

UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

IN THE MATTER OF THE SEARCH
OF:

CASE NO. 8:23-mj-1150-TGW
FILED UNDER SEAL

Twitter Account: @b[REDACTED]og
located in San Francisco, CA

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, (5) Search Warrant Return (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 20th day of May 2024.



THOMAS G. WILSON
United States Magistrate Judge

Copies to: Jay G. Trezevant
Assistant United States Attorney

UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

MAY 20 2024 PM 12:09
FILED - USDC - FLMD - TPA

IN THE MATTER OF THE SEARCH OF:

CASE NO. 8:23-mj-1150-TGW
FILED UNDER SEAL

Twitter Account: @b[REDACTED]og
located in San Francisco, CA

**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 with narrowly tailored proposed redactions, 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, (5) Search Warrant Return (collectively, the "Search Warrant Records"), and (6) this motion. In support, the United States offers as follows:

1. On February 13, 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 Twitter account 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 February 13, 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 20th 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

UNITED STATES DISTRICT COURT

for the
Middle District of FloridaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)Twitter Account: @b[REDACTED]og
located in San Francisco, CA

Case No.

8:23MJ1150TGW

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.

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 February 24, 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 Thomas G. Wilson
(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:

Feb. 13, 2023 at 5:24 PM

S

Judge's signature

City and state:

Tampa, Florida

Thomas G. Wilson, 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 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: _____

*Executing officer's signature*_____
Printed name and title

ATTACHMENT A
Property to be Searched

This warrant applies to information associated with Twitter, Inc. ("Twitter") account, that is stored at premises owned, maintained, controlled, or operated by Twitter, a company headquartered at 1355 Market Street, Suite 900, San Francisco, California 94103:

@b [REDACTED] og (User ID: [REDACTED]) (account creation: December 12, 2006 23:53:15 UTC)

ATTACHMENT B
Particular Things to be Seized

I. Information to be disclosed by Twitter

To the extent that the information described in Attachment A is within the possession, custody, or control of Twitter, regardless of whether such information is located within or outside of the United States, and including any communications, records, files, logs, or information that has been deleted but is still available to Twitter, 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, Twitter is required to disclose to the government for the account or identifier listed in Attachment A for the time period **January 1, 2021 to present**:

A. All business records and subscriber information, in any form kept, pertaining to the account, including:

1. Identity and contact information (past and current), including full name, e-mail address, physical address, date of birth, phone number, gender, and other personal identifiers;
2. All usernames (past and current) and the date and time each username was active, all associated accounts (including those linked by machine cookie, IP address, email address, or any other account or device identifier), and all records or other information about connections with third-party websites and mobile apps (whether active, expired, or removed);

3. Length of service (including start date), types of services utilized, purchases, and means and sources of payment (including any credit card or bank account number) and billing records;

4. Devices used to login to or access the account, including all device identifiers, attributes, user agent strings, and information about networks and connections, cookies, operating systems, and apps and web browsers;

5. All advertising information, including advertising IDs, ad activity, and ad topic preferences;

6. Internet Protocol ("IP") addresses used to create, login, and use the account, including associated dates, times, and port numbers;

7. Privacy and account settings, including change history; and

8. Communications between Twitter and any person regarding the account, including contacts with support services and records of actions taken;

B. All content, records, and other information relating to communications sent from or received by the account, including but not limited to:

1. The content of all Tweets created, drafted, favorited/liked, or retweeted by the account, and all associated multimedia, metadata, and logs;

2. The content of all direct messages sent from, received by, stored in draft form in, or otherwise associated with the account, including all attachments, multimedia, header information, metadata, and logs;

C. All other content, records, and other information relating to all other interactions between the account and other Twitter users, including but not limited to:

1. All users the account has followed, unfollowed, muted, unmuted, blocked, or unblocked, and all users who have followed, unfollowed, muted, unmuted, blocked, or unblocked the account;

2. All information from the "Connect" or "Notifications" tab for the account, including all lists of Twitter users who have favorited or retweeted tweets posted by the account, as well as all tweets that include the username associated with the account (i.e., "mentions" or "replies");

3. All contacts and related sync information; and

4. All associated logs and metadata;

D. All other content, records, and other information relating to the use of the account, including but not limited to:

1. All data and information associated with the profile page, including photographs, "bios," and profile backgrounds and themes;

2. All multimedia uploaded to, or otherwise associated with, the account;

3. All records of searches performed by the account;

4. All location information, including all location data collected by any plugins, widgets, or the "Tweet With Location" service; and

5. All information about the account's use of Twitter's link service, including all longer website links that were shortened by the service, all resulting shortened links, and all information about the number of times that a link posted by the account was clicked.

