

UNITED STATES DISTRICT COURT

for the
Western District of Washington

In the Matter of the Search of
*(Briefly describe the property to be searched
or identify the person by name and address)*
Samsung Galaxy 22 Ultra,
more fully described in Attachment A

Case No. MJ23-624

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

A Samsung Galaxy 22 Ultra, more fully described in Attachment A, incorporated herein by reference.

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

See Attachment B, incorporated herein by reference.

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:

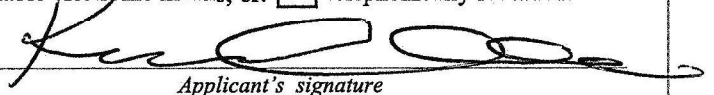
<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 1752(a)(1), (a)(2)	Entering Remaining in Restricted Buildings Grounds in Disorderly or Disruptive Conduct
40 U.S.C. § 5104(3)(D), (G)	Disorderly or Disruptive Conduct in Capitol Buildings and Parading, Demonstrating, or Picketing in a Capitol Building

The application is based on these facts:

See Affidavit of Special Agent Kenna M. Gonzales, 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.

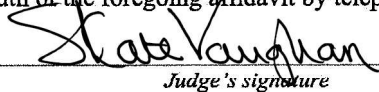
Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: by reliable electronic means; or: telephonically recorded.


Applicant's signature

Kenna M. Gonzales, Special Agent
Printed name and title

- The foregoing affidavit was sworn to before me and signed in my presence, or
- The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 12/29/2023


Judge's signature

City and state: Seattle, Washington

S. Kate Vaughan, United States Magistrate Judge
Printed name and title

AFFIDAVIT OF KENNA M. GONZALES

1
2
3 STATE OF WASHINGTON)
4) ss
5 COUNTY OF KING)
6

7 I, Kenna M. Gonzales, being first duly sworn, hereby depose and state as follows:

8 **INTRODUCTION**

9 1. I make this affidavit in support of an application under Rule 41 of the
10 Federal Rules of Criminal Procedure for a search warrant authorizing the examination of
11 property, a digital device described in Attachment A (the “TARGET DEVICE”), which is
12 currently in the possession of law enforcement, for the information described in
13 Attachment B.

14 2. Unless otherwise noted, wherever in this affidavit I assert that a statement
15 was made, that statement is described in substance and is not intended to be a verbatim
16 recitation of such statement. Wherever in this affidavit I quote statements, those
17 quotations have been taken from draft transcripts, which are subject to further revision.

18 3. Unless otherwise stated, the conclusions and beliefs I express in this
19 affidavit are based on my training, experience, and knowledge of the investigation, and
20 reasonable inferences I’ve drawn from my training, experience, and knowledge of the
21 investigation.

22 **AFFIANT BACKGROUND**

23 4. Your affiant, Kenna M. Gonzales, is a Special Agent by the Federal Bureau
24 of Investigation (FBI) and have been since September of 2022. Currently, I am assigned
25 to the Seattle Field Office, where I am tasked with investigating domestic terrorism. As a
26 Special Agent, I am authorized by law or by a government agency to engage in or
27 supervise the prevention, detention, investigation, or prosecution of a violation of Federal

1 criminal laws. As such, I am an “investigative or law enforcement officer” of the United
2 States within the meaning of Title 18, United States Code, Section 2510(7), that is, an
3 officer of the United States who is empowered by law to conduct investigations of, and to
4 make arrests for, offenses enumerated in Section 2516 of Title 18, United States Code.

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

10 6. Based on my training and experience and the facts set forth in this affidavit,
11 I respectfully submit that there is probable cause to believe that violations of: 18 U.S.C. §
12 1752(a)(1) (entering or remaining in restricted buildings or grounds); 18 U.S.C. §
13 1752(a)(2) (disorderly and disruptive conduct in a restricted building or grounds); 40
14 U.S.C. § 5104(e)(2)(D) (disorderly or disruptive conduct in the Capitol Buildings); and
15 40 U.S.C. § 5104(e)(2)(G) (parading, demonstrating, or picketing in a Capitol Building)
16 (the “TARGET OFFENSES”) have been committed by MATTHEW STICKNEY and
17 others, known and unknown. There is also probable cause to search the TARGET
18 DEVICE for the things described in Attachment B.

19 **IDENTIFICATION OF THE DEVICE TO BE EXAMINED**

20 7. The property to be searched is a Samsung Galaxy 22 Ultra, black in color,
21 with a black Otterbox case, and the phone number 360-930-2065 (hereinafter, the
22 “TARGET DEVICE”). As described below the TARGET DEVICE was owned, used, or
23 controlled by STICKNEY and obtained from STICKNEY’s wife on December 20, 2023.
24 The TARGET DEVICE is currently in the possession of the FBI at 1110 3rd Avenue in
25 Seattle, Washington.

26 **PROBABLE CAUSE**

27 **A. Probable Cause Regarding the Target Offenses**

1 8. On December 15, 2023, Hon. G. Michael Harvey, United States Magistrate
2 Judge for the District of Columbia, found probable cause that STICKEY had committed
3 the TARGET OFFENSES and authorized a warrant for STICKNEY's arrest. *See United*
4 *States v. Matthew Stickney*, 23-mj-00356, ECF Nos. 1 and 1-1. The Statement of Facts
5 submitted in support of that warrant is attached as Exhibit 1 and incorporated by
6 reference herein.

7 9. As laid out in the Statement of Facts, STICKEY was amongst the crowd of
8 rioters that entered the Capitol building without authorization on January 6, 2021, the day
9 on Congress had convened to certify the vote count of the Electoral College of the 2020
10 Presidential Election. Specifically, STICKEY breached the Capitol building via the
11 Parliamentarian Door and spent at least 15 minutes in the Capitol building.

12 **B. Probable Cause Regarding the Target Device**

13 **1. Seizure of the Target Device**

14 10. On December 15, 2023 United States Magistrate Judge Brian Tsuchida of
15 the United States District Court for the Western District of Washington issued a warrant
16 authorizing a search of STICKNEY's person for any digital device capable of containing
17 or reasonably could contain fruits, evidence, information, contraband, or instrumentalities
18 of the TARGET OFFENSES, including any smart phone or cellular telephone that law
19 enforcement had reason to believe belonged to STICKNEY. A copy of that search
20 warrant and the affidavit submitted in support thereof is attached as Exhibit 2 and
21 incorporated by reference herein.

22 11. On December 20, 2023, I, another FBI Special Agent, and a Task Force
23 Officer contacted STICKNEY at approximately 7:30 a.m. at the United States Customs
24 and Immigration Service office at 12500 Tukwila International Blvd in Seattle, WA. I
25 identified myself, and advised STICKNEY that he would be placed in custody for
26 unlawfully entering and remaining on U.S. Capitol grounds. After he was under arrest,
27 but before law enforcement had a chance to search or handcuff him, a Task Force Officer

1 watched as STICKNEY handed his property – to include the TARGET DEVICE – to his
2 wife, who was present with him. STICKNEY stated that the black phone was his, which
3 was distinguishable from his wife’s purple phone. When I asked STICKNEY’s wife for
4 his phone, she denied having it. She then began trying to film law enforcement using her
5 purple, sparkly phone. She then made a call on her purple, sparkly phone and set
6 STICKNEY’s black phone on the floor next to her, where I retrieved it. The background
7 wallpaper on STICKNEY’s black phone was a photo of him and his family. STICKNEY
8 provided the FBI with the security pin number to his phone. I unlocked the device using
9 the pin number STICKNEY had provided, placed the phone in airplane mode, and
10 collected the phone details for inventory purposes only.

