. § 2511(1)(a); and in Counts Thirteen and Fourteen with intentionally disclosing an illegally intercepted wire, oral, or electronic communication, in violation of 18 U.S.C. § 2511(1)(c). *See United States v. Timothy Burke*, Case No. 8:24-cr-0068-KKM-TGW (the “Burke Case”). Burke Case, Doc. 1. The indictment also includes forfeiture allegations that identify, among other items, twenty items subject to forfeiture that were seized from Burke’s residence on May 8, 2023. *Id.*

4. On April 12, 2024, Marco Gaudino, who resides in Washington, was charged in a one-count information in Case No. 8:24-cr-165-CEH-SPF with engaging in a conspiracy with Burke from in or around February 2022, and continuing through May 2023, in violation of 18 U.S.C. § 371 (the “Gaudino

Case”). Gaudino Case, Doc. 1. Gaudino appeared in court on Monday, April 22, 2024, and pleaded guilty for his role in the charged conspiracy. Gaudino Case, Doc. 15.

5. The necessity for the present sealing of the Search Warrant Records no longer exists considering recent developments in this case. Notwithstanding, consistent with the relevant charging documents in the Burke Case and the Gaudino Case, certain narrowly tailored redactions to the Search Warrant Records are appropriate and should remain to protect personal identifying information, pursuant to Fed. R. Crim. P. 49.1 and other policy considerations, and/or to protect the identity and personal safety of a federal special agent or other law enforcement officer.

6. So that this Court can review and consider the United States’ proposed tailored redactions, the United States will submit to the Court *in camera* a copy of the sealed Search Warrant Records with the proposed redactions and a copy of the Search Warrant Records with the proposed redactions boxed in red ink.

7. Wherefore, the United States requests that this Court enter an Order unsealing the Search Warrant Records (with proposed redactions) and directing the clerk to file the Search Warrant Records in the public docket.

Dated this 2nd day of May, 2024.

Respectfully submitted,

ROGER B. HANDBERG
United States Attorney,

By: _____

Jay G. Trezevant
Assistant United States Attorney
Florida Bar No. 0802093
400 N. Tampa Street, Suite 3200
Tampa, Florida 33602-4798
Telephone: (813) 274-6000
Facsimile: (813) 274-6358
E-mail: jay.trezevant@usdoj.gov

Search Warrant Record #1
Search Warrant
(with redactions)

UNITED STATES DISTRICT COURT

for the
Middle District of Florida

In the Matter of the Search of)

(Briefly describe the property to be searched
or identify the person by name and address))Google Accts: [REDACTED]ke@gmail.com associated)
with ID 7607577673375;)tim@b [REDACTED]ns.com associated with ID)
867030490921)

Case No.

8:23 MJ 1544 SPF

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Middle District of Florida
(identify the person or describe the property to be searched and give its location):

See Attachment A.

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.

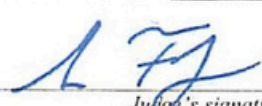
☒ YOU ARE COMMANDED to execute this warrant on or before 5/19/2023 (not to exceed 14 days)
☐ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

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 The Honorable Sean P. Flynn
(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: 5/5/2023 at 10:48 am
Judge's signatureCity and state: Tampa, FLSean P. Flynn, U.S. Magistrate Judge
Printed name and title

Return		
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(s) of any person(s) seized:		
Certification		
I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.		
Date: _____	_____ <i>Executing officer's signature</i>	
	_____ <i>Printed name and title</i>	

ATTACHMENT A
Property to be Searched

This warrant applies to information associated with Google LLC ("Google") account, that is stored at premises owned, maintained, controlled, or operated by Google, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

- t[REDACTED]ke@gmail.com, Google ID 760757673375; and
- tim@b[REDACTED]ns.com, Google ID 867030490921.

ATTACHMENT B
Particular Things to be Seized

I. Information to be disclosed by Google

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made on November 8, 2022 under 18 U.S.C. § 2703(f), which was renewed on January 30, 2023, Google is required to disclose the following information to the government for each account or identifier listed in Attachment A.

For the time period **August 1, 2022 to Present:**

A. The contents of all emails associated with the account including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email.

For the time period **January 1, 2021 to Present:**

A. All records or other information regarding the identification of the accounts, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the accounts were created, the length of service, the IP address used to register the accounts, log-in IP addresses associated with session times and dates, account status, alternative



email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

B. The types of service utilized;

C. All records or other information stored by an individual using the accounts, including address books, contact and buddy lists, calendar data, pictures, Google Drive contents, and files;

D. Google search history for the Target Accounts; and

E. All records pertaining to communications between Google and any person regarding the accounts, including contacts with support services and records of actions taken.

II. Information to be seized by the Government

All information described above in Section I that constitutes fruits, instrumentalities, and/or evidence of an intentional unauthorized access of a computer (in violation of 18 U.S.C. § 1030) and/or intentional interception and disclosure of wire, oral, or electronic communication (in violation of 18 U.S.C. § 2511) (collectively the “criminal conduct”), specifically:

From January 1, 2021 to the present, information pertaining to the following matters:

A. The identity of the person(s) who created or used the accounts, including records that help reveal the whereabouts of such person(s);

B. Evidence indicating how and when the accounts were accessed or used, including any emails, to determine the chronological and geographic context of



account access, use, and events relating to the criminal conduct and the account subscriber(s);

C. Evidence indicating the subscriber's state of mind as it relates to the criminal conduct; and

D. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

From August 1, 2022 to the present, information pertaining to the following matters:

A. Unauthorized network intrusion activity, including the exfiltration of stolen wire, oral, or electronic communication, or other data; and

B. Unauthorized disclosure of wire, oral, or electronic communication, or other data.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law-enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the Government and their support staff for their independent review.

Search Warrant Record #2
Search Warrant Application with
Probable Cause Affidavit
(with redactions)

UNITED STATES DISTRICT COURT

for the
Middle District of Florida

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

Google Accts: [REDACTED]ke@gmail.com associated with
ID 7607577673375; tim@b[REDACTED]ns.com
associated with ID 867030490921

Case No.

8:23MJ1544SPF

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

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.

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

See Attachment B.

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. § 1030	intentional unauthorized access of a computer
18 U.S.C. § 2511	intentional interception and disclosure of wire, oral, or electronic communication

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.

[REDACTED]
Applicant's signature

[REDACTED] Special Agent FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
Telephone (specify reliable electronic means).

Date: 5/5/2023

City and state: Tampa, FL

[Signature]
Judge's signature

Sean P. Flynn, U.S. Magistrate Judge
Printed name and title

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

I, [REDACTED], being duly sworn, depose and state the following:

AGENT BACKGROUND

1. I am employed as a Special Agent with the Federal Bureau of Investigation ("FBI") and have been employed in this capacity since June of 2015. I have been a member of sworn law enforcement since September of 2001. [REDACTED]
[REDACTED]
[REDACTED]

[REDACTED] I am currently assigned to the FBI Tampa field office in Tampa, Florida. In my capacity as a Special Agent, I have conducted a variety of national security and criminal investigations. I have investigated many different federal crimes including those involving national security, computer intrusions, intellectual property rights violations, mail and wire fraud, drugs, and violent crimes. Many of the crimes that I have investigated involved the use of email and social media to help perpetrate or further the crime. I have also assisted in the execution of numerous search warrants, including on electronic accounts, resulting in the seizure of paper, electronic, and other forms of evidence.

