UNITED STATES DISTRICT COURT

for the

District of Columbia

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* INFORMATION ASSOCIATED WITH ONE ACCOUNT STORED AT PREMISES CONTROLLED BY FACEBOOK, INC. PURSUANT TO 18 U.S.C. 2703 FOR INVESTIGATION OF VIOLATION OF 18 U.S.C. § 1512	Case No. 21-sc-446

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 incorporated herein and included as part of this Application for a Search Warrant

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

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

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

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

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1512(c)	Obstruction of Justice
18 U.S.C. § 1752	Unlawful Entry on Restricted Buildings or Grounds
40 U.S.C. § 5104(e)	Unlawful activities [Capitol Grounds]

The application is based on these facts:

See attached affidavit in support of search warrant

- ☐ 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

Matthew Gano, 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: 02/09/2021

Judge's signature

City and state: Washington, DC

Zia M. Faruqui, U.S. Magistrate Judge

Printed name and title

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means ❒ Original ❒ Duplicate Original

UNITED STATES DISTRICT COURT

for the

District of Columbia

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* INFORMATION ASSOCIATED WITH ONE ACCOUNT STORED AT PREMISES CONTROLLED BY FACEBOOK, INC. PURSUANT TO 18 U.S.C. 2703 FOR INVESTIGATION OF VIOLATION OF 18 U.S.C. § 1512	)	Case No. 21-sc-446

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 Northern District of California *(identify the person or describe the property to be searched and give its location)*:

See Attachment A (incorporated by reference)

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

See Attachment B (incorporated by reference)

YOU ARE COMMANDED to execute this warrant on or before February 23, 2021 *(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 Zia M. Faruqui, U.S. Magistrate Judge .
(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: 02/09/2021

Judge's signature

City and state: Washington, DC ZIA M. FARUQUI, U.S. MAGISTRATE JUDGE

Printed name and title

Return

Case No.: 21-sc-446	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: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A
Property to Be Searched

This warrant applies to information which is associated with the Facebook, Inc. account identified by subscriber Josiah Colt with user ID 100005928300442 and which is stored at premises owned, maintained, controlled, or operated by Facebook, Inc., a company that accepts service of legal process at 1601 Willow Road, Menlo Park, California.

ATTACHMENT B

Particular Things to be Seized and Procedures to Facilitate Execution of the Warrant

I. Information to be disclosed by Facebook, Inc. ("PROVIDER") to facilitate execution of the warrant

To the extent that the information described in Attachment A is within the possession, custody, or control of PROVIDER, including any records that have been deleted but are still available to PROVIDER, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), PROVIDER is required to disclose the following information to the government corresponding to each account or identifier ("Account") listed in Attachment A:

a. For the time period November 1, 2020, to the present: The contents of any available messages or other communication associated with the Account (including, but not limited to, messages, attachments, draft messages, posts, chats, video calling history, "friend" requests, discussions, recordings, images, or communications of any kind sent to and from the Account, including stored or preserved copies thereof) and related transactional records for all PROVIDER services used by an Account subscriber/user, including the source and destination addresses and all Internet Protocol ("IP") addresses associated with each message or other communication, the date and time at which each message or other communication was sent, and the size and length of each message or other communication;

b. For the time period November 1, 2020, to the present: All photos and videos uploaded by the Account and all photos or videos uploaded in which the Account has been "tagged", including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos;

c. Basic subscriber records and login history, including all records or other information regarding the identification of the Account, to include full name, physical address, telephone numbers, birthdate, security questions and passwords, and other personal identifying information, records of session times and durations, the date on which the Account was created, the length of service, types of services utilized by the Account, the IP address used to register the Account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, means and source of payment (including any credit or bank account number), and any account(s) linked by machine cookies (meaning all Facebook user identification numbers ("user IDs") that logged into Facebook by the same machine as the Account;

d. For the time period November 1, 2020, to the present: All records or other information related to the Account, including address books, contact and "friend" lists, calendar data, and files; profile information; "News Feed" information; "Wall" postings; Notes; groups and networks of which the Account is a member; future and past event postings; rejected "friend" requests and blocked users; status updates (including relationship status updates); comments; gifts; "pokes"; "tags"; the account's usage of the "like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked"; searches performed by the Account; privacy settings, including privacy settings for individual Facebook posts and activities; information about the Account's access and use of Facebook applications; and the Account's access and use of Facebook Marketplace;