Twitter is hereby ordered to disclose the above information to the Government within 14 days of issuance of this warrant.

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 account, including records that help reveal the whereabouts of such person(s);

B. Evidence indicating how and when the account was accessed or used, including any posted Tweets, to determine the chronological and geographic context of account access, use, and events relating to the criminal conduct and the account subscriber;

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.

UNITED STATES DISTRICT COURT

for the
Middle District of FloridaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)Twitter Account: @b[REDACTED]og
located in San Francisco, CA

Case No. 8:23MJ1150TGW

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.

located in the Northern District of California, 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	Fraud and related activity in connection with computers
18 U.S.C. § 2511	Interception and disclosure of wire, oral, or electronic communications

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

Printed name and title

Sworn to before me and signed in my presence.

Date: Feb. 13, 2023

City and state: Tampa, Florida

Judge's signature

Thomas G. Wilson, 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. Prior to becoming an FBI Special Agent, I served as [REDACTED]
[REDACTED], and as a [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 the Twitter, Inc. ("Twitter") account @b[REDACTED]g (the "Target Account"), that is stored at premises owned, maintained, controlled, or

operated by Twitter, a social media provider, headquartered at 1355 Market Street, Suite 900, San Francisco, California 94103.

3. There is probable cause to believe that the Target Account, as described in Attachment A, contains 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 Account 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 Twitter 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. Twitter also permits its users to exchange private messages, known as “direct messages” or “DMs,” with other Twitter users. DMs, which also may include photos, videos, links, and/or text that can only be viewed by the sender and designated recipient(s). Direct messages may be sent to an individual user or to a group of up to 50 Twitter users. Twitter users have the ability to choose whether they can receive a direct message from anyone. At any time, a Twitter user has the ability to alter the settings on the user’s Twitter account so that the user can receive direct messages only from: (1) individuals to whom the user has already sent a direct message, and (2) Twitter accounts that the user “follows” via his account.

9. 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” accounts 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.

10. While anyone can sign up and use Twitter for free, Twitter has also offered a subscription model since November 2021 that allows users access to additional features and app customizations. This new subscription is called Twitter Blue. A user can sign up for Twitter Blue at any time.

11. 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).

12. 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.

13. 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.

14. Twitter users can also include links to webpages in their Tweets and Direct Messages. Twitter automatically processes and shortens links provided by the user to a shortened link that starts <http://t.co/>. Twitter tracks how many times these shortened links are clicked.

15. 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.

16. As noted above, users can include photographs, images, and videos in their Tweets. Each account has a "media timeline" on its profile that displays the photos, videos, and image files in graphics interchange format (GIFs) the account

holder has uploaded via Tweets. An individual can view a Twitter user's media timeline by visiting the user's Twitter profile page.

17. 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.

18. 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.

19. A Twitter user can also "block" other Twitter users. This prevents the blocked account from contacting or following the user or from seeing the user's Tweets. Twitter does not notify the user of a blocked account when another Twitter account blocks that user.

20. A Twitter user can also use Twitter's integrated search function. When a user types a search term into Twitter's search tool, it will return results that include accounts, Tweets, and photos that match that search term. Twitter users using the service via the Twitter mobile app also have the option of saving searches that they have performed. A user can delete such saved searches at any time.

21. A Twitter user can also join or create "Lists" of other Twitter accounts. These Lists often organize Twitter accounts by group, topic, or interest. Viewing a timeline of a specific List will show you a stream of Tweets made only by accounts that are on that List. Users can pin their favorite lists to their Twitter Home timeline page. Twitter users have the ability to remove their accounts from Lists upon which they may appear.