PURPOSE OF AFFIDAVIT

2. I make this affidavit in support of an application for a search warrant for information associated with Google LLC ("Google") accounts t [REDACTED] ke@gmail.com, associated with Google ID 760757673375, and

tim@b[REDACTED]s.com, associated with Google ID 867030490921 (the “Target Accounts”), that are stored at premises owned, maintained, controlled, or operated by Google, an electronic communications provider, headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

3. There is probable cause to believe that the Target Accounts, as described in Attachment A, contain the fruits, instrumentalities, and/or evidence of:

a. an intentional unauthorized access of a computer, in violation of 18 U.S.C. § 1030; and

b. an intentional interception and disclosure of wire, oral, or electronic communication, in violation of 18 U.S.C. § 2511. Said violations of federal law are collectively referred to in this affidavit as the “Target Offenses.”

Consequently, there is probable cause to search the Target Accounts for evidence of the Target Offenses.

STATUTORY AUTHORITY

4. 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) 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. 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) and (c)(1)(A). Specifically, the Court is a “district court of the United States (including a magistrate judge of such a court) . . . that—has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

5. Because this affidavit is provided for the limited purpose of establishing probable cause for the search warrant, I have not included all aspects of the investigation. Rather, this affidavit is intended to show merely that there is probable cause for the requested warrant. I am familiar with the following facts based upon my personal involvement in the investigation, as well as information I have obtained from other law-enforcement agencies and regulatory bodies and open-source materials including news reports and reports from civilian cybersecurity-research firms.

BACKGROUND ON TWITTER

6. Twitter owns and operates a social networking and microblogging service of the same name that can be accessed at <http://www.twitter.com> and via the Twitter mobile application (“app”). Generally, Twitter allows users to register and create an account; to personalize (if desired) an account profile page; and to send and receive communications via the platform. These functionalities are discussed in more detail below.

7. Twitter permits its users to communicate via messages that can contain photos, videos, links, and/or a maximum of 280 characters of text. Users can choose to share these messages, called “Tweets,” with the public or, alternatively, to “protect” their Tweets by making them viewable by only a preapproved list of

“followers.” Each Tweet includes a timestamp that displays when the Tweet was posted to Twitter. Users can also Tweet a copy of other Tweets (“retweet”) or Tweet a reply to another Tweet. Users can also indicate that they like a Tweet by clicking on a heart icon that appears next to each Tweet on the platform.

8. While individuals are not required to register with Twitter to view the content of unprotected Tweets, individuals must register for a Twitter account to send Tweets, to “follow” account in order to view protected Tweets, and to send and receive direct messages. A user may register for an account for free by visiting Twitter’s website or via the Twitter app. When a user creates a new Twitter account, Twitter assigns that account a unique User ID (“UID”). A user must also select a password as well as a unique Twitter username (also known as a “handle”). Twitter then appends the @ symbol in front of whatever username the user selects to create the Twitter username (for example: @example). The user may also select a different name (the “display name”), which is not automatically preceded by the @ symbol, to be displayed on his profile picture and at the top of his Tweets alongside his Twitter username. The display name can include symbols similar to emojis. The user can change the user’s password, username, and/or display name at any time, but the UID for the account will remain constant.

9. At the time of account creation, Twitter asks the user for certain identity and contact information, including: (1) name; (2) email address and/or telephone number; and (3) month and year of birth. Twitter also keeps certain information relating to the creation of each Twitter account, including: (1) the date

and time at which the user's account was created; and (2) the method of account creation (e.g., website or Twitter app).

10. Upon the creation of a Twitter account, a generic profile page is automatically created for the user. This page displays information, including: (1) the user's Twitter username; (2) the display name; (3) the number of Twitter accounts the user is following; (4) the number of Twitter accounts that are following the user; and (5) Tweets sent by the user (although, as noted above, if the user has chosen to protect their Tweets they will be visible only to preapproved "followers"). The user can personalize this page by posting a personal picture or image (known as an "avatar") to appear on the page and/or a banner image to appear across the top of the profile page. The user can also add text to create a short biography, to identify the user's location, to provide a link to the user's website, or to specify the user's date of birth.

11. As noted above, Twitter users can use their respective accounts to send and receive communications. If a Tweet includes a Twitter username that is preceded by the @ symbol, that is referred to as a "mention." The Twitter user mentioned in the Tweet will receive a notification informing the user that the user has been mentioned and showing the content of that Tweet. Similarly, if another Twitter user replies to a Tweet sent by a user, the user who sent the original Tweet will receive a notification that someone replied to that message, and the notification will show the content of that reply.

12. A registered Twitter user can also “like” a Tweet by clicking a heart icon on a Tweet sent by another user. If another user “likes” a Tweet that is posted by the Twitter user, a notification will appear in the user’s account identifying what Tweet was liked and who liked it.

13. Twitter users can also opt to Tweet with their location attached. This functionality is turned off by default, so Twitter users must opt-in to utilize it. However, if a Twitter user enables Twitter to access the user’s precise location information, the Twitter user will have the option of attaching the user’s location (e.g., the name of a city or neighborhood) to a Tweet at the time it is sent. If the user uses Twitter’s in-app camera to attach a photo or video to the Tweet while the functionality is enabled, the Tweet will include both the location label (e.g., the name of a city or neighborhood) of the user’s choice as well as the device’s precise location in the form of latitude-longitude coordinates. The user can turn this functionality off (thereby removing the user’s location from Tweets) at any time, and the user can delete the user’s past location data from Tweets that have already been sent.

14. A Twitter user may choose to “follow” another Twitter user. If a Twitter account is unprotected (i.e., privacy settings have not been enabled), the user can follow another user simply by clicking the “follow” button on the other user’s Twitter profile page. If a Twitter account is protected (i.e., privacy settings have been enabled), the user can follow another user by clicking the “follow” button and waiting for the other user to approve the request. Once an account is followed by a Twitter user, the Tweets posted by the account the user follows will appear in the

user's Twitter Home timeline. Every time a Twitter user follows another account, Twitter sends a notification to the account being followed to inform that account holder about the new follower. Each user's Twitter profile page includes a list of the people who are following that user and a list of people whom that user follows. Twitter users can "unfollow" other users whom they previously followed at any time. Twitter also provides users with a list of "Who to Follow," which includes a few recommendations of Twitter accounts that the user may find interesting based on the types of accounts that the user is already following and who those people follow.

15. Twitter collects and retains information about a user's use of the Twitter service, to include: (1) content of and metadata relating to Tweets and Direct Messages; (2) photos, images, and videos that are shared via Twitter and stored in the user's Media Timeline; (3) the identity of the accounts that a user follows and the accounts that follow the user's account; (4) the content uploaded to a user's profile page, including the user's avatar, banner image, and bio; (5) information about Tweets the account has liked; (6) information about Lists associated with the account; (7) information about the Spaces that a user has participated in, including the host of the Space, its start and end times, and information about other attendees; and (8) applications that are connected to the Twitter account. Twitter also collects and retains various other data about a user and the user's activity, including:

a. logs of Internet Protocol ("IP") addresses used to login to Twitter and the timestamp associated with such logins;

- b. transactional records reflecting, for example, when a user changed the user's display name or email address;
 - c. the identities of accounts that are blocked or muted by the user;
- and
- d. information relating to mobile devices and/or web browsers used to access the account, including a Twitter-generated identifier called a UUID that is unique to a given device.