e. For the time period November 1, 2020, to the present: All "check ins" and other location information;

f. For the time period November 1, 2020, to the present: All records pertaining to communications between PROVIDER and any person regarding the Account, including contacts with support services and records of actions taken;

g. All records pertaining to devices associated with the Account and software used to create and access the Account, including device serial numbers, instrument numbers, model types/numbers, International Mobile Equipment Identities ("IMEI"), Mobile Equipment Identifiers ("MEID"), Global Unique Identifiers ("GUID"), Electronic Serial Numbers ("ESN"), Android Device IDs, phone numbers, Media Access Control ("MAC") addresses, operating system information, browser information, mobile network information, information regarding cookies and similar technologies, and any other unique identifiers that would assist in identifying any such device(s), including unique application numbers and push notification tokens associated with the Account (including Apple Push Notifications ("APN"), Google Cloud Messaging ("GCM"), Microsoft Push Notification Service ("MPNS"), Windows Push Notification Service ("WNS"), Amazon Device Messaging ("ADM"), Firebase Cloud Messaging ("FCM"), and Baidu Cloud Push);

h. From the time period December 30, 2021, to February 1, 2021: All information held by PROVIDER related to the location and location history of the user(s) of the Account, including geographic locations associated with the Account (including those collected for non-PROVIDER based applications), IP addresses, Global Positioning System ("GPS") information, and information pertaining to nearby devices, Wi-Fi access points, and cell towers; and

i. Information about any complaint, alert, or other indication of malware, fraud, or terms of service violation related to the Account or associated user(s), including any memoranda, correspondence, investigation files, or records of meetings or discussions about the Account or associated user(s) (but not including confidential

j. with legal counsel).

Within 14 DAYS of the issuance of this warrant, PROVIDER shall deliver the information set forth above via United States mail, courier, or e-mail to the following:

Special Agent Matthew Gano
FBI – Washington Field Office
601 4th Street NW
Washington D.C. 20535
202-233-1438
mjgano@fbi.gov

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of 18 U.S.C. §§ 1512(c), 1752, and 40 U.S.C. § 5104(e), as described in the affidavit submitted in support of this Warrant, including, for each Account, information pertaining to the following matters:

(a) Information that constitutes evidence of the identification or location of the user(s) of the Account;

(b) Information that constitutes evidence concerning persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation; or (ii) communicated with the Account about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts;

(c) Information that constitutes evidence indicating the Account user's state of mind, *e.g.*, intent, absence of mistake, or evidence indicating preparation or planning, related to the criminal activity under investigation;

(d) Information that constitutes evidence concerning how and when the Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the Account user;

(e) Information that constitutes evidence concerning organization, planning, or travel to the U.S. Capitol on or preceding January 6, 2021;

(f) Membership in the "Boogaloo Bois or participation in activities associated the "Boogaloo Bois" or "Boogaloo Boys";

(g) Communications with Nate DeGrave, Ronnie Sandlin or any other person who traveled to D.C. for participation in protests or demonstrations on January 5, 2021, or January 6, 2021; and

(h) Information that constitutes evidence that Josiah Colt or any other person participated in the riots at the Capitol on January 6, 2021, or any demonstration held in Washington, D.C., in advance of the riots.

III. Government procedures for warrant execution

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

Law enforcement personnel will then seal any information from the PROVIDER that does not fall within the scope of Section II and will not further review the information absent an order of the Court. Such sealed information may include retaining a digital copy of all information received pursuant to the warrant to be used for authentication at trial, as needed.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH ONE ACCOUNT STORED AT PREMISES CONTROLLED BY FACEBOOK, INC. PURSUANT TO 18 U.S.C. 2703 FOR INVESTIGATION OF VIOLATION OF 18 U.S.C. § 1512	**SC No. 21-sc-446** **Filed Under Seal**

Reference: ***USAO Ref. # 2021R00278; Subject Account(s):*** **Josiah Colt, ID 100005928300442**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Matthew Gano, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information which is associated with one target account – that is, for Josiah Colt, ID 100005928300442 – which is stored at premises controlled by Facebook, Inc. ("PROVIDER"), an electronic communications services provider and/or remote computing services provider which is headquartered at / which accepts service at 1601 Willow Road, Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require PROVIDER to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B, using the procedures described in Section III of Attachment B.