22. Twitter also offers a functionality called “Spaces,” which it calls “a new way to have audio conversations on Twitter.” Any user can create a Space; that user is referred to as the “host.” Spaces are public, so anyone can join and listen to the conversation within a Space once it is created, although a user can send another Twitter user a link to the creating user’s Space and invite the receiving user to join. By default, the only individuals permitted to speak in a Space are the individuals that the host invites to do so, although this setting can be modified to allow a broader set of individuals to speak. Up to 13 people can be in a Space at a given time.

23. Twitter also offers the ability to sign into third-party apps and websites using one’s Twitter account. Typically, the third-party app or website will have a link that enables the user to sign into the third-party service using the user’s Twitter account. Doing so grants the third-party service access to the Twitter user’s account. Depending on the authorizations the Twitter user gives to the third-party service, the third-party service may be able to read the user’s Tweets, see who the user follows on Twitter, post Tweets to the user’s profile, or access the user’s email address. A user can revoke a third-party app or website’s authorization to access the user’s Twitter account and associated data at any time.

24. 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.

25. In some cases, Twitter users may communicate directly with Twitter about issues relating to their accounts, such as technical problems or complaints. Social networking providers like Twitter typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. Twitter may also suspend a particular user for

breaching Twitter's terms of service, during which time the Twitter user will be prevented from using Twitter's services.

26. 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.

27. 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.

28. 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.

29. 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.

30. 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).

31. 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.

32. 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.

STATEMENT OF PROBABLE CAUSE

33. 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 2022 to report an unlawful network intrusion incident, which had occurred on October 6, 2022.

34. On that date at approximately 4:30 p.m. EDT, a program host ("Host") for the 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

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.

interview were later broadcast by NetworkCo News during a television program(s) aired on October 6 and 7, 2022.

35. 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 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.

36. 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 37 through 41 of this affidavit.

37. Through open-source research, it was determined that StreamCo network user credentials and an associated password that had been designated to

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.

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).

38. 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 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.

39. 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.

40. 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.

41. 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.

42. 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

43. 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.

44. 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 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.

45. The CTO said that due to an error in the application programming interface (API) 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 API error, that individual could potentially access any StreamCo identifiers, regardless to which

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.

client it belonged, without reentering user credentials. Additionally, if an individual knew both a StreamCo identifier and the format of the HSL stream query used by StreamCo (both of which were exposed by the aforementioned API 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.

46. 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

47. 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.

48. 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.

49. 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

50. 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]⁷-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.

51. 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

52. 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,

⁷ 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.

2022, was Burke's spouse and that the subscriber's address was [REDACTED]

Tampa, FL 33604.

53. 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 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, 2601:601:ce7f:8d90:128:2341:74d7:3c07, 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.⁸

⁸ Open-source tools have revealed to investigators that IP address 2601:601:ce7f:8d90:128:2341:74d7:3c07 resolved to Comcast. Subscriber records obtained from Comcast further revealed that the account belonged to Person #2 at XXXX [REDACTED], Auburn, WA. Follow-up efforts support the belief that 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 individual who accessed the StreamCo network from said IP address and the purpose for that access is currently unknown and remains under investigation.