16. Additionally, providers of electronic communications services and remote computing services often collect and retain user-agent information from their users. A user agent string identifies, among other information, the browser being used, its version number, and details about the computer system used, such as operating system and version. Using this information, the web server can provide content that is tailored to the computer user's browser and operating system.

17. In my training and experience, evidence of who was using a Twitter account and from where, and evidence related to criminal activity of the kind described above and below, may be found in the files and records described above. This evidence may establish 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.

18. Based on my training and experience, direct messages, photos, videos, and documents are often created and used in furtherance of criminal activity,

including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a Twitter account may provide direct evidence of the offenses under investigation and can also lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

19. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Twitter 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, subscriber information, messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geolocation, date, and time) may be evidence of who used or controlled the account at a relevant time. Similarly, device identifiers and IP addresses can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

20. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.*, information indicating a plan to commit a crime), or consciousness of guilt (*e.g.*, deleting account information in an effort to conceal evidence from law enforcement).

21. Other information connected to the use of an account may lead to the discovery of additional evidence. For example, accounts are often assigned or associated with additional identifiers such as account numbers, advertising IDs, cookies, and third-party platform subscriber identities. This information may help establish attribution, identify and link criminal activity across platforms, and reveal additional sources of evidence.

22. Therefore, Twitter's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Twitter. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

BACKGROUND ON GOOGLE

23. Google is a United States company that offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome, a free search engine called Google Search, a free video streaming site called YouTube, a free mapping service called Google Maps, and a free traffic tracking service called Waze. These services may offer additional capabilities when the user is logged into their Google Account.

24. In addition, Google offers an operating system (“OS”) for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers.

25. Signing up for a Google Account automatically generates an email address at the domain gmail.com. That email address will be the log-in username for access to the Google Account. Enterprises may also establish Google Accounts which allow users to access various Google features and can be accessed using an email address at the enterprise’s domain (e.g., employee[@]company.com).

26. Google advertises its services as “One Account. All of Google working for you.” Once logged into a Google Account, a user can connect to Google’s full suite of services offered to the general public, described in further detail below. In addition, Google keeps certain records indicating ownership and usage of the Google Account across services, described further after the description of services below.

- a. Google provides email services (called Gmail) to Google Accounts through email addresses at gmail.com or enterprise email addresses hosted by Google. Gmail can be accessed through a web browser or a mobile application. Additional email addresses (“recovery,” “secondary,” “forwarding,” or “alternate” email addresses) can be associated with the Google Account by the user. Google preserves emails associated with a Google Account indefinitely, unless the user deletes them.
- b. Google provides an address book for Google Accounts through Google Contacts. Google Contacts stores contacts the user affirmatively adds to the address book, as well as contacts the user has interacted with in Google products. Users can send messages to more than one contact at a time by manually creating a group within Google Contacts or communicate with an email distribution list called a Google Group.

Users have the option to sync their mobile phone or device address book so it is stored in Google Contacts. Google preserves contacts indefinitely, unless the user deletes them.

- c. Google provides an appointment book for Google Accounts through Google Calendar. Users can create events or RSVP to events created by others in Google Calendar. Google Calendar can be set to generate reminder emails or alarms about events or tasks, repeat events at specified intervals, track RSVPs, and auto-schedule appointments to complete periodic goals (like running three times a week). A single Google Account can set up multiple calendars. An entire calendar can be shared with other Google Accounts by the user or made public so anyone can access it. Users have the option to sync their mobile phone or device address book so it is stored in Google Calendar. Google preserves appointments indefinitely, unless the user deletes them.
- d. Google also provides online to-do lists and notepads for Google Accounts. Google Tasks allows users to assign themselves tasks to be completed at scheduled times and marked complete when done. Google Keep allows users to create notes or lists. These notes can be shared with other users to edit. Users can set notifications at particular dates and times for both tasks and notes. Google preserves tasks and notes indefinitely, unless the user deletes them.
- e. Google provides a number of direct messaging services accessible through a browser or mobile application, including Duo, Messages, Hangouts (Chat and Meet), and the now-retired Allo and Chat. These services enable real-time communications. Users can send and receive text messages, videos, photos, locations, links, and contacts from their Google Account using these services. Chat and Hangouts require or required the other user to also have a Google Account. Duo, Messages, and Allo do or did not. Google preserves messages sent through these services indefinitely, unless the user turns off the setting to save conversation history or deletes the message.
- f. Google Drive is a cloud storage service automatically created for each Google Account. Users can store an unlimited number of documents created by Google productivity applications like Google Docs (Google's word processor), Google Sheets (Google's spreadsheet program), Google Forms (Google's web form service), and Google Slides, (Google's presentation program). Users can also upload files to Google Drive, including photos, videos, PDFs, and text documents, until they hit the storage limit. Users can also set up their personal computer or

mobile phone to automatically back up files to their Google Drive Account. Each user gets 15 gigabytes of space for free on servers controlled by Google and may purchase more through a subscription plan called Google One. In addition, Google Drive allows users to share their stored files and documents with up to 100 people and grant those with access the ability to edit or comment. Google maintains a record of who made changes when to documents edited in Google productivity applications. Documents shared with a user are saved in their Google Drive in a folder called "Shared with me." Google preserves files stored in Google Drive indefinitely, unless the user deletes them.

- g. Android device users can also use Google Drive to backup certain data from their device. Android backups on Google Drive may include mobile application data, device settings, and file downloads.
- h. Google offers a cloud-based photo and video storage service called Google Photos. Users can share or receive photos and videos with others. Google Photos can be trained to recognize individuals, places, and objects in photos and videos and automatically tag them for easy retrieval via a search bar. Users have the option to sync their mobile phone or device photos to Google Photos. Google preserves files stored in Google Photos indefinitely, unless the user deletes them.
- i. Google offers a map service called Google Maps which can be searched for addresses or points of interest. Google Maps can provide users with turn-by-turn directions from one location to another using a range of transportation options (driving, biking, walking, etc.) and real-time traffic updates. Users can share their real-time location with others through Google Maps by using the Location Sharing feature. And users can find and plan an itinerary using Google Trips. A Google Account is not required to use Google Maps, but if users log into their Google Account while using Google Maps, they can save locations to their account, keep a history of their Google Maps searches, and create personalized maps using Google My Maps. Google stores Maps data indefinitely, unless the user deletes it.
- j. Google Location History is a feature which allows Google to track users' movements to help users obtain better results and recommendations on Google products. For example, when a user runs a search using Google for "restaurants," it will provide results for restaurants local to the user's location.