2. I am a special agent with the Federal Bureau of Investigation (FBI). I have been in this position since July, 2017. I am assisting in the investigation of the insurrection at the United States Capitol on January 6, 2021.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that violations of 18 U.S.C. §§ 1512(c), 1752, and 40 U.S.C. § 5014(e) have been committed by Josiah Colt. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband or fruits of these crimes further described in Attachment B.

JURISDICTION

5. 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 . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). As discussed more fully below, acts or omissions in furtherance of the offenses under investigation occurred within Washington, DC. *See* 18 U.S.C. § 3237.

PROBABLE CAUSE

The 2020 United States Presidential Election and the Proceedings of January 6, 2021

6. The 2020 United States Presidential Election occurred on November 3, 2020.

7. The United States Electoral College is a group required by the Constitution to form every four years for the sole purpose of electing the president and vice president, with each state appointing its own electors in a number equal to the size of that state's Congressional delegation.

8. On December 14, 2020, the presidential electors of the U.S. Electoral College met in the state capital of each state and in the District of Columbia and formalized the result of the 2020 U.S. Presidential Election: Joseph R. Biden Jr. and Kamala D. Harris were declared to have won the sufficient votes to be elected the next president and vice president of the United States.

9. On January 6, 2021, a Joint Session of the United States House of Representatives and the United States Senate convened in the United States Capitol building ("the Capitol") to certify the vote of the Electoral College of the 2020 U.S. Presidential Election ("Electoral College vote").

The Incursion at the United States Capitol on January 6, 2021

10. The United States Capitol is secured 24 hours a day by United States Capitol Police ("Capitol Police"). The Capitol Police maintain permanent and temporary barriers to restrict access to the Capitol exterior, and only authorized individuals with appropriate identification are allowed inside the Capitol building.

11. The entire Capitol complex—including the Capitol building, the Capitol Visitor Center, and Capitol grounds to include the entire exterior plaza—was barricaded and off limits to the public on January 6, 2021.

12. On January 6, 2021, at approximately 1:00 p.m., the Joint Session convened in the Capitol building to certify the Electoral College vote. Vice President Michael R. Pence, in his constitutional duty as President of the Senate, presided over the Joint Session. Vice-President-

Elect Kamala D. Harris, in her role as a Senator representing the State of California, was also present.

13. A large crowd began to gather outside the Capitol perimeter as the Joint Session got underway. Crowd members eventually forced their way through, up, and over Capitol Police barricades and advanced to the building's exterior façade. Capitol Police officers attempted to maintain order and stop the crowd from entering the Capitol building, to which the doors and windows were locked or otherwise secured. Nonetheless, shortly after 2:00 p.m., crowd members forced entry into the Capitol building by breaking windows, ramming open doors, and assaulting Capitol Police officers. Other crowd members encouraged and otherwise assisted the forced entry. The crowd was not lawfully authorized to enter or remain inside the Capitol, and no crowd member submitted to security screenings or weapons checks by Capitol Police or other security officials.

14. Shortly thereafter, at approximately 2:20 p.m., members of the House and Senate (including Vice President Pence and Vice-President Elect Harris)—who had withdrawn to separate chambers to resolve an objection—were evacuated from their respective chambers. The Joint Session and the entire official proceeding of the Congress was halted while Capitol Police and other law enforcement officers worked to restore order and clear the Capitol of the unlawful occupants.

15. Later that night, law enforcement regained control of the Capitol. At approximately 8:00 p.m., the Joint Session reconvened, presided over by Vice President Pence, and attended by Vice-President-Elect Harris, both of whom had remained within the Capitol building throughout these events.

16. In the course of these events, approximately 81 members of the Capitol Police and 58 members of the Metropolitan Police Department were assaulted. Additionally, one subject was

shot and killed while attempting to enter the House chamber through broken windows; many media members were assaulted and had cameras and other news gathering equipment destroyed; and the Capitol suffered millions of dollars in damage—including broken windows and doors, graffiti, and residue of various pepper sprays, tear gas, and fire extinguishers deployed both by crowd members who stormed the Capitol and by Capitol Police officers trying to restore order.