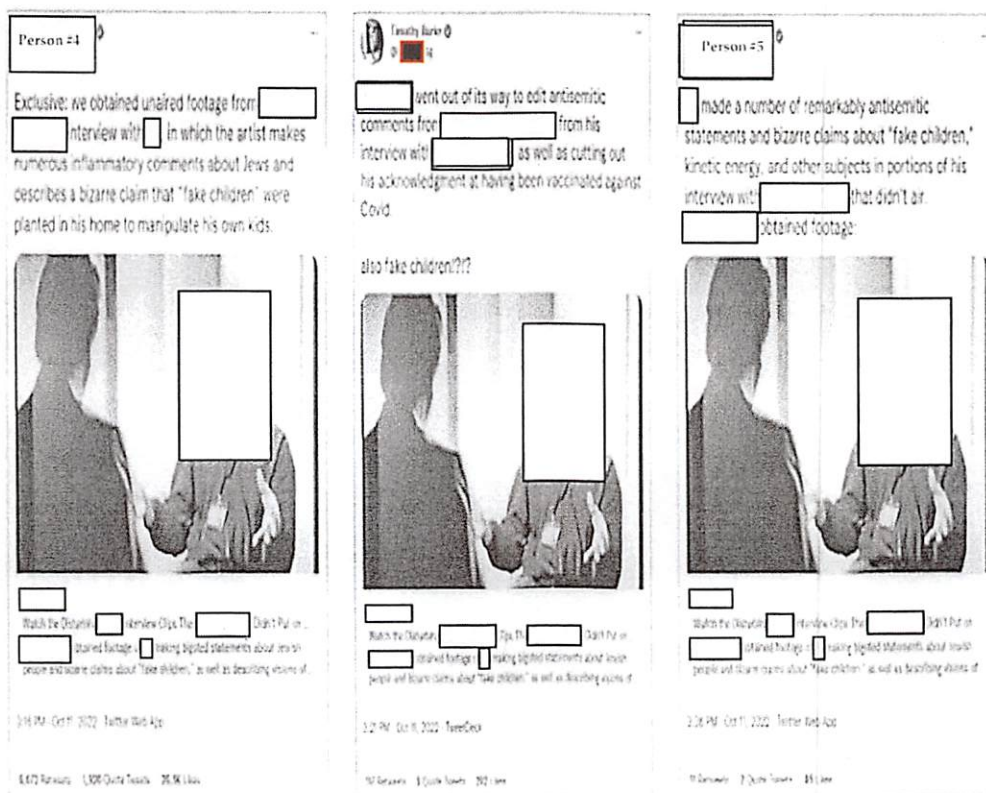
The Target Account

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

55. 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.

56. 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:



57. Review of LinkedIn profiles for Burke, Person #4, and Person #5 revealed that all three individuals were employed by a design, technology, and science website⁴ from January of 2018 through July of 2018.
58. Moreover, the three individuals have continued to associate with one another following their overlapping time at the common employer, in that: (1) Burke "follows" Person #4 and Person #5 on Twitter; and (2) Burke, Person #4, and

⁴ 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.

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.



59. Burke has demonstrated his knowledge concerning video streaming technology by posting multiple Tweets using @b[REDACTED]og 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]og 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.



60. As outlined above, activity on the Target Account is evidence related to the criminal activity under investigation and described in this affidavit, and the affiant believes that the Target Account will likely contain fruits, instrumentalities, and/or evidence of the Target Offenses. Specifically, the affiant believes that the Target Account will contain exchanges about the pertinent intentional unauthorized access of StreamCo's interview stream, as well as the intentional interception and disclosure of excerpts extracted from that stream.

CONCLUSION

61. 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 Account contains 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.

[REDACTED]

Special Agent [REDACTED]
Federal Bureau of Investigation

Sworn to me this 13th day of February, 2023.

Thomas G. Wilson

THOMAS G. WILSON
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A
Property to be Searched

This warrant applies to information associated with Twitter, Inc. ("Twitter") account, that is stored at premises owned, maintained, controlled, or operated by Twitter, a company headquartered at 1355 Market Street, Suite 900, San Francisco, California 94103:

@b[REDACTED]og (User ID: [REDACTED]) (account creation: December 12, 2006 23:53:15 UTC)

ATTACHMENT B
Particular Things to be Seized

I. Information to be disclosed by Twitter

To the extent that the information described in Attachment A is within the possession, custody, or control of Twitter, regardless of whether such information is located within or outside of the United States, and including any communications, records, files, logs, or information that has been deleted but is still available to Twitter, 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, Twitter is required to disclose to the government for the account or identifier listed in Attachment A for the time period **January 1, 2021 to present**:

A. All business records and subscriber information, in any form kept, pertaining to the account, including:

1. Identity and contact information (past and current), including full name, e-mail address, physical address, date of birth, phone number, gender, and other personal identifiers;
2. All usernames (past and current) and the date and time each username was active, all associated accounts (including those linked by machine cookie, IP address, email address, or any other account or device identifier), and all records or other information about connections with third-party websites and mobile apps (whether active, expired, or removed);

3. Length of service (including start date), types of services utilized, purchases, and means and sources of payment (including any credit card or bank account number) and billing records;

4. Devices used to login to or access the account, including all device identifiers, attributes, user agent strings, and information about networks and connections, cookies, operating systems, and apps and web browsers;