- k. A subsidiary of Google, Google Payment Corporation, provides Google Accounts an online payment service called Google Pay (previously Google Wallet), which stores credit cards and gift cards for users and allows them to send or receive payments for online and brick-and-mortar purchases. Users may delete some data associated with Google Pay transactions from their profile, but Google Payment Corporation retains some records for regulatory purposes.
- l. Google Accounts can buy electronic media, like books, movies, and music, and mobile applications from the Google Play Store. Google Play records can include records of whether a particular application has been or is currently installed on a device. Users cannot delete records of Google Play transactions without deleting their entire Google Account.
- m. Google offers a service called Google Voice through which a Google Account can be assigned a telephone number that can be used to make, record, and forward phone calls and send, receive, store, and forward SMS and MMS messages from a web browser, mobile phone, or landline. Google Voice also includes a voicemail service. Records are stored indefinitely, unless the user deletes them.
- n. Google offers a free web-browser service called Google Chrome which facilitates access to the Internet. Chrome retains a record of a user's browsing history and allows users to save favorite sites as bookmarks for easy access. If a user is logged into their Google Account on Chrome and has the appropriate settings enabled, their browsing history, bookmarks, and other browser settings may be saved to their Google Account.
- o. Google provides an automatic translation service called Google Translate where users can input text or a photograph of text in one language and receive a rough translation in another. If a logged-in Google Account uses Google Translate, the entered text and translated output may be preserved.
- p. Google offers a blogging platform for Google Accounts called Google Blogger, where users can upload blog posts, including photo and video content. Users can allow others to edit or share their blog posts or comment on their posts and control whether their blog is accessible through search engines or searches on Blogger. Blog content can be shared with other websites in real-time. Google maintains a record of Blogger activity with the account indefinitely, unless the user deletes it.

- q. Google Sites is a web-page creation tool offered by Google. It allows users to create a team-orientated site where multiple people can collaborate and share files.
- r. Google also offers a video platform called YouTube that offers Google Accounts the ability to upload videos and share them with others. Users can create a YouTube channel where they can upload videos, leave comments, and create playlists available to the public. Users can subscribe to the YouTube channels of others, search for videos, save favorite videos, like videos, share videos with others, and save videos to watch later. More than one user can share control of a YouTube channel. YouTube may keep track of a user's searches, watch history, likes, comments, and change history to posted videos.

27. Google integrates these various services to make it easier for Google Accounts to access the full suite of Google services. Users accessing their Google Account through their browser can toggle between Google Services via a toolbar displayed on the top of most Google service pages, including Gmail and Drive. Google Hangout, Meet, and Chat conversations pop up within the same browser window as Gmail. Attachments in Gmail are displayed with a button that allows the user to save the attachment directly to Google Drive. If someone shares a document with a Google Account user in Google Docs, the contact information for that individual will be saved in the user's Google Contacts. Google Voice voicemail transcripts and missed call notifications can be sent to a user's Gmail account. And if a user logs into their Google Account on the Chrome browser, for example to access their Gmail, their subsequent Chrome browser and Google Search activity may be associated with that Google Account, depending on user settings.

28. When individuals register with Google for a Google email account, Google assigns each user with a unique number called a "Google ID." This number

is used to link all Google services to which that user subscribes, including the Google Drive cloud storage service. Google asks users to provide certain PII, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

29. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures 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 by the Google Account, 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 Google's website or using a mobile application), details about the devices used to access the account, and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") address used to register the account and accept Google's terms of service, as well as 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 Google Account.

30. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a communication or file from their Google Account, it may continue to be

available on Google's servers for a certain period of time. This is particularly true for Google G Suite customers who use Google Vault.

31. Google collects and retains data about searches that users conduct within their own Google Account or using the Google Search service, including voice queries made to Google Assistant. Google also has the capacity to track the websites visited using its Google Chrome web browser service, applications used by Android users, and the use of Google applications by iPhone users. According to Google, this search, browsing, and application use history may be associated with a Google Account when the user is logged into their Google Account on the browser or device and certain global settings are enabled, such as Web & App Activity. Google also collects and retains data about the voice queries made to its artificial intelligence-powered virtual assistant, Google Assistant, on Android devices and associated it with the registered Google Account if certain global settings are enabled, such as Voice & Audio Activity tracking. Google maintains these records indefinitely, unless the user deletes them.

32. Google collects and retains data about the location at which Google Account services are accessed from any mobile device, as well as the periodic location of Android devices, regardless of service usage. This location data can derive from a range of sources, including GPS data, Wi-Fi access points, cell-site locations, geolocation of IP addresses, sensor data, user searches, and Bluetooth beacons within range of the device. According to Google, this location data may be associated with the Google Account signed-in or registered to the device when

Location Services are activated on the device and the user has enabled certain global settings for their Google Account, such as Location History or Web & App Activity tracking. The data retained may be both precision location data, like latitude and longitude coordinates derived from GPS, and inferential location data, such as the inference that a Google Account is in New York because it conducts a series of searches about places to eat in New York and directions from one New York location to another. Google maintains these records indefinitely, unless the user deletes it.

33. When an individual uses an Android device for the first time, they are prompted to register the device to a new or existing Google Account. Data about the use of the Android device is saved to the registered Google Account, including device characteristics such as the device serial number, model type/number, and international mobile equipment identity ("IMEI"). In addition, users may opt-in to Android device backups to Google cloud servers. Android device backups are not saved as a unique backup file. Rather, data from the device is associated with the registered Google Account and stored with similar data in the Google Account. For example, photos and videos on the device are backed up to Google Photos; contacts are backed up to Google Contacts; events and appointments are backed up to Google Calendar; and files and certain application data are backed up to Google Drive. Google maintains these records indefinitely, though users may delete Android backup files in the same manner as any other file associated with the relevant Google service.

34. Google also maintains records of the device characteristics of iPhones used to access Google services, including the make and model of the device. Depending on user settings, those records may be associated with the Google Account logged into the service in use on the device. Google maintains these records indefinitely, unless the user deletes them.

35. According to Google's Privacy & Terms website (available at <https://www.google.com/policies/technologies/cookies>) the company sends a "cookie" for a variety of purposes. Cookies allow the websites visited, such as Google.com or Gmail.com, to recognize the electronic device when it returns to the website later, and then tailor the user's online experience accordingly. Google's cookies, for example, record all of the Google accounts accessed from the same browser on an electronic device; information about those visits; and the user's preferences and other settings. This warrant requires Google to identify any other accounts accessed by the same device(s) that accessed the accounts described in Attachment A, including accounts linked by cookies, recovery email address, or telephone number.

36. In my training and experience, evidence of who was using a Google Account, and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, where, when, why, 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. This

can be true even if subscribers insert false information to conceal their identity; this information often nevertheless provides clues to their identity, location or illicit activities.

37. For example, the stored communications and files connected to a Google account may provide direct evidence of the offenses under investigation. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

38. In addition, the user's account activity, logs, stored electronic communications, location history, and other data retained by Google 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, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and

chronological context of access, use, and events relating to the crime under investigation.

39. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

40. Other information connected to a Google Account may lead to the discovery of additional evidence. For example, the identification of apps downloaded from the Google Play Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

41. Therefore, Google's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

STATEMENT OF PROBABLE CAUSE

42. Law Firm #1,¹ legal representation for a broadcast network ("NetworkCo"), contacted the United States Attorney's Office for the Middle District of Florida and the FBI in early November of 2022 to report an unlawful network intrusion incident, which had occurred on October 6, 2022.