17. Based on information I have reviewed, I estimate that between 2:00 p.m., and no later than 4:00 p.m., the defendant, Josiah Colt, entered the United States Capitol without authorization to do so. He was photographed hanging off a balcony and landing on the floor of the Senate chamber.

18. In a video posted to Facebook and circulated widely on other social media platforms, the defendant claims he was the first person to sit in the House Speaker's chair and calls House Speaker Nancy Pelosi a traitor. The defendant appears to be mistaken as he was also photographed in the seat reserved for the vice president, and not Speaker Pelosi.

19. According to public reporting, the defendant has admitted his involvement in the riots, and apologized for it. In a statement given to CBS2 News he stated: "I love America, I love the people, I didn't hurt anyone and I didn't cause any damage in the Chamber. I got caught up in the moment and when I saw the door to to [sic] the Chamber open, I walked in, hopped down, and sat on the chair. I said my peace then I helped a gentlemen get to safety that was injured then left."

20. Agents from the FBI's Washington Field Office conducted a telephonic interview with a relative of the defendant following submission of information to the FBI's online tip system.

The relative confirmed that the individual in the aforementioned photographs hanging from the balcony and sitting in the vice president's seat is the defendant.

21. Defendant Colt appears to have coordinated his efforts with fellow rioters Ronnie Sandlin, Nate DeGrave, and possibly others.[1] A Facebook search warrant return for an account linked to Sandlin (the "Ronnie Sandlin" account), as well as once publicly-available content for the account, revealed numerous communications between the three individuals. Several posts detail the trio's plans to travel to Washington, DC on January 6, 2021. For example, in a post dated December 31, 2020, Sandlin stated:

> Dear Patriots, I'm organizing a caravan of patriots who are going to Washington D.C. to stand behind our president Donald J. Trump. I posted about this last week and a got almost a dozen messages from people asking how they can help or expressing their wish to participate somehow. Josiah Colt, Nate DeGrave, and myself have already booked and paid for our trip to Washington D.C. but we could use your help and support! Every dollar you contribute to us is a smack in the face to Antifa. Every penny is a boot in the ass against tyranny. Every Buffalo nickel is a body slam against China. If you can't be there in person this is the next best thing. We will be documenting our journey and every contributer will get a personal thank you video shot on location in Washington D.C. and will be featured as a contributor on the video mini documentary. Share, comment, like, and hate on us in the comments.

22. The post also contains a link to a GoFundMe webpage with the caption "Patriots Defending Our Country On Jan. 6th, organized by Ronnie Sandlin" and a photo appearing to depict Sandlin in a car holding what appears to be a semi-automatic rifle. In addition, a screenshot from Sandlin's Facebook account shows Colt lying in a bed holding a firearm, with the caption: "My

[1] Both Sandlin, and Nate DeGrave, whom investigators believe was present with Sandlin inside the Capitol building during the riot, have been charged with multiple offenses in connection with the insurrection at the Capitol.

fellow patriot Josiah Colt sleeping ready for the boogaloo Jan 6." Colt responds to the post that he is "[r]eady for any battle."

23. A "selfie"-style video that the FBI received as an anonymous tip shows Sandlin, DeGrave, and Colt discussing their plans for the 6th inside a TGI Friday's. Based on some of Sandlin's statements in the video, it appears this video was recorded after a rally in DC the morning of January 6, 2021, but prior to the insurrection.

24. In the video, Sandlin says, no less than three times, "freedom is paid for with blood." Sandlin also states:

> Alright so we have been at the protests…we were there pretty early, scoped it out…there were some scrimmages, I will upload the video later…I think a precursor of what is going to [happen] in a few hours. People are really mad…it is just a precursor to what's going to happen…Either way there is going to be violence.

25. A little later in the video, Sandlin states:

> What is happening to this country is absolutely horrific, absolutely horrific…we are ready to occupy the state capitol if needed to…I urge other patriots watching this too, to be willing to take the capitol…if you are watching this and you are a patriot and are here, I think it is time to take the capitol and I don't say that lightly…. I am willing to do it, I

> willing to go and fight for this country. Even if that means I have to sacrifice in some capacity. It is not what I want to do…

26. In the video, Sandlin appears to hand the device used to record the video to Colt and DeGrave. In the video, Colt states that "they are leaving bricks everywhere. There are piles of bricks. It seems like they are encouraging people to riot, because they are leaving stacks of bricks around the city." Sandlin interrupts Colt, stating "allegedly." Colt replies: "No, there are pictures, dude…Nate, show him." DeGrave then shows a picture on his phone of what appeared to be a stack of bricks. Sandlin proceeds to ask "Nate" if he wants "to say something," at which point DeGrave responds:

> We are out here protecting the country, if shit goes down, if Pence does what we think he is going to do. Then we are here to defend this city, defend any city in this country. Let Antifa try us, we are here, we are ready. I say bring it. We are not silent anymore.