5. All advertising information, including advertising IDs, ad activity, and ad topic preferences;

6. Internet Protocol ("IP") addresses used to create, login, and use the account, including associated dates, times, and port numbers;

7. Privacy and account settings, including change history; and

8. Communications between Twitter and any person regarding the account, including contacts with support services and records of actions taken;

B. All content, records, and other information relating to communications sent from or received by the account, including but not limited to:

1. The content of all Tweets created, drafted, favorited/liked, or retweeted by the account, and all associated multimedia, metadata, and logs;

2. The content of all direct messages sent from, received by, stored in draft form in, or otherwise associated with the account, including all attachments, multimedia, header information, metadata, and logs;

C. All other content, records, and other information relating to all other interactions between the account and other Twitter users, including but not limited to:

1. All users the account has followed, unfollowed, muted, unmuted, blocked, or unblocked, and all users who have followed, unfollowed, muted, unmuted, blocked, or unblocked the account;

2. All information from the "Connect" or "Notifications" tab for the account, including all lists of Twitter users who have favorited or retweeted tweets posted by the account, as well as all tweets that include the username associated with the account (i.e., "mentions" or "replies");

3. All contacts and related sync information; and

4. All associated logs and metadata;

D. All other content, records, and other information relating to the use of the account, including but not limited to:

1. All data and information associated with the profile page, including photographs, "bios," and profile backgrounds and themes;

2. All multimedia uploaded to, or otherwise associated with, the account;

3. All records of searches performed by the account;

4. All location information, including all location data collected by any plugins, widgets, or the "Tweet With Location" service; and

5. All information about the account's use of Twitter's link service, including all longer website links that were shortened by the service, all resulting shortened links, and all information about the number of times that a link posted by the account was clicked.

Twitter is hereby ordered to disclose the above information to the Government within 14 days of issuance of this warrant.

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 account, including records that help reveal the whereabouts of such person(s);

B. Evidence indicating how and when the account was accessed or used, including any posted Tweets, to determine the chronological and geographic context of account access, use, and events relating to the criminal conduct and the account subscriber;

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.

UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

IN THE MATTER OF THE SEARCH OF:

CASE NO.

TWITTER ACCOUNT: @B [REDACTED] OG
LOCATED IN SAN FRANCISCO, CA

8:23MJ1150TGW

IN CAMERA

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

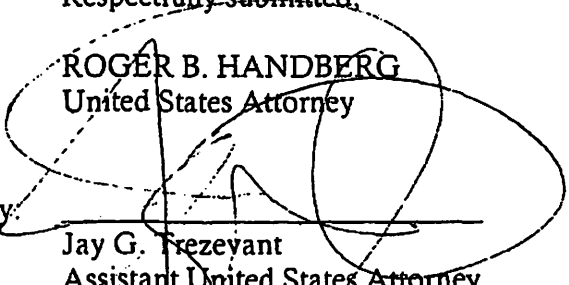
The United States of America, by Roger B. Handberg, United States Attorney for the Middle District of Florida, respectfully moves this Court to seal the (1) Application for Search Warrant, (2) Warrant, (3) Affidavit for Search Warrant in this matter, and (4) this Motion to Seal, and in support thereof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

Disclosure of the contents of the affidavit may cause the subjects to flee, 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 further order of the Court.

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

UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

IN THE MATTER OF THE SEARCH OF:

CASE NO.

TWITTER ACCOUNT: @B [REDACTED] OG
LOCATED IN SAN FRANCISCO, CA

8:23MJ1150TGW

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 further order of the Court;

DONE AND ORDERED at TAMPA, Florida this 13th day of February,
2023.



THOMAS G. WILSON
United States Magistrate Judge

Copy to: AUSA Jay G. Trezevant

UNITED STATES DISTRICT COURT

for the
Middle District of FloridaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)Twitter Account: @b[REDACTED]og
located in San Francisco, CA

Case No.

8:23MJ1150TGW
8:23MJ1150TGW

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.