43. On that date at approximately 4:30 p.m. EDT, a program host ("Host") for NetworkCo's news arm, NetworkCo News, conducted an interview ("the interview") of a celebrity ("Celebrity") in Los Angeles. As the interview was being recorded, it was being streamed from the onsite location to New York City via satellite. Backup streams of the interview content were transmitted using encrypted and proprietary software over the internet to NetworkCo servers in New York City by another company ("StreamCo"), a video contribution technology company hired by NetworkCo to provide live video technology and related services. Portions of this interview were later broadcast by NetworkCo News during a television program(s) aired on October 6 and 7, 2022.

44. On October 11, 2022, a different media company's website ("WebPub"), published unauthorized excerpts from the interview conducted on October 6, 2022. The article from WebPub was entitled, "Watch the Disturbing [Celebrity] Interview Clips That [NetworkCo News Host] Didn't Put on Air." The

¹ The identities of potential victims, witnesses, and third parties have been anonymized in this affidavit to protect their privacy and the integrity of the federal criminal investigation.

article included six links² to interview excerpts on YouTube, which had been edited from the original footage and never released by NetworkCo News to the public. Additionally, NetworkCo did not authorize release of any part(s) of the unaired interview.

45. As a result of this information leak, NetworkCo hired a digital forensics company ("DFCo") to investigate the incident. Through a digital forensic investigation, DFCo was able to determine that the interview had been intercepted by an unauthorized user during live transmission. The investigation by DFCo revealed the information contained below in paragraphs 46 through 50 of this affidavit.

46. Through open-source research, it was determined that StreamCo network user credentials and an associated password that had been designated to another broadcast network ("Network #2") were exposed on a radio-station website of a Network #2 radio affiliate located in Tennessee. Said credentials were exposed as early as January 16, 2022, and were found on the Internet Archive (The Way Back Machine).

47. Through review of StreamCo network logs, it was determined that IP address 47.197. 207.14 (the IP address) was logged into the StreamCo network using

² Articles and links are as follows: "Celebrity Vaccinated" at <https://www.youtube.com/watch?v=qVbmguP1oG8>, "Celebrity on Planned Parenthood" at <https://www.youtube.com/watch?v=qn6PTWBXmpU>, "Celebrity: 'We're no longer trauma drunk'" at <https://www.youtube.com/watch?v=jqwOb-cPyLE>, "Celebrity on Kwanzaa and Hannukah" at <https://www.youtube.com/watch?v=soGtt2OU8ms>, "Celebrity on Virgil" at <https://www.youtube.com/watch?v=sWOicUe7Qsk>, and "Celebrity on Energy Communities" at https://www.youtube.com/watch?v=0DgC8MJfC_8.

the Network #2 credentials contemporaneously with the stream of the interview and for the entire duration. The IP address was first observed on StreamCo network logs on August 22, 2022, and repeatedly thereafter until at least October 14, 2022.

48. Using open-source tools, it was determined that the IP address resolved to Tampa, Florida, and more specifically the residence of Timothy Burke and his spouse, who reside within the confines of the Middle District of Florida. DFCo discovered four web domains being hosted from the IP address, which included one web domain associated with Burke's spouse and the following three associated with Burke:

- burke-communications[.]com: This website for Burke's media consulting company resolves to 47.197.207.14, according to commercial domain lookup repositories. This is an active domain that was created on June 3, 2019, and is registered through a proxy registrar called Wild West Domains.
- ilovecitr[.]us: Burke's professional website, which provides prior work samples and links to his social media accounts, resolves to 47.197.207.14, according to commercial domain lookup repositories. This is an active domain that was created on November 30, 2012, and is registered through a proxy registrar called Wild West Domains.
- mocksession[.]com: This website, which focuses on making memes regarding sports and music, is owned and operated by Burke, and

resolves to 47.197.207.14, according to commercial domain lookup repositories. It was created on November 25, 2005, and is registered through a proxy registrar called Wild West Domains.

49. Burke is the former Director of Video Editing for a popular news website. Burke also previously worked for at least two other media outlets as an investigative journalist. While not presently working in the media as a news journalist, Burke maintains a presence by collecting video clips and information and disseminating them via the internet. Currently, Burke owns and operates Burke Communications, which is advertised on its website as a media consultation company.

50. The research by DFCo further revealed that a violator using the IP address entered StreamCo's restricted computer network environment using the Network #2 credentials without authorization. Once there, the violator had access to StreamCo's system of URL-based video feeds and, with that knowledge, could determine the non-public URL and the StreamCo specific identifier for NetworkCo, which would then have allowed the violator to contemporaneously intercept the live electronic video feed, eavesdropping on the conversation between the NetworkCo News Host and Celebrity without authorization. Investigation to date leads your affiant to believe that the violator then recorded the interview and disseminated the contents of the electronic communication without authorization.

51. All open-source information provided by DFCo was later confirmed to be accurate by the FBI investigative team.

Interview of StreamCo CTO and The StreamCo Network

52. On December 20, 2022, agents from FBI Tampa interviewed the Chief Technical Officer (CTO) for StreamCo. The CTO stated that he became aware of the unauthorized intrusion incident on October 13, 2022, when NetworkCo notified him of the leaked interview footage. NetworkCo requested that StreamCo provide all applicable network logs to assist in a forensic investigation. StreamCo provided all logs which were deemed by StreamCo to be relevant.

53. The CTO stated that the StreamCo network is a system that streams content from point to point on a non-public network. Clients who currently utilize the StreamCo network for streaming include many established, major media companies. The stream is sent from an origin, a transmission unit, on this occasion located in Los Angeles, CA, to a receiver at a different location, on this occasion located at NetworkCo Headquarters in New York City. Each unit has up to four channels, or "instances," each denoting a separate video camera. Each receiver is assigned a universal identifier unique to that receiver for use by StreamCo. The StreamCo network utilizes a Python³ Script to generate this StreamCo identifier as digits in a Uniform Resource Locator (URL), ultimately used to access and identify streamed content. In the StreamCo network, content is streamed via HLS⁴ streaming

³ Python is a computer programming language often used to build websites and software, automate tasks, and conduct data analysis. Python is a general-purpose language, meaning it can be used to create a variety of different programs and is not specialized for any specific problems.

⁴ HLS Streaming, also referred to as HTTP Streaming, was released by Apple in 2009 and is currently the most widely used format for streaming video content over the internet.

and via a separate stream over satellite to ensure redundancy. Live streams are encrypted from point to point; however, the HLS live streams pass through the StreamCo server while in transit, where they are decrypted in low resolution making it viewable for the purpose of quality management. The signal is then encrypted again and continues to the receiver at the final location where it is recorded and stored in normal high-resolution format.

54. The CTO said that due to an error in the application programming interface (the “application”) of the StreamCo network, it would have been possible to utilize developer tools embedded in the web browser to access a full list of StreamCo identifiers across the StreamCo network. If a user had a basic understanding of how the StreamCo identifiers were created by the Python Script, it would be possible for a user to link certain StreamCo identifiers to certain clients, allowing the individual to target and monitor streaming content over multiple StreamCo identifiers/clients. Once a user authenticated into the StreamCo network, due to another application error, that individual could potentially access any StreamCo identifiers, regardless to which client it belonged, without reentering user credentials. Additionally, if an individual knew both a StreamCo identifier and the format of the HLS stream query used by StreamCo (both of which were exposed by the aforementioned application errors), that individual would be able to create a URL to access any active StreamCo device through an HLS-compatible viewer without authenticating into the StreamCo network.

