

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)

IN THE MATTER OF THE SEARCH OF INFORMATION
ASSOCIATED WITH ONE FACEBOOK, INC. ACCOUNT
PURSUANT TO 18 U.S.C. § 2703 FOR INVESTIGATION OF
VIOLATION OF 18 U.S.C. § 1512(c)(2)

Case No. 21-sc-657

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):

Facebook, Inc. account identified by User Name: "Derek Jancart," User ID: 100000415172654, and which is stored at Facebook, Inc., (See Attachment A)
located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

violations of 18 U.S.C. §§ 1512(c)(2), 111, 231, 371, 372, 930, 641, 1361, 2101, 1752(a)(1) and (2) and 40 U.S.C. § 5104(e)(2) (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.

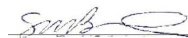
The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. §§ 1512(c)(2), 111, 231, 371, 372	obstruction of Congress, assaulting a federal agent, civil disorders, conspiracy to
18 U.S.C. §§ 930, 641, 1361, 2101	impede or injure officer; possession of firearms, theft of government property,
1752(a)(1) and (2), 40 U.S.C. § 5104(e)(2)	destruction of government property, violet entry, interstate travel to participate in riot

The application is based on these facts:

SEE 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

Stuart Bronstein, FBI Special Agent

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: 02/25/2021

Judge's signature

City and state: Washington, D.C.

Robin M. Meriweather, U.S. Magistrate Judge

Printed name and title

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)IN THE MATTER OF THE SEARCH OF INFORMATION
ASSOCIATED WITH ONE FACEBOOK, INC. ACCOUNT
PURSUANT TO 18 U.S.C. § 2703 FOR INVESTIGATION OF
VIOLATION OF 18 U.S.C. § 1512(c)(2)

Case No. 21-sc-657

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):

a Facebook, Inc. account identified by User Name: "Derek Jancart," User ID: 100000415172654, 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. (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):

violations of 18 U.S.C. § 1512(c)(2) (obstruction of Congress); 111 (assaulting a federal agent); 231 (civil disorders), 371 (conspiracy); 372 (conspiracy to impede or injure officer); 930 (possession of firearms and dangerous weapons in federal facilities); 641 (theft of government property); 1361 (destruction of government property); 2101 (interstate travel to participate in riot); 1752(a)(1) and (2) (unlawful entry on restricted buildings or grounds); and 40 U.S.C. § 5104(e)(2) (violent entry, disorderly conduct, and other offenses on capitol grounds) (See Attachment B)

YOU ARE COMMANDED to execute this warrant on or before March 11, 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 Robin M. Meriweather, 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: 02/25/2021

Judge's signature

City and state: Washington, D.C.

Robin M. Meriweather, U.S. Magistrate Judge

Printed name and title

Case No.:
21-sc-657

Copy of warrant and inventory left with:

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

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Executing officer's signature

Printed name and title

ATTACHMENT A
Property to Be Searched

This warrant applies to information which is associated with a Facebook, Inc. account identified by **User Name: “Derek Jancart,” User ID: 100000415172654**, 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 September 1, 2020 to 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 September 1, 2020 to 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 September 1, 2020 to 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 September 1, 2020 to Present: All “check ins” and other location information;
- f. For the time period September 1, 2020 to 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. For the time period September 1, 2020 to Present: 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 communications with legal counsel).

Within SEVEN (7) 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 Stuart M Bronstein
425 W. Nationwide Blvd
Columbus, Ohio 43215
Email: smbronstein@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)(2) (obstruction of Congress); 111 (assaulting a federal agent); 231 (civil disorders), 371 (conspiracy); 372 (conspiracy to impede or injure officer); 930 (possession of firearms and dangerous weapons in federal facilities); 641 (theft of government property); 1361 (destruction of government property); 2101 (interstate travel to participate in riot); 1752(a)(1) and (2) (unlawful entry on restricted buildings or grounds); and 40 U.S.C. § 5104(e)(2) (violent entry, disorderly conduct, and other offenses on capitol grounds) 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 the unlawful entry into the Capitol on January 6, 2021, disorderly conduct within the Capitol on January 6, 2021, acts of obstruction within the Capitol on January 6, 2021, other crimes committed by participants in the January 6, 2021 riot including destruction of property and assault on police officers, and evidence of any planning or agreement regarding events at the Capitol on January 6, 2021, including any information shared or received regarding the events on January 6, 2021.
- (f) The Identity of any person(s) who communicated with the user ID about matters relating to the above items including records that may help reveal their whereabouts or preplanned actions.