27. Colt then says: "The whole thing is a scam, dude. The whole election, they can't just steal an election. Like they are trying to do in Georgia last night. It is a lie." DeGrave responds: "We are sick and tired of the fucking lies. It is time to put an end to this once and for all." Towards the end of the video, Sandlin states:

> If we need to occupy the capitol, we will occupy the capitol. You guys are driving all the way to DC and you are missing the rally. We have been at the rally, we went last night, we have been at the rally since six in the morning. We needed to grab a bite to eat, and like decompress because we went through a few intense moments and also regroup and plan for the next….one o'clock is when it is all going to go down. So we are going to be there back by one o'clock when it is action time it is game time.

28. These statements appear to refer to the joint session of Congress at the U.S. Capitol building that began at approximately 1:00 p.m. Eastern Standard Time (EST). Based on his

statements in the video, it appears Sandlin was addressing other individuals on their way to or already in DC to encourage them to join in the effort to "take the Capitol."

29. The investigation revealed another video, posted to Youtube, titled "Josiah Colt Says Violence at the Capital Might be Necessary." In the video, Sandlin and Colt were interviewed alongside an individual, believed to be DeGrave, dressed in tactical gear—i.e., black body armor, a helmet, and a face mask—and a red-white-and-blue bandanna around his neck. In the video, Colt says "[i]f violence happens, it happens" and "we're just hear to defend ourselves." Sandlin interjects, stating that he "support[s] Trump" and, again, "freedom is paid for with blood."

30. On February 5, 2021, law enforcement received subpoena results for Facebook account ID: 100005928300442. The subscriber information listed the name "Josiah Colt" and email address "josiahcolt@gmail.com" as the most recently verified registered email.

31. During the investigation, Law-enforcement authorities discovered that telephone number "208-703-7900" is serviced by Verizon and linked to an Apple iPhone device and iCloud account registered to the name "Josiah Colt" and email address "josiahcolt@gmail.com". Additionally, law enforcement identified records confirming this mobile device uploaded photo and video content from Washington DC on January 6, 2021. This is consistent with posts to Facebook accounts made in Josiah Colt's name immediately after exiting the U.S. Capitol on January 6, 2021.

32. On January 13, 2021, law enforcement sent a preservation letter to Facebook for account ID: 100005928300442.

BACKGROUND CONCERNING PROVIDER'S ACCOUNTS

33. PROVIDER is the provider of the internet-based account identified by Josiah Colt with user ID 100005928300442.

34. PROVIDER owns and operates a free-access social networking website of the same name that can be accessed at http://www.facebook.com ("Facebook"). The website is owned and operated by PROVIDER. PROVIDER allows Facebook users to establish accounts with PROVIDER, and users can then use their Facebook accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

35. PROVIDER asks users to provide basic contact and personal identifying information to PROVIDER, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers (for password retrieval), physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. PROVIDER also assigns a user-identification number ("user ID") to each account. PROVIDER identifies unique Facebook accounts by a user's e-mail address, the user ID, or the username associated with a Facebook profile.

36. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. PROVIDER assigns a group identification number to each Facebook group. A Facebook user can also connect directly with individual Facebook users by sending each user a "friend" request. If the recipient of a "friend" request accepts the request, then the two users will become "friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "friends" and a "News Feed," which highlights information about the user's "friends," such as profile changes, upcoming events, and birthdays.

37. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a

Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook "friends" to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

38. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

39. PROVIDER allows Facebook users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides Facebook users the ability to "tag" (*i.e.*, label) other Facebook users in a photo or video. When a user is "tagged" in a photo or video, he or she receives a notification of the "tag" and a link to see the photo or video. For PROVIDER's purposes, the photos and videos associated with a Facebook user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user "tagged" in them.