55. The CTO said that nobody by the name of Timothy Burke works at or has worked at StreamCo, nor did anyone by that name have authorization to access the StreamCo network or any content therein.

Interview of NetworkCo CTO

56. On November 30, 2022, agents from FBI Tampa interviewed the CTO for NetworkCo regarding the intrusion. The CTO stated that there were two unidentified IP addresses which accessed the live stream of the interview. One, an IPV6, was observed on the logs having accessed approximately the last 30 minutes of the interview. IP address 47.197.207.14 was the only unauthorized IP address which was logged on for the entirety of the interview stream.

57. The CTO stated that the interview streamed via satellite as its primary method. It also streamed via HLS through StreamCo. The satellite feed had multiple instances of loss of service or transmission. The leaked footage had no signs of these instances of lost signal, and therefore must have derived from the HLS stream. NetworkCo conducted an internal investigation into the source of the leaked footage and concluded that it was not possible that the footage had been leaked by a NetworkCo employee.

58. According to the CTO, Timothy Burke was not currently, nor had he ever been, an employee of NetworkCo. Likewise, Burke did not have permission to access and release the leaked interview footage.

Interview of Network #2 BEMS

59. On January 10, 2023, agents from FBI Tampa interviewed the Broadcast Engineer Maintenance Supervisor (BEMS) for Network #2. The BEMS stated that the credentials, [Network #2-Network]⁵-Demo, are used at Network #2 for demonstration purposes when reselling access to the StreamCo network to Network #2 affiliates, which is done via contract with StreamCo. These credentials are only authorized to be utilized by the Network #2 sales team.

60. The BEMS advised that Timothy Burke does not, nor has ever, worked for Network #2, nor did he have authorization to use the credentials to access the StreamCo network.

IP Address 47.197. 207.14

61. IP address 47.197. 207.14 resolved to Frontier Communications ("Frontier") using open-source tools. Records secured from Frontier during the ongoing investigation reveal that the subscriber of the IP address as of October 6, 2022, was Burke's spouse and that the subscriber's address was [REDACTED] Tampa, FL 33604.

62. A review of pertinent logs provided by StreamCo revealed that IP address 47.197. 207.14 was viewing content of the interview on and off throughout the interview duration. Log activity showed that 47.197. 207.14 was the only IP address which viewed all the aforementioned unlawfully intercepted and distributed

⁵ The term "Network #2-Network" is used pursuant to the effort throughout this affidavit to anonymize the identities of potential victims, witnesses, and third parties.

excerpts in their entirety, making it highly likely that the individual using that IP address was the individual who distributed the footage to WebPub.

Notwithstanding, a second IP address, [REDACTED], was observed in the logs as having viewed content on three occasions during the interview. However, only two of the unlawfully distributed excerpts were viewed by the user of that IP address, thereby confirming that the user or users at that address was/were not the person(s) who intercepted and distributed the six excerpts to WebPub.

63. A check of IP address [REDACTED] using open-source tools revealed that it resolved to Comcast Cable Services. Subscriber records obtained from Comcast further revealed that the account belonged to Person #2 at [REDACTED] Auburn, WA. The same subscriber records also show that an IPV4 address, 67.183.179.97, was simultaneously assigned to that account, and remained assigned so until at least February 7, 2023. Follow-up investigation supports the belief that at least two individuals reside at that location, Person #2 and Person #3. Records checks by NetworkCo, StreamCo, and Network #2 all show that neither Person #2 nor Person #3 were or are employees of the companies; and therefore, neither person was or is authorized to access the StreamCo network using said companies' passwords.

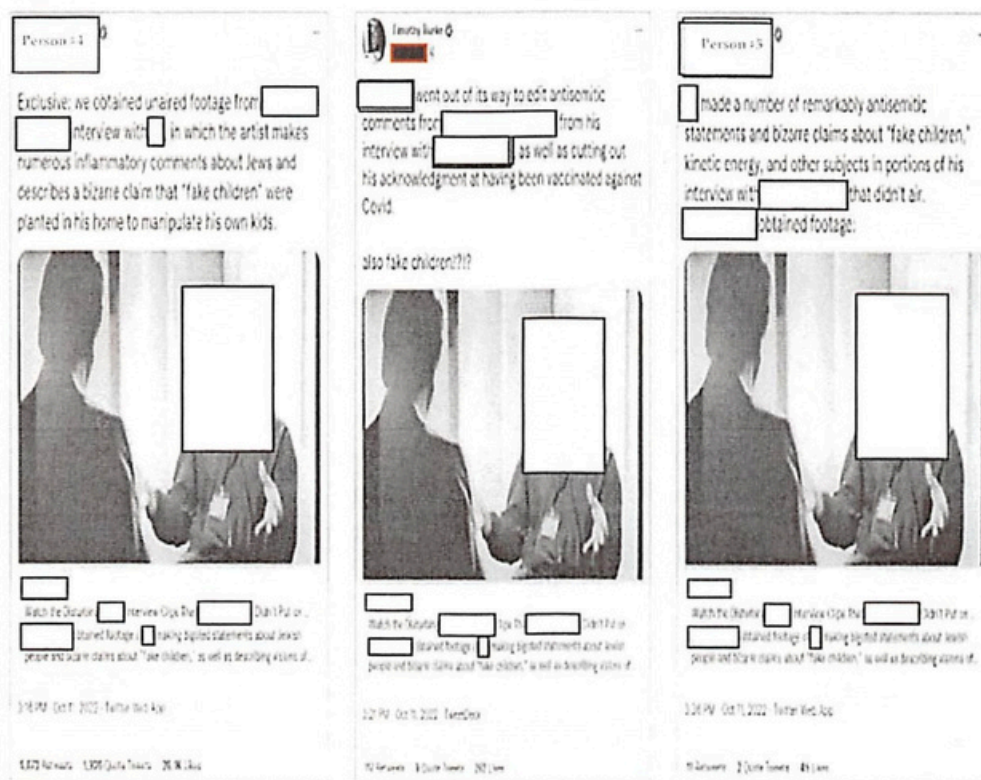
The Twitter Account

64. Investigators discovered relevant Twitter activity from Twitter account @b [REDACTED] og, which is linked to Timothy Burke via his website burke-communications.com.

65. Twitter subscriber records for @b [REDACTED] og reveal that the account was created on or about December 12, 2006, and is currently associated with email address t [REDACTED] ke@gmail.com. The account was logged into as recently as January 28, 2023, from IP address 47.197.207.14. The phone number associated with the account is a known telephone number associated with Burke.