11 12. STICKNEY’s attorney has since asked the government for the return of the
12 phone, and indicated that – according to STICKNEY – the phone was purchased well
13 after January 6, 2021.

14 **2. STICKNEY’s Use of the Target Device on January 6, 2021**

15 13. According to records obtained through search warrants served on Google
16 LLC, a mobile device associated with the email mattXXXstickney@gmail.com, that
17 listed the phone number 360-930-2065 as a recovery SMS number, was present at the
18 U.S. Capitol between 2:32 p.m. and 3:51 p.m. on January 6, 2021 (“Device 1” in Exhibits
19 1 and 2 and herein).

20 14. As illustrated in Image 1 below, the listed locations were entirely within
21 areas of the U.S. Capitol Grounds which were restricted on January 6, 2021.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27

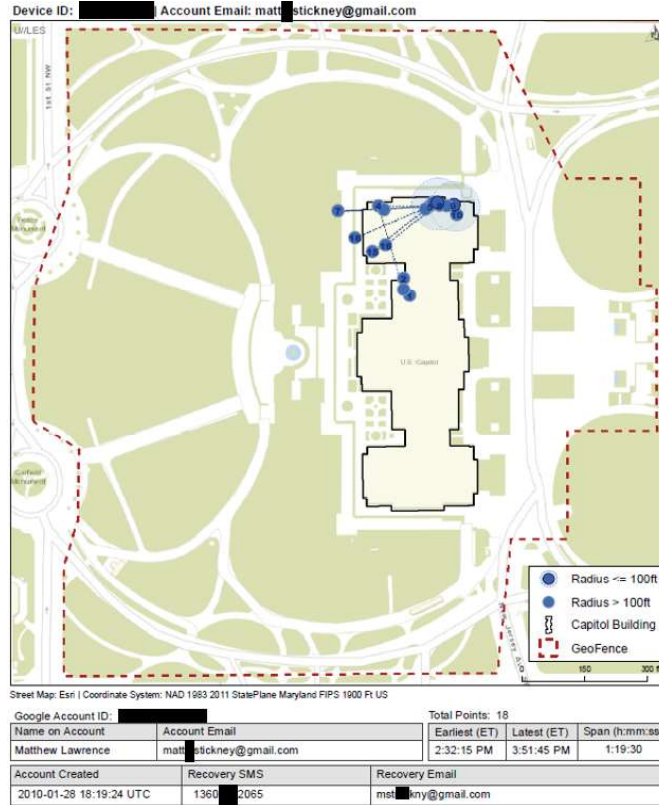


Image 1 – Location of Device 1 on January 6, 2021

15 Pursuant to a grand jury subpoena to Google LLC served on October 19,
16 2021, the Google voice number associated with the account associated with the email
17 mattXXXstickney@gmail.com (“Account 1” in Appendix A and herein) forwarded to the
18 360-930-2065 number. The Google voice greeting associated with that account says
19 “Matt Stickney.”

20 **3. Probable Cause that Evidence of the TARGET OFFENSES will**
21 **be found on the TARGET DEVICE**

22 16. Please see the affidavit submitted in support of the search warrant of
23 STICKNEY’s person (Exhibit 2) provides additional detail about how the TARGET
24 DEVICE was used on January 6, 2021, what evidence of the TARGET OFFENSES a
25 search of the TARGET DEVICE may yield, technical terms, computers,
26 electronic/magnetic storage, and forensic analysis, and methods to be used to search
27 digital devices. See Exhibit 2 ¶¶ 31-34, 45-55.

1 17. As described above and in Exhibits 1 and 2, there is evidence that
2 STICKNEY had in his possession a digital device while at the U.S. Capitol on January 6,
3 2021. In addition, based on photos and videos of the offenses that date, numerous persons
4 committing the TARGET OFFENSES possessed digital devices that they used to record
5 and post photos and videos of themselves and others committing those offenses.

6 18. I know, based on my training and experience, that when individuals obtain
7 new mobile phones, they often transfer their data from their old phone to their new
8 phone.

9 19. Based on my training and experience, and conversations I have had with
10 other law enforcement officers, it is common for individuals to back up or preserve
11 copies of digital media (such as photographs or videos) across multiple devices to prevent
12 loss.

13 20. I also know that during searches of phones belonging to others arrested in
14 connection to the January 6, 2021 riot on the U.S. Capitol, from early 2021 through
15 present, in multiple jurisdictions, law enforcement has recovered evidence of their (and
16 others') participation in criminal activity on January 6, 2021. This has even been the case
17 when the phone recovered was obtained after January 6, 2021. For example, in December
18 of 2021, the home of a defendant in the Middle District of Florida was searched. During
19 that search law enforcement recovered a cellphone that the defendant had obtained after
20 January 6, 2021, replacing the cellphone he had used on January 6, 2021 (which had
21 previously been seize by law enforcement). However, the replacement phone still
22 contained the defendant's videos and texts from the January 6, 2021 riot.

23 CONCLUSION

24 21. Based upon the above-referenced facts, your affiant asserts that there is
25 probable cause to believe that the TARGET DEVICE contains evidence of the TARGET
26 OFFENSE.

1 22. Based on the foregoing, I request that the Court issue the proposed search
2 warrant, pursuant to Federal Rule of Criminal Procedure 41.

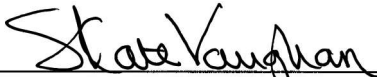
3 23. I further request that the Court permit the search warrant to be executed at
4 any time given that the TARGET DEVICE is contained on the premises of the Federal
5 Bureau of Investigation.

6 Respectfully submitted,

7 

8 Kenna M. Gonzales
9 Federal Bureau of Investigation

10
11 Affidavit submitted by email and attested to me as true and accurate by telephone,
12 consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) this 29th day of December, 2023.

13
14 
15 The Honorable S. Kate Vaughan
16 United States Magistrate Judge

ATTACHMENT A

Property to be searched

The property to be searched is specifically a Samsung Galaxy 22 Ultra, black in color, with a black Otterbox case, and the phone number 360-930-2065.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27

ATTACHMENT B

Property to be Seized

1
2
3 1. The items, information, and data to be seized are fruits, evidence, and
4 instrumentalities, in whatever form and however stored, of violations of 18 U.S.C. §
5 1752(a)(1) (entering or remaining in restricted buildings or grounds), 18 U.S.C. §
6 1752(a)(2) (disorderly and disruptive conduct in a restricted building or grounds), 40
7 U.S.C. § 5104(e)(2)(D) (disorderly or disruptive conduct in a Capitol building or
8 grounds), and 40 U.S.C. § 5104(e)(2)(G) (parading, demonstrating, or picketing in a
9 Capitol building or grounds) (the “TARGET OFFENSES”), as described in the search
10 warrant affidavit, including, but not limited to call logs, phone books, photographs, voice
11 mail messages, text messages, images and video, Global Positioning System data, and
12 any other stored electronic data that contain, constitute evidence of, document, establish,
13 identify, or reflect:

14 a. Establishing or documenting the commission of the TARGET
15 OFFENSES;

16 b. Identifying locations where the individual committed the TARGET
17 OFFENSES, traveled to before and after the commission of the TARGET OFFENSES,
18 and in preparation for the TARGET OFFENSES;

19 c. Reflecting the ownership and use of the item identified in
20 Attachment A by the individual committing the TARGET OFFENSES;

21 d. Documenting meetings and communications between individuals
22 committing one or more of the TARGET OFFENSES;