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 FACEBOOK, INC.
ACCOUNT PURSUANT TO 18 U.S.C.
§ 2703 FOR INVESTIGATION OF
VIOLATION OF 18 U.S.C. § 1512(c)(2)**

SC No. 21-SC-657

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

I, **Stuart Bronstein** 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 an account— that is, Facebook User Name: “Derek Jancart,” User ID: 100000415172654 (“TARGET ACCOUNT”) – 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. I have been in this position since June of 2014. Prior to June 2014, I was a Police Officer with the Memphis Police Department, Memphis, TN for ten (10) years. I have investigated numerous crimes including, but not limited to bank robbery, drug trafficking, aggravated assaults, criminal trespass, and property crimes. While performing my duties as a Special Agent, I have participated in various investigations involving computer-related offenses and have executed search warrants, including searches and seizures of computers, smart phones, digital media, software, and electronically stored information. I have received both formal and informal training in the detection and investigation of offenses utilizing electronic media. As a federal agent, I am authorized to investigate violations of laws of the United States, and as a law enforcement officer I am authorized to execute warrants issued under the authority of the United States.

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)(2) (obstruction of Congress); 111 (assaulting a federal agent); 231 (civil disorders), 371 (conspiracy); 372 (conspiracy to impede or injure officer); 930 (possession of firearms and dangerous weapons in federal facilities); 641 (theft of government property); 1361 (destruction of government property); 2101 (interstate travel to participate in riot); 1752(a)(1) and (2) (unlawful entry on restricted buildings or grounds); and 40 U.S.C. § 5104(e)(2) (violent entry, disorderly conduct, and other offenses on capitol grounds) (the "Target Offenses") have been committed by DEREK

JANCART (“the Subject”) and other identified and unidentified persons, including others who may have been aided and abetted by, or conspiring with, the Subject, as well as others observed by the Subject. 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

Background – The U.S. Capitol on January 6, 2021

6. USCP, the FBI, and assisting law enforcement agencies are investigating a riot and related offenses that occurred at the United States Capitol Building, located at 1 First Street, NW, Washington, D.C., 20510 at latitude 38.88997 and longitude -77.00906 on January 6, 2021.

7. At the U.S. Capitol, the building itself has 540 rooms covering 175,170 square feet of ground, roughly four acres. The building is 751 feet long (roughly 228 meters) from north to south and 350 feet wide (106 meters) at its widest point. The U.S. Capitol Visitor Center is 580,000 square feet and is located underground on the east side of the Capitol. On the west side of the Capitol building is the West Front, which includes the inaugural stage scaffolding, a variety of open concrete spaces, a fountain surrounded by a walkway, two broad staircases, and multiple

terraces at each floor. On the East Front are three staircases, porticos on both the House and Senate side, and two large skylights into the Visitor's Center surrounded by a concrete parkway. All of this area was barricaded and off limits to the public on January 6, 2021.

8. The U.S. Capitol is secured 24 hours a day by USCP. Restrictions around the U.S. Capitol include permanent and temporary security barriers and posts manned by USCP. Only authorized people with appropriate identification are allowed access inside the U.S. Capitol.

9. On January 6, 2021, the exterior plaza of the U.S. Capitol was closed to members of the public.

10. On January 6, 2021, a joint session of the United States Congress convened at the U.S. Capitol. During the joint session, elected members of the United States House of Representatives and the United States Senate were meeting in separate chambers of the U.S. Capitol to certify the vote count of the Electoral College of the 2020 Presidential Election, which took place on November 3, 2020 ("Certification"). The joint session began at approximately 1:00 p.m. Eastern Standard Time (EST). Shortly thereafter, by approximately 1:30 p.m., the House and Senate adjourned to separate chambers to resolve a particular objection. Vice President Mike Pence was present and presiding, first in the joint session, and then in the Senate chamber.

11. As the proceedings continued in both the House and the Senate, and with Vice President Mike Pence present and presiding over the Senate, a large crowd gathered outside the U.S. Capitol. As noted above, temporary and permanent barricades were in place around the exterior of the U.S. Capitol building, and USCP were present and attempting to keep the crowd away from the Capitol building and the proceedings underway inside.