66. The investigation has revealed that on October 11, 2022, at 3:16 p.m. EDT, Person #4, a WebPub reporter, tweeted a link to the above-mentioned article—"Watch the Disturbing [Celebrity] Interview Clips That [NetworkCo News Host] Didn't Put on Air"—which was the first appearance of the unaired interview excerpts in the media. The Tweet contained a comment plus a still photo extracted from one of the unauthorized aired interview excerpts. *Approximately 5 minutes later*, @b [REDACTED] og (Burke) tweeted the same still photo from the interview with a different comment. *Approximately thirty seconds following Burke's Tweet*, Person #4 retweeted Burke's Tweet. Finally, *on the same day approximately 15 minutes after Person #4's retweet*, a second WebPub representative, Person #5, tweeted the same still photo with different commentary. The interview photo in question was in low definition, with a reflection in the upper left corner of the screen. This leads investigators to

believe that the image was likely captured using a secondary recording device as the image was shown on a computer screen. The relevant Tweets are shown below:

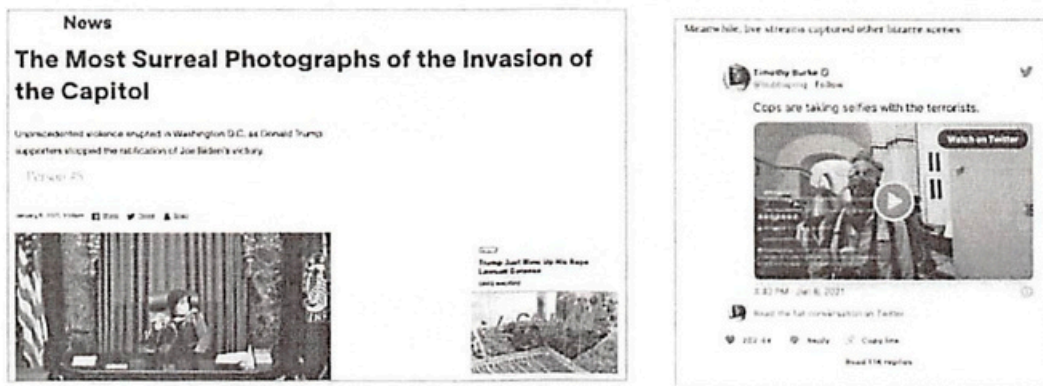


67. Review of LinkedIn profiles for Burke, Person #4, and Person #5 revealed that all three individuals were employed by a design, technology, and science website⁶ from January of 2018 through July of 2018.

68. Moreover, the three individuals have continued to associate with one another following their overlapping time at the common employer, in that: (1) Burke

⁶ The referenced website launched in 2002 and merged with another website in 2015, after which it began to post articles on subjects such as science fiction, fantasy, futurism, science, technology, and astronomy.

“follows” Person #4 and Person #5 on Twitter; and (2) Burke, Person #4, and Person #5 have publicly conversed using Tweets and replies. As a pertinent example, Person #5 posted an article on January 6, 2021, which was originally posted to Burke’s Twitter page. Notably, Burke’s post of the article occurred at 3:42 p.m. on that day, and Person #5’s article was published 14 minutes later, at 3:56 p.m.



69. Burke has demonstrated his knowledge concerning video streaming technology by posting multiple Tweets using @b [REDACTED] about different video feeds, resolution, aspect ratio, and other elements of videography, as well as specific information regarding the resolution and picture quality of NetworkCo streams. Burke has also posted multiple Tweets via @b [REDACTED] about having experience with StreamCo’s streaming, as well as having knowledge of NetworkCo’s streaming methods. For example, Burke posted a Tweet on December 22, 2021, about seeing “...high quality [StreamCo] signals every day...,” despite Burke having never worked for StreamCo and never having been authorized to access the StreamCo network. The referenced Tweet is included below.



70. Results of a search warrant served on Burke's Twitter account @b[REDACTED]og revealed direct message communications between @b[REDACTED]og and several other Twitter accounts from dates January 1, 2021 through February 15, 2023. One Twitter account, @E[REDACTED]es, had extensive communications with @b[REDACTED]og regarding what appears to be criminal activity. One such direct message related to the interception and later dissemination of the October 6 interview is listed below.

- August 22, 2022, 7:43:41 PM – @E[REDACTED]es to @b[REDACTED]og:
 “Oh, also [Network#2-Network]-demo [Network#2]news!!
<https://t.co/BW30vuhCoT>”

71. In the above direct message, the user of @E[REDACTED]es provided to Burke via @t[REDACTED]og the username and password for Network #2's compromised

⁷ Twitter uses shortened versions of URLs when sent in direct message. The actual URL was also provided by Twitter, which was [https://XXXXX.\[StreamCo\].tv](https://XXXXX.[StreamCo].tv). The lead portion of the URL contains proprietary information and has been redacted to protect the victim's identity.

login credentials into StreamCo's website. According to logs provided by StreamCo, IP address 67.183.179.97 logged onto StreamCo's website on August 22, 2022, at 19:43:04 UTC, approximately 37 seconds prior to the user of @E [REDACTED] es sending the credentials to Burke. Less than two minutes later, Burke, using IP address 47.197.207.14, logged onto StreamCo's website. This was the first time both IP addresses were observed in StreamCo's logs.

72. From August 22, 2022, through December 30, 2022, Burke (using @b [REDACTED] og) and the user of @E [REDACTED] es exchanged well over 400 direct messages discussing the structure of StreamCo's network, how to exploit flaws in that network's application, and interception and recording of content being streamed across the network. This intercepted content included, but was not limited to, the October 6 interview.

The Telephone Records

73. Review of domain burke-communications.com revealed Burke listed his telephone number as [REDACTED]. Using open-source tools, investigators determined that this number was serviced by T-Mobile.

74. Records from T-Mobile showed that, from October 10, 2022 through November 29, 2022, phone number [REDACTED] had incoming or outgoing calls with telephone number XXX-XXX-3112 on at least 10 occasions. There were no other contacts between these two numbers from January 1, 2022 through January 28, 2023.

75. Open-source research on telephone number XXX-XXX-3112 revealed it was associated with Person #5, an employee of WebPub. This telephone activity occurred contemporaneously with the release of the above discussed previously unaired video footage.

The Bank Account

76. Investigators discovered that Burke utilized Bank #1 for financial transactions. Records from Bank #1 revealed that Burke had two checking accounts there for which Burke was the sole signatory. One account was titled "TIMOTHY JOHN BURKE" while the other was titled "MOCKSESSION LLC DBA BURKE COMMUNICATIONS." On January 23, 2023, Burke received payment into the latter account from WebPub in the amount of \$1,500.00.

The Google Accounts

77. Review of the domains discussed in paragraph 48 revealed Burke's use of email address t[REDACTED]ke@gmail.com (one of the Target Accounts). Email header information for t[REDACTED]ke@gmail.com received from Google showed that, from October 10, 2022, through November 29, 2022, Burke used t[REDACTED]ke@gmail.com for approximately eight email exchanges with Person #5. Additionally, during the same period, email header information revealed three emails to t[REDACTED]ke@gmail.com involving the use of Adobesign and two emails involving the use of Formstack,⁸ with Person #5 carbon copied (CC'd). Use of

⁸ Adobesign and Formstack are software programs utilized for the purpose of sending, receiving, and electronically signing documents.

Adobesign and Formstack often occurred shortly after telephone contact between Burke and Person #5. Investigators found no other emails between Person #5 and Burke, outside of the above date range and using these accounts, from dates January 1, 2021, through February 13, 2023.