23 e. Reflecting communications between the individual committing one
24 or more of the TARGET OFFENSES and other individuals, discussing the commission
25 of one or more of the TARGET OFFENSES;

1 f. Reflecting communications between the individual committing one
2 or more of the TARGET OFFENSES and other individuals who may have assisted or
3 provided support in the commission of one or more of the TARGET OFFENSES;

4 g. Containing photographs or video that would constitute evidence of a
5 violation of the TARGET OFFENSES;

6 h. Evidence of any conspiracy, planning, or preparation to commit the
7 TARGET OFFENSES;

8 i. Evidence concerning efforts after the fact to conceal evidence of the
9 TARGET OFFENSES, or to flee prosecution for the same;

10 j. Evidence concerning materials, devices, or tools that were used to
11 unlawfully commit the TARGET OFFENSES;

12 k. Evidence of communication devices used in relation to the TARGET
13 OFFENSES;

14 l. Evidence of the state of mind of the subject in committing the
15 TARGET OFFENSES, e.g., intent, absence of mistake, or evidence indicating
16 preparation or planning, or knowledge and experience, related to the criminal activity
17 under investigation;

18 m. Evidence concerning the identity of persons who either (i)
19 collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the
20 criminal activity under investigation; or (ii) communicated with the unlawful actors about
21 matters relating to the criminal activity under investigation, including records that help
22 reveal their whereabouts;

23 n. Evidence concerning planning to unlawfully enter the U.S. Capitol,
24 including any maps or diagrams of the building or its internal offices;

25 o. Evidence concerning unlawful entry into the U.S. Capitol, including
26 any property of the U.S. Capitol;

1 p. Evidence concerning the official proceeding that was to take place at
2 Congress on January 6, 2021, i.e., the certification process of the 2020 Presidential
3 Election;

4 q. Evidence concerning efforts to obstruct, impede, or disrupt the
5 official proceeding that was to take place at Congress on January 6, 2021, i.e., the
6 certification process of the 2020 Presidential Election;

7 r. Evidence concerning the breach and unlawful entry of the United
8 States Capitol on January 6, 2021;

9 s. Evidence concerning the riot and/or civil disorder at the United
10 States Capitol on January 6, 2021;

11 t. Evidence concerning the assaults of federal officers/agents and
12 efforts to impede such federal officers/agents in the performance of their duties the
13 United States Capitol on January 6, 2021;

14 u. Evidence concerning damage to, or theft of, property at the United
15 States Capitol on January 6, 2021;

16 v. Evidence concerning awareness that the U.S. Capitol was closed to
17 the public on January 6, 2021;

18 w. Evidence of the subject's presence at the U.S. Capitol on or around
19 January 6, 2021;

20 x. Evidence concerning the results of, challenges to, or questions about
21 the legitimacy of the 2020 Presidential Election;

22 y. Evidence regarding travel to Washington, D.C. in or around January
23 2021, motive and intent for travel to Washington, D.C. in or around January 2021, the
24 planning of travel to and activity in Washington, D.C. on or about January 6, 2021,
25 research about the U.S. Capitol, and mode of travel, travel expenses, and travel logistics
26 on or about January 6, 2021;

27 z. Evidence regarding the riot at the U.S. Capitol on January 6, 2021;

1 aa. Records and information related to the email addresses, phone
2 numbers, social media, account identifiers used by perpetrators, aiders and abettors, co-
3 conspirators, and accessories after the fact concerning the TARGET OFFENSE;

4 bb. Evidence of who used, owned, or controlled the Device(s) at the
5 time the things described in this warrant were created, edited, or deleted, such as logs,
6 registry entries, configuration files, saved usernames and passwords, documents,
7 browsing history, user profiles, email, email contacts, chat, instant messaging logs,
8 photographs, and correspondence;

9 cc. Evidence of software, or the lack thereof, that would allow others to
10 control the Device(s), such as viruses, Trojan horses, and other forms of malicious
11 software, as well as evidence of the presence or absence of security software designed to
12 detect malicious software;

13 dd. Evidence of the attachment to the Device(s) of other storage devices
14 or similar containers for electronic evidence;

15 ee. Evidence of counter-forensic programs (and associated data) that are
16 designed to eliminate data from the Device(s);

17 ff. Evidence of the times the Device(s) was used;

18 gg. Passwords, encryption keys, and other access devices that may be
19 necessary to access the Device(s);

20 hh. Records of or information about Internet Protocol addresses used by
21 the Device(s); and

22 ii. Records of or information about the Device(s)'s Internet activity,
23 including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite"
24 web pages, search terms that the user entered into any Internet search engine, and records
25 of user-typed web addresses.

EXHIBIT 1

Case: 1:23-mj-00356
Assigned To : Harvey, G. Michael
Assign. Date : 12/15/2023
Description: Complaint W/ Arrest Warrant

Statement of Facts

Your affiant, Kenna M. Gonzales, is a Special Agent by the Federal Bureau of Investigation (FBI) and have been since September of 2022. Currently, I am assigned to the Seattle Field Office, where I am tasked with investigating domestic terrorism. As a Special Agent, I am authorized by law or by a government agency to engage in or supervise the prevention, detention, investigation, or prosecution of a violation of Federal criminal laws.

Background: Events at the U.S. Capitol on January 6, 2021

The U.S. Capitol is secured 24 hours a day by U.S. Capitol Police. Restrictions around the U.S. Capitol include permanent and temporary security barriers and posts manned by U.S. Capitol Police. Only authorized people with appropriate identification were allowed access inside the U.S. Capitol. On January 6, 2021, the exterior plaza of the U.S. Capitol was also closed to members of the public.

On January 6, 2021, a joint session of the United States Congress convened at the United States Capitol, which is located at First Street, SE, in Washington, D.C. 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 United States Capitol to certify the vote count of the Electoral College of the 2020 Presidential Election, which had taken place on November 3, 2020. The joint session began at approximately 1:00 p.m. 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.

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 U.S. Capitol Police were present and attempting to keep the crowd away from the Capitol building and the proceedings underway inside.

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 the U.S. Capitol Police attempted to maintain order and keep the crowd from entering the Capitol; however, around 2:00 p.m., individuals in the crowd forced entry into the U.S. Capitol, including by breaking windows and by assaulting members of the U.S. Capitol Police, as others in the crowd encouraged and assisted those acts.

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. Accordingly, the joint session of the United States Congress was effectively suspended until shortly after 8:00 p.m. Vice President Pence remained in the United States Capitol from the time he was evacuated from the Senate Chamber until the sessions resumed.

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.

Facts Specific to Matthew Lawrence Stickney

As set out in more detail below, based on my review of United States Capitol Police (“USCP”) surveillance and Metropolitan Police Department (“MPD”) body-worn camera footage, I have observed Matthew Lawrence Stickney among a large group of rioters who committed illegal acts on the ground of the U.S. Capitol as part of the January 6, 2021 riots there. Specifically, he illegally entered the U.S. Capitol grounds and building despite clearly marked signage and numerous other indicators that the area was closed to the public.

A. Identification of Stickney

According to records obtained through search warrants served on Google LLC, two mobile devices (“Device 1” and “Device 2”), both associated with the email mattXXXstickney@gmail.com, were present at the U.S. Capitol on January 6, 2021. Device 1 corresponds to a Google account (“Google Account 1”) for which the email is mattXXXstickney@gmail.com, the name is Matthew Lawrence, the recovery SMS number is the 2065 number, and the recovery email is mstXXXXkny@gmail.com. Device 2 corresponds to another Google account (“Google Account 2”) for which the email is mstickney.XXX@gmail.com, the name is Matt Stickney, the recovery SMS number begins with area code 206 ending in 4145 (the “4145 number”), and the recovery email mattXXXstickney@gmail.com.