12. At around 1:00 p.m. EST, known and unknown individuals broke through the police lines, toppled the outside barricades protecting the U.S. Capitol, and pushed past USCP and supporting law enforcement officers there to protect the U.S. Capitol.

13. At around 1:30 p.m. EST, USCP ordered Congressional staff to evacuate the House Cannon Office Building and the Library of Congress James Madison Memorial Building in part because of a suspicious package found nearby. Pipe bombs were later found near both the Democratic National Committee and Republican National Committee headquarters.

14. Media reporting showed a group of individuals outside of the Capitol chanting, “Hang Mike Pence.” I know from this investigation that some individuals believed that Vice President Pence possessed the ability to prevent the certification of the presidential election and that his failure to do so made him a traitor.

15. At approximately 2:00 p.m., some people in the crowd forced their way through, up, and over the barricades and law enforcement. The crowd advanced to the exterior façade of the building. The crowd was not lawfully authorized to enter or remain in the building and, prior to entering the building, no members of the crowd submitted to security screenings or weapons checks by U.S. Capitol Police Officers or other authorized security officials. At such time, the certification proceedings were still underway and the exterior doors and windows of the U.S. Capitol were locked or otherwise secured. Members of law enforcement attempted to maintain order and keep the crowd from entering the Capitol.

16. Shortly after 2:00 p.m., individuals in the crowd forced entry into the U.S. Capitol, including by breaking windows and by assaulting members of law enforcement, as others in the crowd encouraged and assisted those acts. Publicly available video footage shows an unknown

individual saying to a crowd outside the Capitol building, “We’re gonna fucking take this,” which your affiant believes was a reference to “taking” the U.S. Capitol.



17. Shortly thereafter, at approximately 2:20 p.m. members of the United States House of Representatives and United States Senate, including the President of the Senate, Vice President Mike Pence, were instructed to—and did—evacuate the chambers. That is, at or about this time, USCP ordered all nearby staff, Senators, and reporters into the Senate chamber and locked it down. USCP ordered a similar lockdown in the House chamber. As the subjects attempted to break into the House chamber, by breaking the windows on the chamber door, law enforcement were forced to draw their weapons to protect the victims sheltering inside.

18. At approximately 2:30 p.m. EST, known and unknown subjects broke windows and pushed past USCP and supporting law enforcement officers forcing their way into the U.S. Capitol on both the west side and the east side of the building. Once inside, the subjects broke windows and doors, destroyed property, stole property, and assaulted federal police officers. Many of the

federal police officers were injured, several were admitted to the hospital, and at least one federal police officer died as a result of the injuries he sustained. The subjects also confronted and terrorized members of Congress, Congressional staff, and the media. The subjects carried weapons including tire irons, sledgehammers, bear spray, and Tasers. They also took police equipment from overrun police including shields and police batons. At least one of the subjects carried a handgun with an extended magazine. These actions by the unknown individuals resulted in the disruption and ultimate delay of the vote Certification.

19. Also at approximately 2:30 p.m. EST, USCP ordered the evacuation of lawmakers, Vice President Mike Pence, and president pro tempore of the Senate, Charles Grassley, for their safety.