78. Records from Google also show that Burke has utilized the Google Drive cloud storage service associated with t[REDACTED]urke@gmail.com from the inception of the account to the present. As explained above, Google Drive is a cloud storage service provided by Google to its customers for storage of personal data and telephone content back-up.

79. Records obtained from Twitter revealed that Burke and the user of @E[REDACTED] shared files via Twitter direct messages using links to the Google Drive cloud storage service on at least 50 occasions from June 2021 through January 2023. On at least three of those occasions, Burke utilized a Google Drive associated with tim@b[REDACTED]ns.com (the second Target Account).

80. Moreover, in reference to the October 6 streamed interview, Burke (using @b[REDACTED]og) and the user of @E[REDACTED] exchanged Twitter direct messages and shared content via the Google Drive cloud storage service on October 7, 2022 (at 04:05 UTC and 04:13 UTC), October 8, 2022 (at 08:41 UTC), and October 11, 2022 (at 00:40 UTC). This file sharing occurred from the time and date that the October 6 interview was streamed and intercepted through the date the unauthorized interview content was released by WebPub. While it is not possible at this point to definitively conclude which Google account was utilized to share the

content, investigators believe, given the above, it is likely that one or both of the Target Accounts was used for those exchanges.

CONCLUSION

81. Based on the affiant's training and experience, and the facts as set forth in this affidavit, the affiant respectfully submits that there is probable cause to believe that the Target Accounts contain the fruits, instrumentalities, and/or evidence of the Target Offenses. For those reasons, the affiant requests that the Court issue the proposed search warrant. The government will execute the warrant by serving it on the Provider. Because the warrant will be served on the Provider, which will then compile the requested records at a time convenient to them, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

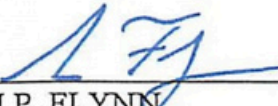
The affiant further requests that the Court order that all papers in support of the application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to the target of the investigation. Accordingly, there is

good cause to seal the documents because their premature disclosure may seriously jeopardize that investigation.

FURTHER AFFIANT SAYETH NAUGHT.


Special Agent 
Federal Bureau of Investigation

by telephone
Sworn to me this 5th day of May, 2023.


SEAN P. FLYNN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A
Property to be Searched

This warrant applies to information associated with Google LLC ("Google") account, that is stored at premises owned, maintained, controlled, or operated by Google, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

- t [REDACTED] ke@gmail.com, Google ID 760757673375; and
- tim@b [REDACTED] ns.com, Google ID 867030490921.

ATTACHMENT B
Particular Things to be Seized

I. Information to be disclosed by Google

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made on November 8, 2022 under 18 U.S.C. § 2703(f), which was renewed on January 30, 2023, Google is required to disclose the following information to the government for each account or identifier listed in Attachment A.

For the time period **August 1, 2022 to Present:**

A. The contents of all emails associated with the account including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email.

For the time period **January 1, 2021 to Present:**

A. All records or other information regarding the identification of the accounts, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the accounts were created, the length of service, the IP address used to register the accounts, log-in IP addresses associated with session times and dates, account status, alternative



email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

B. The types of service utilized;

C. All records or other information stored by an individual using the accounts, including address books, contact and buddy lists, calendar data, pictures, Google Drive contents, and files;

D. Google search history for the Target Accounts; and

E. All records pertaining to communications between Google and any person regarding the accounts, including contacts with support services and records of actions taken.

II. Information to be seized by the Government

All information described above in Section I that constitutes fruits, instrumentalities, and/or evidence of an intentional unauthorized access of a computer (in violation of 18 U.S.C. § 1030) and/or intentional interception and disclosure of wire, oral, or electronic communication (in violation of 18 U.S.C. § 2511) (collectively the “criminal conduct”), specifically:

From January 1, 2021 to the present, information pertaining to the following matters:

A. The identity of the person(s) who created or used the accounts, including records that help reveal the whereabouts of such person(s);

B. Evidence indicating how and when the accounts were accessed or used, including any emails, to determine the chronological and geographic context of



account access, use, and events relating to the criminal conduct and the account subscriber(s);

C. Evidence indicating the subscriber's state of mind as it relates to the criminal conduct; and

D. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

From August 1, 2022 to the present, information pertaining to the following matters:

A. Unauthorized network intrusion activity, including the exfiltration of stolen wire, oral, or electronic communication, or other data; and

B. Unauthorized disclosure of wire, oral, or electronic communication, or other data.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law-enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the Government and their support staff for their independent review.

Search Warrant Record #3
Motion to Seal Search Warrant
Related Records (with redactions)

UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

IN THE MATTER OF THE SEARCH OF:

Google Accts: t[REDACTED]ke@gmail.com

associated with ID7607577673375;

tim@b[REDACTED]ns.com

associated with ID867030490921

CASE NO. 8:23-mj-1544SPF

IN CAMERA

**MOTION TO SEAL APPLICATION FOR SEARCH WARRANT,
WARRANT AND AFFIDAVIT FOR SEARCH WARRANT**

The United States of America, by Roger B. Handberg, United States Attorney for the Middle District of Florida, respectfully moves this Court to seal the (1) Application for Search Warrant, (2) Warrant, (3) Affidavit for Search Warrant in this matter, and (4) this Motion to Seal, and in support thereof says as follows:

Disclosure of the contents of the affidavit may cause the subject(s) to destroy evidence, disclose facts that could jeopardize an ongoing criminal investigation, and cause witnesses named in the affidavit to be subject to possible harassment or retaliation from individuals who are the subjects of the investigation or who have an interest therein.

WHEREFORE, the United States respectfully moves the Court to seal
(1) Application for Search Warrant, (2) Warrant, (3) Affidavit for Search Warrant in
this matter, and (4) this Motion to Seal until May 4, 2024.

Respectfully submitted,

ROGER B. HANDBERG
United States Attorney

By:

Jay G. Trezevant
Assistant United States Attorney
Florida Bar No. 0802093
400 N. Tampa Street, Suite 3200
Tampa, Florida 33602-4798
Telephone: (813) 274-6000
Facsimile: (813) 274-6358
E-mail: jay.trezevant@usdoj.gov

Search Warrant Record #4
Order Regarding Motion to Seal Search Warrant
Related Records (with redactions)

UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

IN THE MATTER OF THE SEARCH OF:

Google Accts: t[REDACTED]ke@gmail.com

associated with ID7607577673375;

tim@b[REDACTED]ns.com

associated with ID867030490921

CASE NO. 8:23-mj-1544SPF

IN CAMERA ORDER

Upon the written motion of the United States of America to seal the

(1) Application for Search Warrant, (2) Warrant, (3) Affidavit for Search Warrant in this matter, and (4) Motion to Seal:

The Court finds that the interests of justice require that the Application for Search Warrant, Warrant, Affidavit for Search Warrant in this matter, and Motion be sealed; therefore

IT IS ORDERED that the Motion to Seal is Granted;

IT IS FURTHER ORDERED that the (1) Application for Search Warrant, (2) Warrant, (3) Affidavit for Search Warrant in this matter, and (4) Motion to Seal be sealed by the Clerk of the Court until May 4, 2024;

DONE AND ORDERED at TAMPA, Florida this 30th day of November, 2023.


SEAN P. FLYNN
United States Magistrate Judge

Copy to: AUSA Jay G. Trezevant