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 February 24, 2023 (not to exceed 14 days)
☒ in the daytime 6:00 a.m. to 10:00 p.m. TH ☒ 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 Thomas G. Wilson
(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: Feb. 13, 2023 at 5:24 pmThomas G. Wilson
Judge's signatureCity and state: Tampa, FloridaThomas G. Wilson, U.S. Magistrate Judge
Printed name and title

Return

Case No.: 8:23 MT 1150 TGW	Date and time warrant executed: Downloaded 3/29/2023	Copy of warrant and inventory left with: Twitter LE Portal
-------------------------------	---	---

Inventory made in the presence of:

N/A

Inventory of the property taken and name of any person(s) seized:

ACCOUNT INFORMATION FROM TWITTER AS DESCRIBED IN ATTACHMENT B.

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: 4/4/2023

Executing officer's signature_____
SPECIAL AGENT FBI
Printed name and title

ATTACHMENT A
Property to be Searched

This warrant applies to information associated with Twitter, Inc. ("Twitter") account, that is stored at premises owned, maintained, controlled, or operated by Twitter, a company headquartered at 1355 Market Street, Suite 900, San Francisco, California 94103:

@b [REDACTED] .org (User ID: [REDACTED]) (account creation: December 12, 2006 23:53:15 UTC)

ATTACHMENT B
Particular Things to be Seized

I. Information to be disclosed by Twitter

To the extent that the information described in Attachment A is within the possession, custody, or control of Twitter, regardless of whether such information is located within or outside of the United States, and including any communications, records, files, logs, or information that has been deleted but is still available to Twitter, 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, Twitter is required to disclose to the government for the account or identifier listed in Attachment A for the time period **January 1, 2021 to present**:

A. All business records and subscriber information, in any form kept, pertaining to the account, including:

1. Identity and contact information (past and current), including full name, e-mail address, physical address, date of birth, phone number, gender, and other personal identifiers;

2. All usernames (past and current) and the date and time each username was active, all associated accounts (including those linked by machine cookie, IP address, email address, or any other account or device identifier), and all records or other information about connections with third-party websites and mobile apps (whether active, expired, or removed);

3. Length of service (including start date), types of services utilized, purchases, and means and sources of payment (including any credit card or bank account number) and billing records;

4. Devices used to login to or access the account, including all device identifiers, attributes, user agent strings, and information about networks and connections, cookies, operating systems, and apps and web browsers;

5. All advertising information, including advertising IDs, ad activity, and ad topic preferences;

6. Internet Protocol ("IP") addresses used to create, login, and use the account, including associated dates, times, and port numbers;

7. Privacy and account settings, including change history; and

8. Communications between Twitter and any person regarding the account, including contacts with support services and records of actions taken;

B. All content, records, and other information relating to communications sent from or received by the account, including but not limited to:

1. The content of all Tweets created, drafted, favorited/liked, or retweeted by the account, and all associated multimedia, metadata, and logs;

2. The content of all direct messages sent from, received by, stored in draft form in, or otherwise associated with the account, including all attachments, multimedia, header information, metadata, and logs;

C. All other content, records, and other information relating to all other interactions between the account and other Twitter users, including but not limited to:

1. All users the account has followed, unfollowed, muted, unmuted, blocked, or unblocked, and all users who have followed, unfollowed, muted, unmuted, blocked, or unblocked the account;

2. All information from the "Connect" or "Notifications" tab for the account, including all lists of Twitter users who have favorited or retweeted tweets posted by the account, as well as all tweets that include the username associated with the account (i.e., "mentions" or "replies");

3. All contacts and related sync information; and

4. All associated logs and metadata;

D. All other content, records, and other information relating to the use of the account, including but not limited to:

1. All data and information associated with the profile page, including photographs, "bios," and profile backgrounds and themes;

2. All multimedia uploaded to, or otherwise associated with, the account;

3. All records of searches performed by the account;

4. All location information, including all location data collected by any plugins, widgets, or the "Tweet With Location" service; and

5. All information about the account's use of Twitter's link service, including all longer website links that were shortened by the service, all resulting shortened links, and all information about the number of times that a link posted by the account was clicked.

Twitter is hereby ordered to disclose the above information to the Government within 14 days of issuance of this warrant.

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 account, including records that help reveal the whereabouts of such person(s);

B. Evidence indicating how and when the account was accessed or used, including any posted Tweets, to determine the chronological and geographic context of account access, use, and events relating to the criminal conduct and the account subscriber;

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.