20. At around 2:45 p.m. EST, subjects broke into the office of House Speaker Nancy Pelosi.

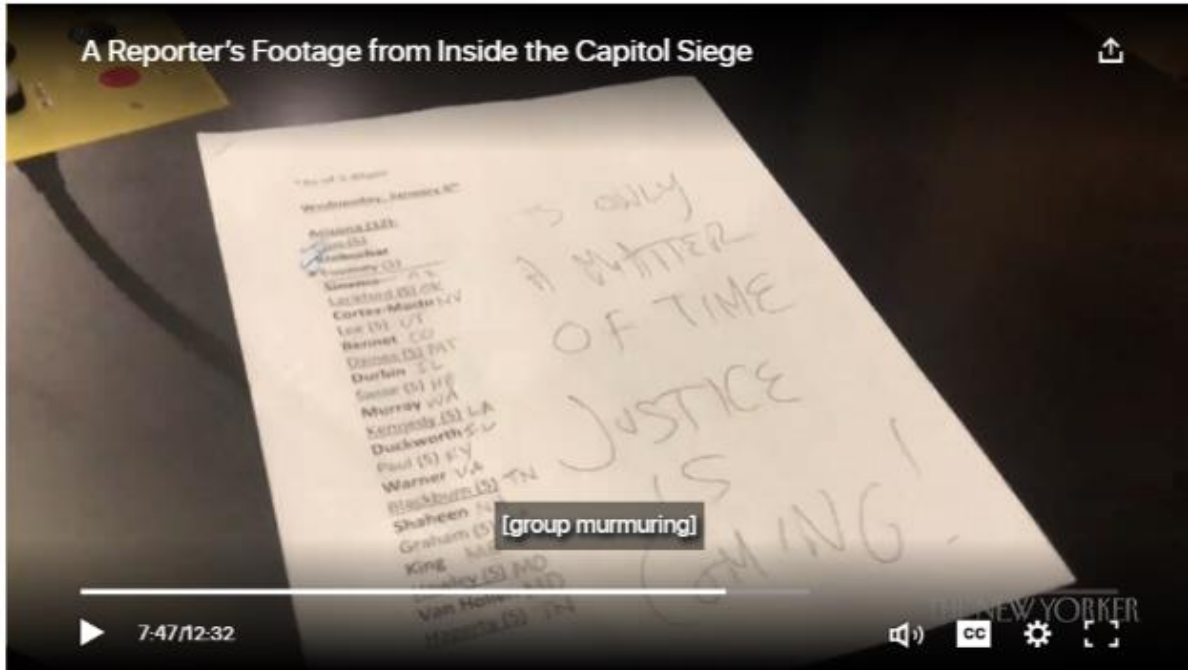
21. At around 2:47 p.m., subjects broke into the United States Senate Chamber. Publicly available video shows an individual asking, “Where are they?” as they opened up the door to the Senate Chamber. Based upon the context, law enforcement believes that the word “they” is in reference to members of Congress.



22. After subjects forced entry into the Senate Chamber, publicly available video shows that an individual asked, “Where the fuck is Nancy?” Based upon other comments and the context, law enforcement believes that the “Nancy” being referenced was the Speaker of the House of Representatives, Nancy Pelosi.



23. An unknown subject left a note on the podium on the floor of the Senate Chamber. This note, captured by the filming reporter, stated “A Matter of Time Justice is Coming.”



24. During the time when the subjects were inside the Capitol building, multiple subjects were observed inside the US Capitol wearing what appears to be, based upon my training and experience, tactical vests and carrying flex cuffs. Based upon my knowledge, training, and experience, I know that flex cuffs are a manner of restraint that are designed to be carried in situations where a large number of individuals were expected to be taken into custody.



25. At around 2:48 p.m. EST, DC Mayor Muriel Bowser announced a citywide curfew beginning at 6:00 p.m.

26. At around 2:45 p.m. EST, one subject was shot and killed while attempting to break into the House chamber through the broken windows.

27. At about 3:25 p.m. EST, law enforcement officers cleared the Senate floor.

28. Between 3:25 and around 6:30 p.m. EST, law enforcement was able to clear the U.S. Capitol of all of the subjects.

29. Based on these events, all proceedings of the United States Congress, including the joint session, were effectively suspended until shortly after 8:00 p.m. the same day. In light of the dangerous circumstances caused by the unlawful entry to the U.S. Capitol, including the danger posed by individuals who had entered the U.S. Capitol without any security screening or weapons check, Congressional proceedings could not resume until after every unauthorized occupant had left the U.S. Capitol, and the building had been confirmed secured. The proceedings resumed at approximately 8:00 pm after the building had been secured. Vice President Pence remained in the United States Capitol from the time he was evacuated from the Senate Chamber until the session resumed.

30. Beginning around 8:00 p.m., the Senate resumed work on the Certification.

31. Beginning around 9:00 p.m., the House resumed work on the Certification.

32. Both chambers of Congress met and worked on the Certification within the Capitol building until approximately 3 a.m. on January 7, 2021.

33. During national news coverage of the aforementioned events, video footage which appeared to be captured on mobile devices of persons present on the scene depicted evidence of violations of local and federal law, including scores of individuals inside the U.S. Capitol building without authority to be there.

34. Based on my training and experience, I know that it is common for individuals to carry and use their cell phones during large gatherings, such as the gathering that occurred in the area of the U.S. Capitol on January 6, 2021. Such phones are typically carried at such gatherings to allow individuals to capture photographs and video footage of the gatherings, to communicate with other individuals about the gatherings, to coordinate with other participants at the gatherings, and to post on social media and digital forums about the gatherings.