Google estimates device location using sources including GPS data and information about nearby Wi-Fi access points and Bluetooth beacons. This location data varies in its accuracy, depending on the source(s) of the data. As a result, Google assigns a “maps display radius” for each location data point. Thus, where Google estimates that its location data is accurate to within 10 meters, Google assigns a “maps display radius” of 10 meters to the location data point. Finally, Google reports that its “maps display radius” reflects the actual location of the covered device approximately 68% of the time.

In this case, Google location data shows that Device 1 and Device 2 were present at the locations illustrated in Image 1 and Image 2, below. Device 1 and Device 2 were within the U.S. Capitol Grounds at locations reflected by each darker blue circle in Image 1 and Image 2, with the “maps display radius” reflected by each lighter blue ring around each darker blue circle. As illustrated in Image 1 and Image 2, the listed locations encompass areas that are at least partially within the U.S. Capitol Building between approximately 2:29:19 p.m. and 4:04:54 p.m. on January 6, 2021. In addition, as illustrated in Image 1 and Image 2, the listed locations were entirely within areas of the U.S. Capitol Grounds which were restricted on January 6, 2021.

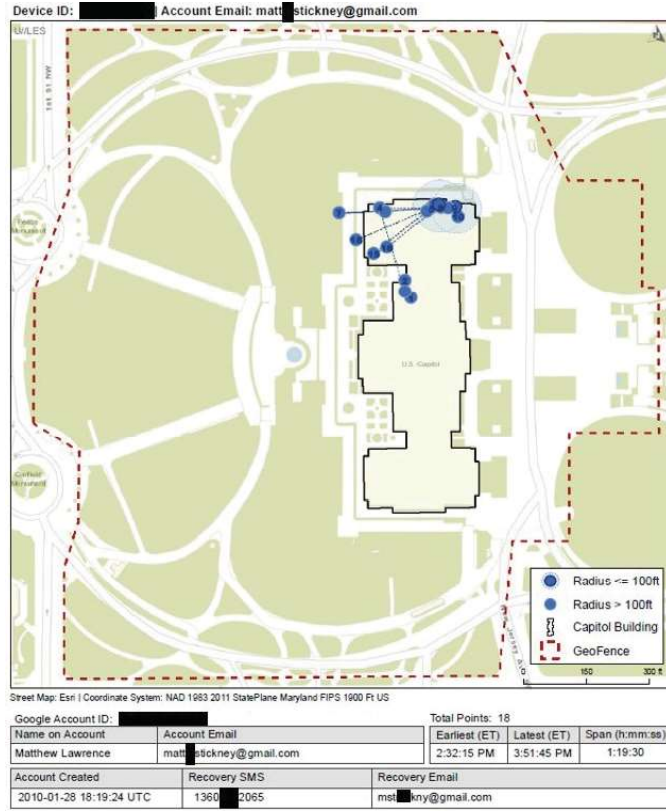


Image 1 – Location of Device 1 on January 6, 2021

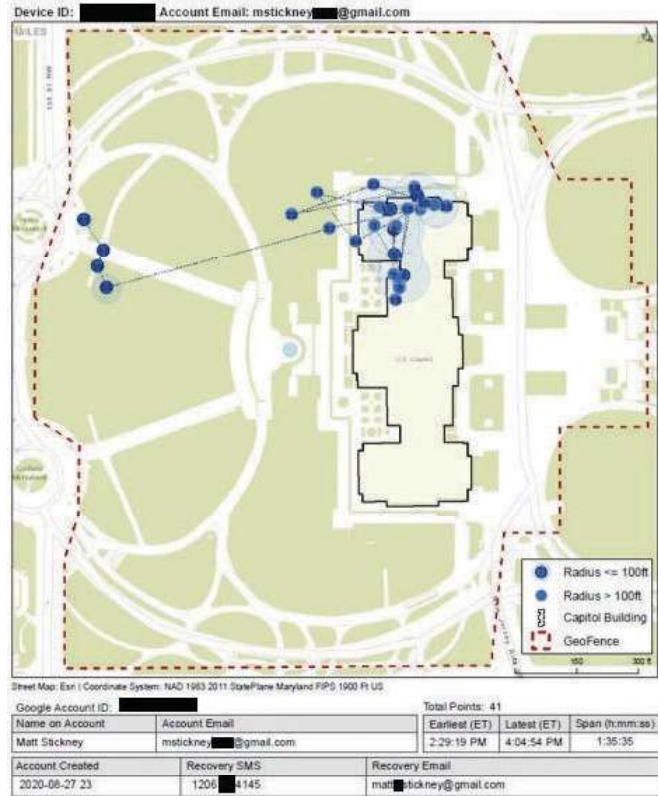


Image 2 – Location of Device 2 on January 6, 2021

Pursuant to a grand jury subpoena to Google LLC served on October 19, 2021, the Google voice number associated with Account 1 forwarded to the 2065 number. The Google voice greeting associated with that account says “Matt Stickney.”

Pursuant to a grand jury subpoena to Verizon Wireless served on June 21, 2021, the account related to 4145 number was subscribed to by an individual other than Stickney, with a business name of “Alexandria Real Estate” in Pasadena, CA. “Matt Stickney” was listed as the “contact” name, at an address in Seattle, WA (the “Seattle Address”).

The Seattle Address is listed on the website for Alexandria Real Estate Equities. On his publicly available LinkedIn page, Matthew Stickney of Mountlake Terrace, Washington indicates that he was a Maintenance Technician at Alexandria Real Estate Equities, Inc. from August 2020-July 2022. The LinkedIn profile photo appears to match Matthew Lawrence Stickney’s Washington driver’s license photo and the images from the U.S. Capitol on January 6, 2021.



Image 3 – Stickney’s LinkedIn Photo

In June 2021, the FBI identified a video originally posted to a user’s Instagram story depicting a person resembling Stickney inside the Capitol. The FBI contacted a personal associate of Stickney (“Witness 1”) and showed Witness 1 Image 4, below. Witness 1 pointed out Stickney as the individual depicted in the yellow circle below. In particular, Witness 1 stated that since the photo was not great, Witness 1 could not know for sure, but said that the person certainly looked like Stickney.



Image 4 – Instagram Story Depicting Stickney

B. Stickney’s Conduct on January 6, 2021

Based on my review of USCP surveillance and body-worn camera footage from January 6, 2021, I have learned that, on that day, Stickney was wearing a black jacket with a gray hooded sweatshirt underneath, a black backpack, and dark pants, as depicted below.



Image 5 – Stickney in the U.S. Capitol on January 6, 2021

USCP surveillance footage shows Stickney entering the U.S. Capitol building through the Parliamentarian Door at approximately 2:45:09 p.m. Stickney puts his hands to his mouth and shouts something down the hall as he enters room S131 shortly thereafter, at 2:45:17 p.m.



Image 6 – Stickney Yelling Inside the U.S. Capitol

Following this, Stickney exits S131 at 2:48:17 p.m., briefly turns around to go look into S131 at 2:48:22 p.m., and then turns back around. Stickney exits the camera's view, proceeding down the hall to the north, further into the U.S. Capitol Building, at 2:49:12 p.m.

Stickney is visible in that hallway again, on both USCP surveillance footage and MPD body-worn camera, at 3:00:56 p.m. His gray hood is pulled down, he is carrying an American flag, and being directed towards the Parliamentarian Door by police.