40. Facebook users can exchange private messages on Facebook with other users. Those messages are stored by PROVIDER unless deleted by the user. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a chat feature that allows users to send and receive instant messages through Facebook Messenger. These chat communications are stored in the chat history for the account. Facebook also has Video and Voice Calling features, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

41. In general, user-generated content and information about the account (such as a user's photos, "status" updates, an activity log as described below, and the like) that is written using, stored on, sent from, or sent to a PROVIDER account can be indefinitely stored in connection with that account, unless the subscriber deletes the material. Further, such user-generated content can remain on PROVIDER's servers indefinitely if not deleted by the subscriber, and even after being deleted, it may continue to be available on PROVIDER's servers for a certain period of time.

42. A Facebook user also can send other Facebook users a notification indicating that the recipient has been "poked". Facebook "pokes" enable Facebook users to get the attention of other Facebook users without delivering any user generated messages or other content.

43. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.

44. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as webpages or

content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages.

45. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

46. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos in which the user has been "tagged", as well as connections made through the account, such as "liking" a Facebook page or adding someone as a "friend". The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.

47. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

48. In addition to the applications described above, PROVIDER also provides Facebook users with access to thousands of other applications ("apps") on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

49. PROVIDER also retains Internet Protocol ("IP") logs for a given Facebook user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

50. Depending on the user's privacy settings, PROVIDER may also obtain and store the physical location of the user's device(s), including Global Positioning System ("GPS") data, as the user interacts with the Facebook service on those device(s).

51. Social networking providers like PROVIDER typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with PROVIDER about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like PROVIDER 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.

52. Based on my training and experience, I know that providers such as PROVIDER also collect information relating to the devices used to access a subscriber's account – such as laptop or desktop computers, cell phones, and tablet computers. Such devices can be identified in various ways. For example, some identifiers are assigned to a device by the manufacturer and relate to the specific machine or "hardware," some identifiers are assigned by a telephone carrier concerning a particular user account for cellular data or voice services, and some identifiers are actually assigned by PROVIDER in order to track what devices are using PROVIDER's accounts and services. Examples of these identifiers include unique application number, hardware model, operating system version, Global Unique Identifier ("GUID"), device serial number, mobile network information, telephone number, Media Access Control ("MAC") address, and International Mobile Equipment Identity ("IMEI"). Based on my training and experience, I know

that such identifiers may constitute evidence of the crimes under investigation because they can be used (a) to find other PROVIDER accounts created or accessed by the same device and likely belonging to the same user, (b) to find other types of accounts linked to the same device and user, and (c) to determine whether a particular device recovered during course of the investigation was used to access the PROVIDER account.

53. PROVIDER also allows its subscribers to access its various services through an application that can be installed on and accessed via cellular telephones and other mobile devices. This application is associated with the subscriber's PROVIDER account. In my training and experience, I have learned that when the user of a mobile application installs and launches the application on a device (such as a cellular telephone), the application directs the device in question to obtain a Push Token, a unique identifier that allows the provider associated with the application (such as PROVIDER) to locate the device on which the application is installed. After the applicable push notification service (*e.g.*, Apple Push Notifications (APN) or Google Cloud Messaging) sends a Push Token to the device, the Token is then sent to the application, which in turn sends the Push Token to the application's server/provider. Thereafter, whenever the provider needs to send notifications to the user's device, it sends both the Push Token and the payload associated with the notification (*i.e.*, the substance of what needs to be sent by the application to the device). To ensure this process works, Push Tokens associated with a subscriber's account are stored on the provider's server(s). Accordingly, the computers of PROVIDER are likely to contain useful information that may help to identify the specific device(s) used by a particular subscriber to access the subscriber's PROVIDER account via the mobile application.

54. Based on my training and experience, I know that providers such as PROVIDER use cookies and similar technologies to track users visiting PROVIDER's webpages and using its

products and services. Basically, a "cookie" is a small file containing a string of characters that a website attempts to place onto a user's computer. When that computer visits again, the website will recognize the cookie and thereby identify the same user who visited before. This sort of technology can be used to track users across multiple websites and online services belonging to PROVIDER. More sophisticated cookie technology can be used to identify users across devices and web browsers. From training and experience, I know that cookies and similar technology used by providers such as PROVIDER may constitute evidence of the criminal activity under investigation. By linking various accounts, devices, and online activity to the same user or users, cookies and linked information can help identify who was using a PROVIDER account and determine the scope of criminal activity.