35. Many subjects seen on news footage in the area of the U.S. Capitol are using a cell phone in some capacity. It appears some subjects were recording the events occurring in and around the U.S. Capitol and others appear to be taking photos, to include photos and video of themselves after breaking into the U.S. Capitol itself, including photos of themselves damaging and stealing property. As reported in the news media, others inside and immediately outside the U.S. Capitol live-streamed their activities, including those described above as well as statements about these activities.

36. Photos below, available on various publicly available news, social media, and other media show some of the subjects within the U.S. Capitol during the riot. In several of these photos, the individuals who broke into the U.S. Capitol can be seen holding and using cell phones, including to take pictures and/or videos:



¹ <https://losangeles.cbslocal.com/2021/01/06/congresswoman-capitol-building-takeover-an-attempted-coup/>

² <https://www.businessinsider.com/republicans-objecting-to-electoral-votes-in-congress-live-updates-2021-1>.



Facts Specific to This Application

37. On January 9, 2021, a concerned citizen, C-1 provided a tip to the FBI that Facebook User “Derek Jancart” posted on Facebook images from the Capitol riot inside the U.S. Capitol Building, specifically, a photograph from outside the Office of the Speaker conference room. The Facebook post (shown in the Facebook Screenshot, below) was captioned “we’re in”. C-1 is a former co-worker of DEREK JANCART.

³<https://www.thv11.com/article/news/arkansas-man-storms-capitol-pelosi/91-41abde60-a390-4a9e-b5f3-d80b0b96141e>



Facebook Screenshot

38. On February 9, 2021, during a follow up interview, C-1 was shown the below photographs which included screen captures from Metropolitan Police Department body worn camera and Capital Building Security Camera footage (including Photos 1 through 5, below). Also included was a picture of the original screen capture provided in C-1's complaint, as shown above. C-1 positively identified DEREK JANCART in each picture as well as his/her original submission to the FBI.