Image 7 – Stickney Carrying American Flag Inside U.S. Capitol on January 6, 2021

At 3:01:42 p.m. Stickney leans the flag against the door of the Parliamentarian's Office (S132) and leaves it there before continuing to exit the Capitol. He pulls his gray hood back over his head and exits the U.S. Capitol at 3:01:51 p.m.



Images 8 & 9 – Stickney Inside the U.S. Capitol on January 6, 2021

According to records obtained through the follow-up search warrant served on Google LLC, the Google account associated with the email address mattXXXstickney@gmail.com, belonging to Matthew Lawrence Stickney – Google Account 1 – made a number of internet search queries and views relevant to Stickney’s planning, travel, and participation in the events at the U.S. Capitol on January 6, 2021 in Washington D.C. These occurred both before and after that date. (The following does not represent the entirety of Stickney’s search history.):

Searched for hilton garden inn washington dc/u.s. capitol¹
Dec 24, 2020, 5:46:41 PM UTC

Viewed Hilton Garden Inn Washington DC/U.S. Capitol²
Dec 24, 2020, 5:46:41 PM UTC

Searched for hotels in washington
Dec 24, 2020, 5:46:30 PM UTC

Searched for how do i take my gun with me on a flight
Dec 24, 2020, 8:09:20 PM UTC

Searched for is weed legal in d.c.
Dec 28, 2020, 5:04:52 AM UTC

¹ In the context of this search history, if Stickney “searched for” X, it means that an individual logged in to the mattXXXstickney@gmail.com completed a Google internet search query for the term in question.

² In the context of this search history, if Stickney “viewed” X, it means an individual logged in to the mattXXXstickney@gmail.com visited the named website.

Viewed AC Hotel by Marriott Washington DC Downtown
Jan 3, 2021, 2:24:01 AM UTC

Searched for can i bring a gas mask on a plane
Jan 4, 2021, 4:06:24 AM UTC

Searched for can i bring walkie talkies on a plane
Jan 4, 2021, 4:06:16 AM UTC

Searched for can i carry a knife on a plane
Jan 4, 2021, 5:32:37 AM UTC

Searched for boy that escalated quickly³
Jan 6, 2021, 9:12:36 PM UTC

Searched for hands burning from pepper spray
Jan 7, 2021, 3:12:56 AM UTC

Searched for hd security cameras
Jan 7, 2021, 6:29:33 PM UTC

Searched for cs gas
Jan 9, 2021, 12:18:46 AM UTC

Searched for us capitol
Jan 10, 2021, 9:15:54 AM UTC

Pursuant to a grand jury subpoena to Delta Airlines, Matthew Stickney associated with the email address mattXXXstickney@gmail.com and the 2065 number was listed as a passenger on flights that would have put him in the Washington D.C. Metro area on January 6, 2021. He purchased these trips on December 24, 2020. Specifically, he was listed as a passenger on the following flights:

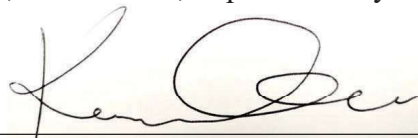
- Delta flight number 356, departing from Seattle-Tacoma International Airport (SEA) at 11:30 p.m. on January 4, 2021, arriving at Atlanta Hartsfield Jackson International Airport (ATL) at 6:57 a.m. on January 5, 2021.
- Delta flight number 1411, departing from ATL at 8:05 a.m. on January 5, 2021, arriving at Baltimore-Washington International Airport (BWI) at 9:46 a.m. on January 5, 2021.
- Delta flight number 1411, departing BWI at 11:01 a.m. on January 7, 2021, arriving at ATL at 12:55 p.m. on January 7, 2021.
- Delta flight number 2123, departing ATL at 1:40 p.m. on January 7, 2021, arriving at SEA at 4:05 p.m. on January 7, 2021.

Based on the foregoing, your affiant submits that there is probable cause to believe that Matthew Lawrence Stickney violated 18 U.S.C. § 1752(a)(1) and (2), which make it a crime to (1) knowingly enter or remain in any restricted building or grounds without lawful authority to do;

³ “Boy, that escalated quickly” is a reference from the 2004 film “Anchorman: The Legend of Ron Burgundy” to a fight that got out of hand, resulting in serious injury and death to some participants.

and (2) knowingly, and with intent to impede or disrupt the orderly conduct of Government business or official functions, engage in disorderly or disruptive conduct in, or within such proximity to, any restricted building or grounds when, or so that, such conduct, in fact, impedes or disrupts the orderly conduct of Government business or official functions. For purposes of Section 1752 of Title 18, a “restricted building” includes a posted, cordoned off, or otherwise restricted area of a building or grounds where the President or other person protected by the Secret Service, including the Vice President, is or will be temporarily visiting; or any building or grounds so restricted in conjunction with an event designated as a special event of national significance.

Your affiant submits there is also probable cause to believe that Matthew Lawrence Stickney violated 40 U.S.C. § 5104(e)(2)(D) and (G), which make it a crime to willfully and knowingly (D) utter loud, threatening, or abusive language, or engage in disorderly or disruptive conduct, at any place in the Grounds or in any of the Capitol Buildings with the intent to impede, disrupt, or disturb the orderly conduct of a session of Congress or either House of Congress, or the orderly conduct in that building of a hearing before, or any deliberations of, a committee of Congress or either House of Congress; and (G) parade, demonstrate, or picket in any of the Capitol Buildings.



Special Agent Kenna M. Gonzales
Federal Bureau of Investigation

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone, this 15th day of December 2023.

**G. Michael
Harvey**



Digitally signed by G.
Michael Harvey
Date: 2023.12.15
10:53:42 -05'00'

Judge G. Michael Harvey

U.S. MAGISTRATE JUDGE

EXHIBIT 2

UNITED STATES DISTRICT COURT

for the

Western District of Washington



In the Maner of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
The Person of Matthew Lawrence Stickney, more fully described in Attachment A

Case No. MJ23-600

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Person Matthew Lawrence Stickney, more fully described in Attachment A, incorporated herein by reference.

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

See Attachment B, incorporated herein by reference.

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

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

The search is related to aviolation of:

Table with 2 columns: Code Section, Offense Description. Rows include 18 U.S.C. § 1752(a)(1), (a)(2) and 40 U.S.C. § 5104(3)(2)(D), (G).

The application is based on these facts:

See Affidavit of Special Agent Jared Gibb, 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. § 3103j, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: [i] by reliable electronic means: telephonically recorded.

Applicant's signature
Kenna M. Gonzales, Special Agent
Printed name and title

The foregoing affidavit was sworn to before me and signed in my presence, or
The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 12/15/2023

Judge's signature
Brian A. Tsuchida, United States Magistrate Judge
Printed name and title

City and state: Seattle, Washington

AFFIDAVIT OF KENNA M. GONZALES

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I, Kenna M. Gonzales, being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property, any digital device which is capable of containing or reasonably could contain fruits, evidence, information, contraband, or instrumentalities described in paragraph 1 of Attachment B, specifically including any smart phone(s) and/or cellular telephone(s) that law enforcement has reason to believe belong to STICKNEY (hereinafter, the “TARGET DEVICE(s)”), as described in Attachment A. Such a search would include an examination of the TARGET DEVICE(s) for information described in Attachment B.

2. Unless otherwise noted, wherever in this affidavit I assert that a statement was made, that statement is described in substance and is not intended to be a verbatim recitation of such statement. Wherever in this affidavit I quote statements, those quotations have been taken from draft transcripts, which are subject to further revision.