55. Based on my training and experience, I know that PROVIDER maintains records that can link different PROVIDER accounts to one another, by virtue of common identifiers, such as common e-mail addresses, common telephone numbers, common device identifiers, common computer cookies, and common names or addresses, that can show a single person, or single group of persons, used multiple PROVIDER accounts. Based on my training and experience, I also know that evidence concerning the identity of such linked accounts can be useful evidence in identifying the person or persons who have used a particular PROVIDER account.

56. Based on my training and experience, I know that subscribers can communicate directly with PROVIDER about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Providers such as PROVIDER typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the

crimes under investigation because the information can be used to identify the account's user or users.

57. In summary, based on my training and experience in this context, I believe that the computers of PROVIDER are likely to contain user-generated content such as stored electronic communications (including retrieved and unretrieved messages for PROVIDER subscribers), as well as PROVIDER-generated information about its subscribers and their use of PROVIDER services and other online services. In my training and experience, all of that information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. In fact, even if subscribers provide PROVIDER with false information about their identities, that false information often nevertheless provides clues to their identities, locations, or illicit activities.

58. As explained above, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the investigating authorities to establish and prove each element of the offense or, alternatively, to exclude the innocent from further suspicion. From my training and experience, a Facebook user's IP log, stored electronic communications, and other data retained by PROVIDER, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and "tagged" photos (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described above, PROVIDER logs the IP addresses from which Facebook users access

their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, PROVIDER builds geo-location into some of its Facebook services. Geo-location allows, for example, users to "tag" their location in posts and Facebook "friends" to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the Facebook account user. Last, Facebook account activity may provide relevant insight into the Facebook account user's state of mind as it relates to the offense under investigation. For example, information on the Facebook 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).[2]

59. Based on my training and experience, I know that evidence of who controlled, used, and/or created a PROVIDER account may be found within the user-generated content created or stored by the PROVIDER subscriber. This type of evidence includes, for example, personal correspondence, personal photographs, purchase receipts, contact information, travel itineraries, and other content that can be uniquely connected to a specific, identifiable person or group. In

[2] At times, social media providers such as PROVIDER can and do change the details and functionality of the services they offer. While the information in this section is true and accurate to the best of my knowledge and belief, I have not specifically reviewed every detail of PROVIDER's services in connection with submitting this application for a search warrant. Instead, I rely upon my training and experience, and the training and experience of others, to set forth the foregoing description for the Court.

addition, based on my training and experience, I know that this type of user-generated content can provide crucial identification evidence, whether or not it was generated close in time to the offenses under investigation. This is true for at least two reasons. First, people that commit crimes involving electronic accounts (*e.g.*, e-mail accounts) typically try to hide their identities, and many people are more disciplined in that regard right before (and right after) committing a particular crime. Second, earlier-generated content may be quite valuable, because criminals typically improve their tradecraft over time. That is to say, criminals typically learn how to better separate their personal activity from their criminal activity, and they typically become more disciplined about maintaining that separation, as they become more experienced. Finally, because e-mail accounts and similar PROVIDER accounts do not typically change hands on a frequent basis, identification evidence from one period can still be relevant to establishing the identity of the account user during a different, and even far removed, period of time.

REQUEST TO SUBMIT WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

60. I respectfully request, pursuant to Rules 4.1 and 41(d)(3) of the Federal Rules of Criminal Procedure, permission to communicate information to the Court by telephone in connection with this Application for a Search Warrant. I submit that Assistant U.S. Attorney Elizabeth Aloi, an attorney for the United States, is capable of identifying my voice and telephone number for the Court.

CONCLUSION

61. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on PROVIDER, who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested

warrant at any time in the day or night. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Respectfully submitted,

Matthew Gano
Special Agent
Federal Bureau of Investigation

Subscribed and sworn pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3) on February 9, 2021.

ZIA M. FARUQUI
UNITED STATES MAGISTRATE JUDGE

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by _____ ("PROVIDER"), and my title is _____. I am a custodian of records for PROVIDER, and I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of PROVIDER. The attached records consist of:

_____

[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]

I further state that:

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

b. such records were generated by PROVIDER's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of PROVIDER in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by PROVIDER, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

_____ _____

Date Signature