Photo 1

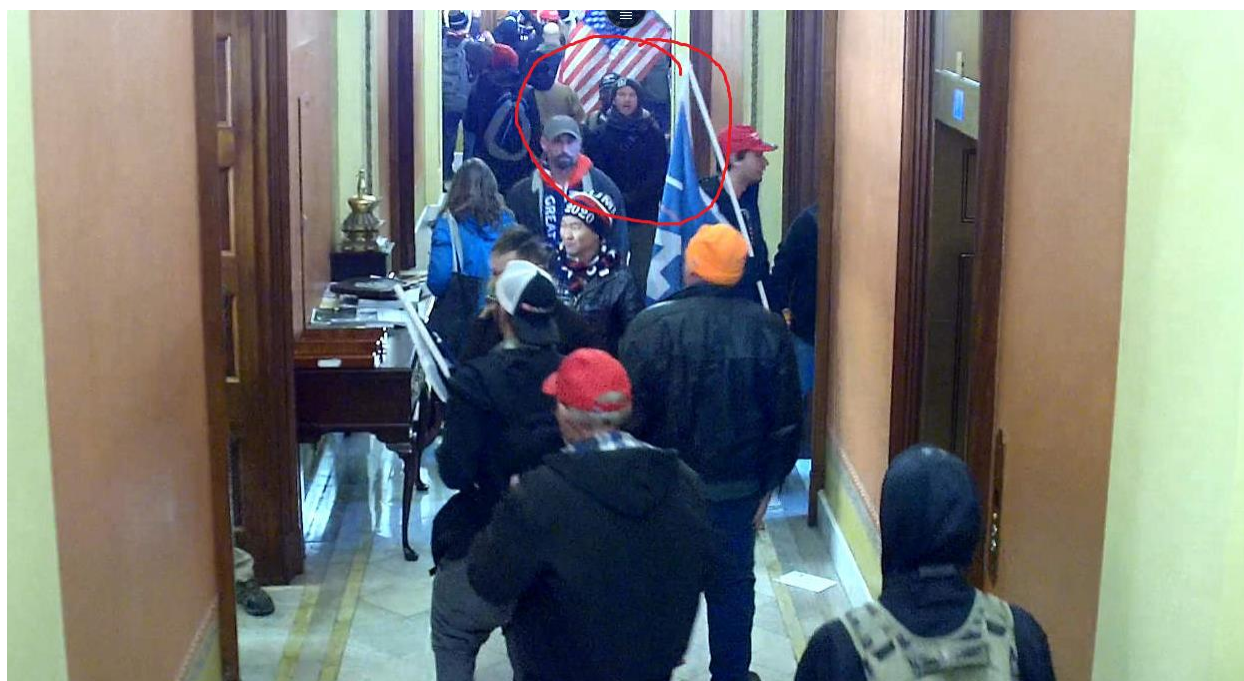


Photo 2

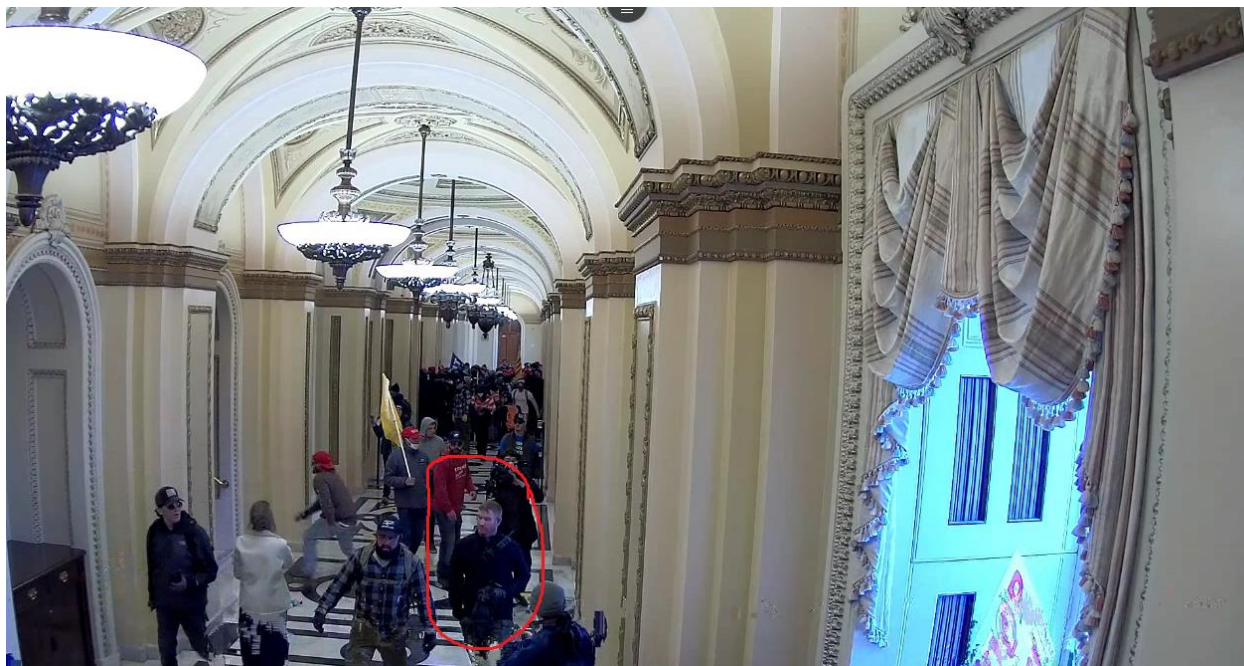


Photo 3

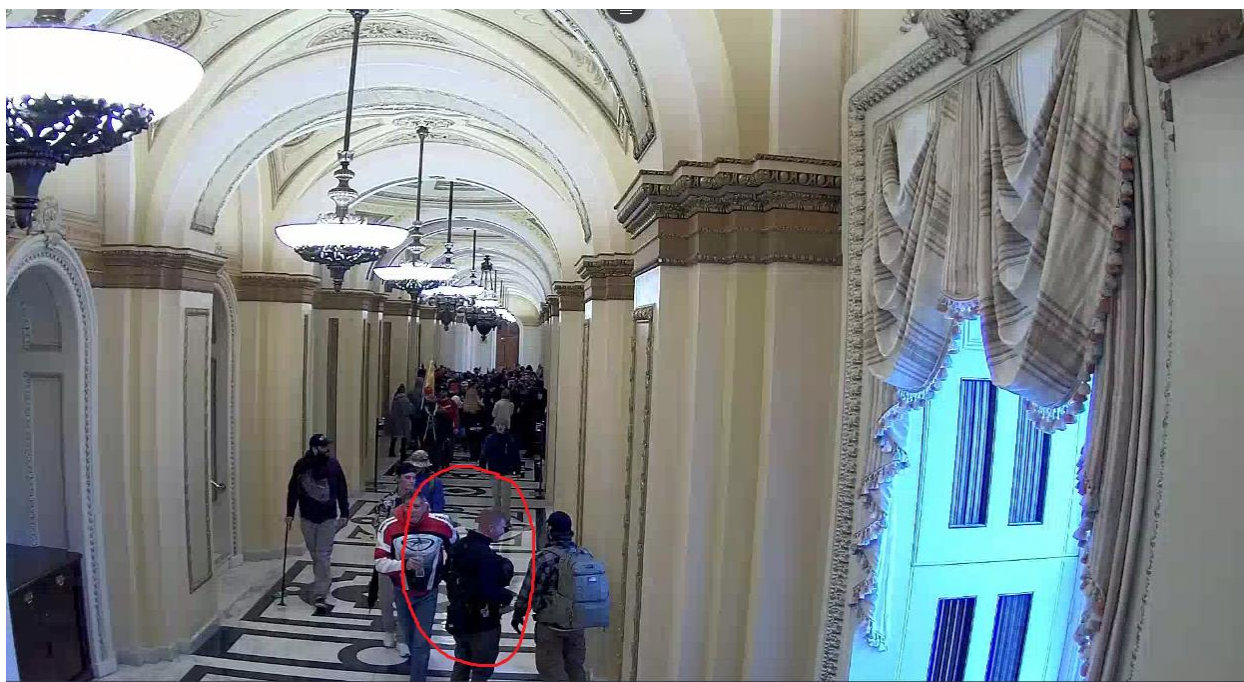


Photo 4



Photo 5

39. On February 10, 2021, a concerned citizen, C-2, a family member of DEREK JANCART, was interviewed and advised that he/she provided a tip to the FBI (01/10/21), that his/her family member, DEREK JANCART, was at and inside the U.S. Capitol during the events of January 6, 2021. C-2 received a phone call from another family member, who advised that DEREK JANCART was inside the Capitol building. C-2 contacted DEREK JANCART via text message. Your affiant has reviewed the text message exchange between C-2 and DEREK JANCART, and saw that DEREK JANCART confirmed his presence inside of the Capitol. C-2 was shown the above photographs and positively identified DEREK JANCART in all photographs except for Photo 2, above. C-2 also positively identified the Facebook post in front of the Office of the Speaker conference room as the post from JANCART'S Facebook account.

40. Records subpoenaed from AT&T show that DEREK JANCART is the subscriber of a cellular phone number ending in 4899. The records from AT&T also showed the subscriber listed an email address of spoonze22@yahoo.com.

41. According to records obtained through a search warrant which was served on A&T, on January 6, 2021, in and around the time of the incident, that same cell phone number, ending in 4899, was identified as having utilized a cell site consistent with providing service to a geographic area that includes the interior of the United States Capitol Building.

42. Records subpoenaed from Facebook showed that the subscriber of the TARGET ACCOUNT is DEREK JANCART. The records showed the subscriber provided an email address of spoonze22@yahoo.com and the same telephone number ending in 4899 referenced above.

43. On February 5, 2021, PROVIDER was served with a preservation letter under 18 U.S.C. § 2703(f) related to the TARGET ACCOUNT.

44. Based on the foregoing I submit that there is probable cause that fruits, contraband, evidence and instrumentalities of the Target Offenses will be found in the TARGET ACCOUNT.

BACKGROUND CONCERNING PROVIDER'S ACCOUNTS

45. PROVIDER is the provider of the TARGET ACCOUNT.

46. 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.

47. 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.

48. 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.

49. 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.

50. 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.

51. 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.

52. 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.

53. 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.

54. 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.

55. 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.

56. 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.

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

58. 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.

59. 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.

60. 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.

61. 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.

62. 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).

63. 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.

64. 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.

65. 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.

66. 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.

67. 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.

68. 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.

69. 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.

70. 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 inculcate 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).⁴

71. 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 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,

⁴ 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.

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**

72. 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 Leslie Goemaat, an attorney for the United States, is capable of identifying my voice and telephone number for the Court.

CONCLUSION

73. 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,



STUART BRONSTEIN
Special Agent
Federal Bureau of Investigation

Subscribed and sworn pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3) on February 25, 2021.

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