3. Unless otherwise stated, the conclusions and beliefs I express in this affidavit are based on my training, experience, and knowledge of the investigation, and reasonable inferences I’ve drawn from my training, experience, and knowledge of the investigation.

AFFIANT BACKGROUND

4. Your affiant, Kenna M. Gonzales, is a Special Agent by the Federal Bureau of Investigation (FBI) and have been since September of 2022. Currently, I am assigned to the Seattle Field Office, where I am tasked with investigating domestic terrorism. As a

1 Special Agent, I am authorized by law or by a government agency to engage in or supervise
2 the prevention, detention, investigation, or prosecution of a violation of Federal criminal
3 laws. As such, I am an “investigative or law enforcement officer” of the United States
4 within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of
5 the United States who is empowered by law to conduct investigations of, and to make
6 arrests for, offenses enumerated in Section 2516 of Title 18, United States Code.

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

12 6. Based on my training and experience and the facts set forth in this affidavit,
13 I respectfully submit that there is probable cause to believe that violations of: 18 U.S.C. §
14 1752(a)(1) (entering or remaining in restricted buildings or grounds); 18 U.S.C. §
15 1752(a)(2) (disorderly and disruptive conduct in a restricted building or grounds); 40
16 U.S.C. § 5104(e)(2)(D) (disorderly or disruptive conduct in the Capitol Buildings); and 40
17 U.S.C. § 5104(e)(2)(G) (parading, demonstrating, or picketing in a Capitol Building) (the
18 “TARGET OFFENSES”) have occurred. There is also probable cause to search the
19 TARGET DEVICE(s), further described in Attachment A, for the things described in
20 Attachment B.

21 **PROBABLE CAUSE**

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

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

1 8. At the U.S. Capitol, the building itself has 540 rooms covering 175,170
2 square feet of ground, roughly four acres. The building is 751 feet long (roughly 228
3 meters) from north to south and 350 feet wide (106 meters) at its widest point. The U.S.
4 Capitol Visitor Center is 580,000 square feet and is located underground on the east side
5 of the Capitol. On the west side of the Capitol building is the West Front, which includes
6 the inaugural stage scaffolding, a variety of open concrete spaces, a fountain surrounded
7 by a walkway, two broad staircases, and multiple terraces at each floor. On the East Front
8 are three staircases, porticos on both the House and Senate side, and two large skylights
9 into the Visitor’s Center surrounded by a concrete parkway. All of this area was barricaded
10 and off limits to the public on January 6, 2021.

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

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

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

26 12. As the proceedings continued in both the House and the Senate, and with
27 Vice President Mike Pence present and presiding over the Senate, a large crowd gathered

1 outside the U.S. Capitol. As noted above, temporary and permanent barricades were in
2 place around the exterior of the U.S. Capitol building, and USCP were present and
3 attempting to keep the crowd away from the Capitol building and the proceedings
4 underway inside.

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

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

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

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

26 17. Beginning shortly after 2:00 p.m. EST, individuals in the crowd forced entry
27 into the U.S. Capitol, including by breaking windows and by assaulting members of law

1 enforcement, as others in the crowd encouraged and assisted those acts. Publicly available
 2 video footage shows an unknown individual saying to a crowd outside the Capitol building,
 3 “We’re gonna fucking take this,” which your affiant believes was a reference to “taking”
 4 the U.S. Capitol.



18 18. Once inside, the subjects broke windows and doors, destroyed property,
 19 stole property, and assaulted federal police officers. Many of the federal police officers
 20 were injured and several were admitted to the hospital. The subjects also confronted and
 21 terrorized members of Congress, Congressional staff, and the media. The subjects
 22 carried weapons including tire irons, sledgehammers, bear spray, and tasers. They also
 23 took police equipment from overrun police including shields and police batons. At least
 24 one of the subjects carried a handgun with an extended magazine.

25 19. Between approximately 2:10 p.m, EST and 2:30 p.m. EST, Vice President
 26 Pence evacuated the Senate Chamber, and the Senate and House of Representatives were
 27

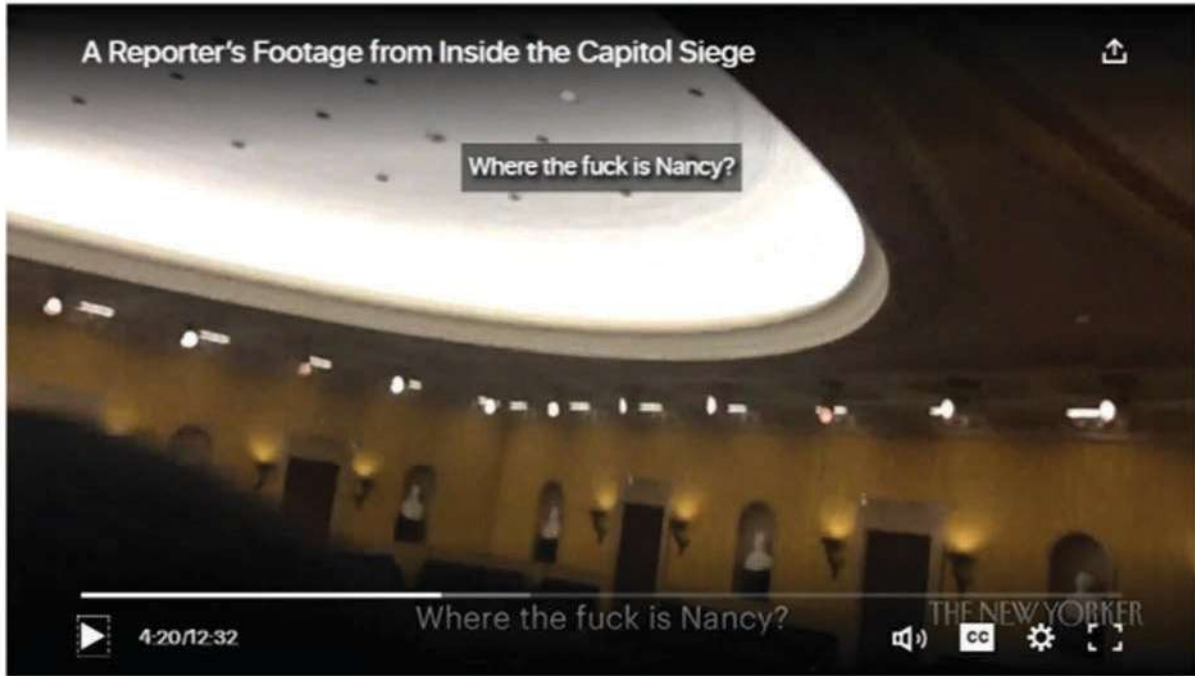
1 locked down and went into recess. Both the Senate and the House of Representatives
2 Chamber were evacuated.

3 20. As the subjects attempted to break into the House chamber, by breaking the
4 windows on the chamber door, law enforcement were forced to draw their weapons to
5 protect the victims sheltering inside. At around 2:45 p.m. EST, subjects broke into the
6 office of House Speaker Nancy Pelosi.

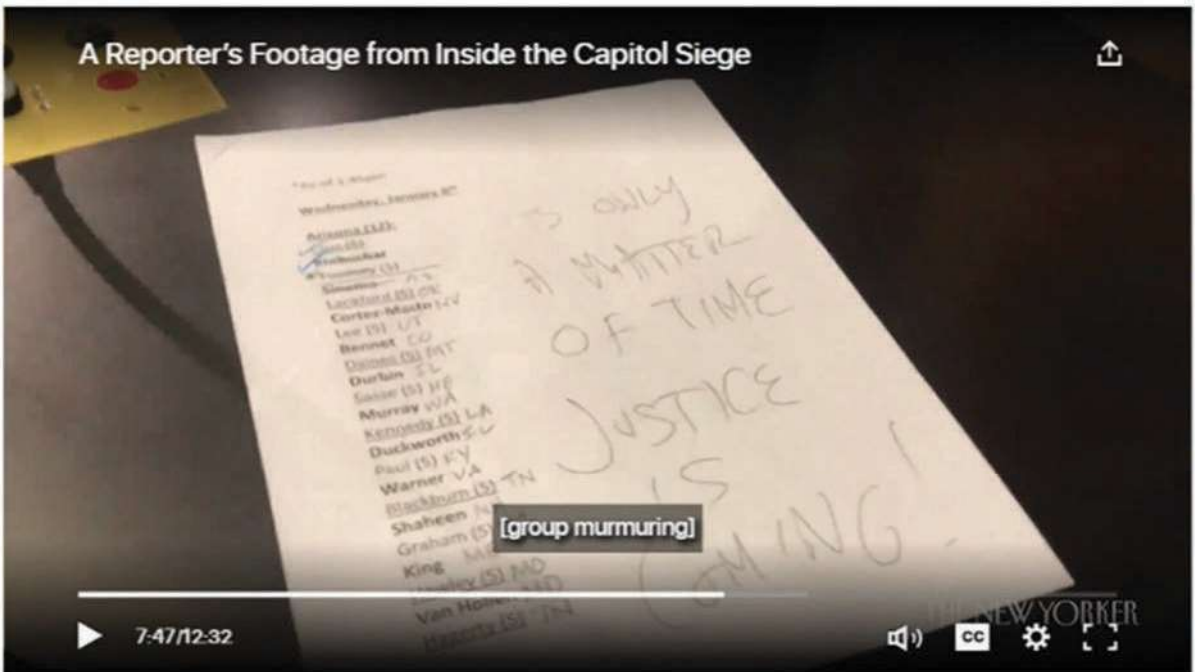
7 21. At around 2:47 p.m. EST, subjects broke into the Senate Chamber not long
8 after I had been evacuated. Publicly available video shows an individual asking, “Where
9 are they?” as they opened up the door to the Senate Chamber. Based upon the context, law
10 enforcement believes that the word “they” is in reference to members of Congress.



22 22. After subjects forced entry into the Senate Chamber, publicly available video
23 shows that an individual asked, “Where the fuck is Nancy?” Based upon other comments
24 and the context, law enforcement believes that the “Nancy” being referenced was the
25 Speaker of the House of Representatives, Nancy Pelosi.
26
27



23. One 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."



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





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

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. EST 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

1 building had been secured. Vice President Pence remained in the United States Capitol
2 from the time he was evacuated from the Senate Chamber until the session resumed.

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

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

7 32. Both chambers of Congress met and worked on the Certification within the
8 Capitol building until approximately 3:00 a.m. EST on January 7, 2021.

9 ***The Use of Electronic Devices at the U.S. Capitol on January 6, 2021***

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

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

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

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



18
19
20
21
22
23
24
25
26
27

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



21
22

STICKNEY's Actions at the U.S. Capitol on January 6, 2021

23 37. According to records obtained through search warrants served on Google
24 LLC, two mobile devices (“Device 1” and “Device 2”), both associated with the email

25
26 ² <https://www.businessinsider.com/republicans-objecting-to-electoral-votes-in-congress-live-updates-2021-1>.

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

1 mattXXXstickney@gmail.com, were present at the U.S. Capitol on January 6, 2021.
2 Device 1 corresponds to a Google account (“Google Account 1”) for which the email is
3 mattXXXstickney@gmail.com, the name is Matthew Lawrence, the recovery SMS number
4 is the 2065 number, and the recovery email is mstXXXXkny@gmail.com. Device 2
5 corresponds to another Google account (“Google Account 2”) for which the email is
6 mstickney.XXX@gmail.com, the name is Matt Stickney, the recovery SMS number begins
7 with area code 206 ending in 4145 (the “4145 number”), and the recovery email
8 mattXXXstickney@gmail.com.

9 38. Google estimates device location using sources including GPS data and
10 information about nearby Wi-Fi access points and Bluetooth beacons. This location data
11 varies in its accuracy, depending on the source(s) of the data. As a result, Google assigns a
12 “maps display radius” for each location data point. Thus, where Google estimates that its
13 location data is accurate to within 10 meters, Google assigns a “maps display radius” of 10
14 meters to the location data point. Finally, Google reports that its “maps display radius”
15 reflects the actual location of the covered device approximately 68% of the time.

16 39. In this case, Google location data shows that the Device was present at the
17 locations illustrated in Image 1, below. The Device was within the U.S. Capitol Grounds
18 at locations reflected by each darker blue circle in Image 1, with the “maps display radius”
19 reflected by each lighter blue ring around each darker blue circle. As illustrated in Image
20 1, the listed locations encompass areas that are at least partially within the U.S. Capitol
21 Building between approximately 2:29:19 p.m. and 4:04:54 p.m. on January 6, 2021. In
22 addition, as illustrated in Image 1, the listed locations were entirely within areas of the U.S.
23 Capitol Grounds which were restricted on January 6, 2021.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27

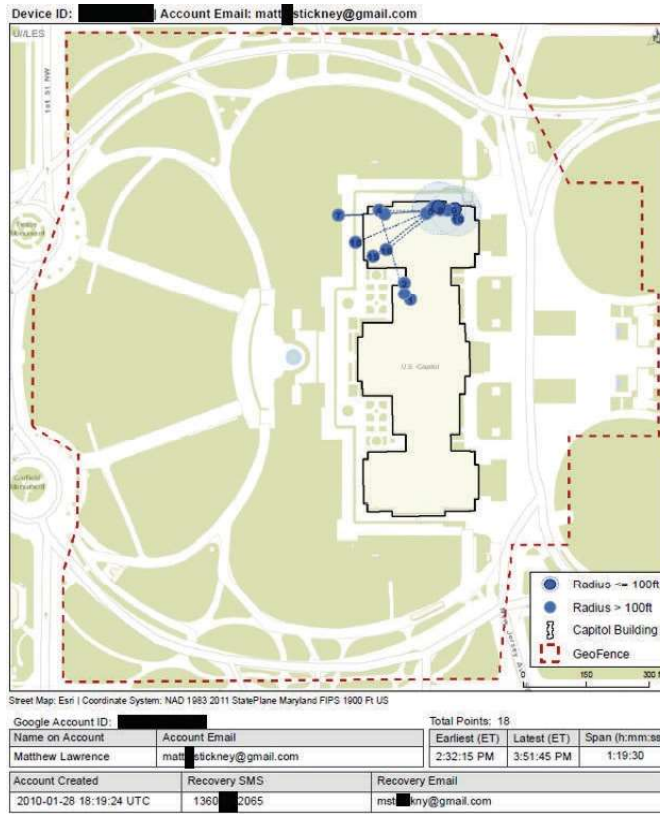


Image 1 – Location of Device 1 on January 6, 2021

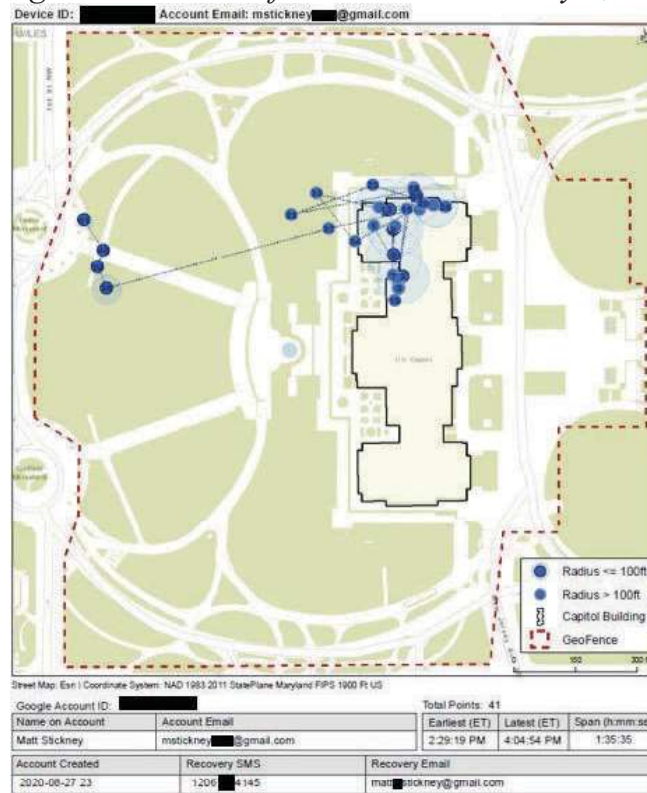


Image 2 – Location of Device 2 on January 6, 2021

1 40. Pursuant to a grand jury subpoena to Google LLC served on October 19,
2 2021, the Google voice number associated with Account 1 forwarded to the 2065
3 number. The Google voice greeting associated with that account says “Matt Stickney.”

4 41. Pursuant to a grand jury subpoena to Verizon Wireless served on June 21,
5 2021, the account related to 4145 number was subscribed to by an individual other than
6 Stickney, with a business name of “Alexandria Real Estate” in Pasadena, CA. “Matt
7 Stickney” was listed as the “contact” name, at an address in Seattle, WA (the “Seattle
8 Address”).

9 42. The Seattle Address is listed on the website for Alexandria Real Estate
10 Equities. On his publicly available LinkedIn page, Matthew Stickney of Mountlake
11 Terrace, Washington indicates that he was a Maintenance Technician at Alexandria Real
12 Estate Equities, Inc. from August 2020-July 2022. The LinkedIn profile photo appears to
13 match Matthew Lawrence Stickney’s Washington driver’s license photo and the images
14 from the U.S. Capitol on January 6, 2021.



Image 3 – Stickney’s LinkedIn Photo

1 43. In June 2021, the FBI identified video originally posted to a user’s Instagram
2 story depicting a person resembling Stickney inside the Capitol. The FBI contacted a
3 personal associate of Stickney (“Witness 1”) and showed Witness 1 Image 4, below.
4 Witness 1 pointed out Stickney as the individual depicted in the yellow circle below. In
5 particular, Witness 1 stated that since the photo was not great, Witness 1 could not know
6 for sure, but said that the person certainly looked like Stickney.



19 *Image 4 – Instagram Story Depicting Stickney*

20 44. Based on my review of USCP surveillance and body-worn camera footage
21 from January 6, 2021, I have learned that, on that day, Stickney was wearing a black
22 jacket with a gray hooded sweatshirt underneath, a black backpack, and dark pants, as
23 depicted below.



11 *Image 5 – Stickney in the U.S. Capitol on January 6, 2021*

12
13 45. USCP surveillance footage shows Stickney entering the U.S. Capitol
14 building through the Parliamentarian Door at approximately 2:45:09 p.m. Stickney puts
15 his hands to his mouth and shouts something down the hall as he enters room S131
16 shortly thereafter, at 2:45:17 p.m.



Image 6 – Stickney Yelling Inside the U.S. Capitol

1 46. Following this, Stickney exits S131 at 2:48:17 p.m., briefly turns around to
2 go look into S131 at 2:48:22 p.m., and then turns back around. Stickney exits the
3 camera's view, proceeding down the hall to the north, further into the U.S. Capitol
4 Building, at 2:49:12 p.m.

5 47. Stickney is visible in that hallway again, on both USCP surveillance
6 footage and MPD body-worn camera, at 3:00:56 p.m. His gray hood is pulled down, he is
7 carrying an American flag, and being directed towards the Parliamentarian Door by
8 police.



9
10
11
12
13
14
15
16
17
18
19
20 *Image 7 – Stickney Carrying American Flag Inside U.S. Capitol on January 6, 2021*

21 48. At 3:01:42 p.m. Stickney leans the flag against the door of the
22 Parliamentarian's Office (S132) and leaves it there before continuing to exit the Capitol.
23 He pulls his gray hood back over his head and exits the U.S. Capitol at 3:01:51 p.m.



Images 8 & 9 – Stickney Inside the U.S. Capitol on January 6, 2021

49. According to records obtained through the follow-up search warrant served on Google LLC, the Google account associated with the email address mattXXXstickney@gmail.com, belonging to Matthew Lawrence Stickney – Google Account 1 – made a number of internet search queries and views relevant to Stickney’s planning, travel, and participation in the events at the U.S. Capitol on January 6, 2021 in Washington D.C. These occurred both before and after that date. (The following does not represent the entirety of Stickney’s search history.):

Searched for hilton garden inn washington dc/u.s. capitol⁴
Dec 24, 2020, 5:46:41 PM UTC

Viewed Hilton Garden Inn Washington DC/U.S. Capitol⁵
Dec 24, 2020, 5:46:41 PM UTC

Searched for hotels in washington
Dec 24, 2020, 5:46:30 PM UTC

Searched for how do i take my gun with me on a flight
Dec 24, 2020, 8:09:20 PM UTC

⁴ In the context of this search history, if Stickney “searched for” X, it means that an individual logged in to the mattXXXstickney@gmail.com completed a Google internet search query for the term in question.

⁵ In the context of this search history, if Stickney “viewed” X, it means an individual logged in to the mattXXXstickney@gmail.com visited the named website.

1 Searched for is weed legal in d.c.
Dec 28, 2020, 5:04:52 AM UTC
2 Viewed AC Hotel by Marriott Washington DC Downtown
3 Jan 3, 2021, 2:24:01 AM UTC
4 Searched for can i bring a gas mask on a plane
5 Jan 4, 2021, 4:06:24 AM UTC
6 Searched for can i bring walkie talkies on a plane
7 Jan 4, 2021, 4:06:16 AM UTC
8 Searched for can i carry a knife on a plane
9 Jan 4, 2021, 5:32:37 AM UTC
10 Searched for boy that escalated quickly⁶
11 Jan 6, 2021, 9:12:36 PM UTC
12 Searched for hands burning from pepper spray
13 Jan 7, 2021, 3:12:56 AM UTC
14 Searched for hd security cameras
15 Jan 7, 2021, 6:29:33 PM UTC
16 Searched for cs gas
17 Jan 9, 2021, 12:18:46 AM UTC
18 Searched for us capitol
19 Jan 10, 2021, 9:15:54 AM UTC

20 50. Pursuant to a grand jury subpoena to Delta Airlines, Matthew Stickney
21 associated with the email address mattXXXstickney@gmail.com and the 2065 number
22 was listed as a passenger on flights that would have put him in the Washington D.C.
23 Metro area on January 6, 2021. He purchased these trips on December 24, 2020.
24 Specifically, he was listed as a passenger on the following flights:

- 25 - Delta flight number 356, departing from Seattle-Tacoma International Airport
26 (SEA) at 11:30 p.m. on January 4, 2021, arriving at Atlanta Hartsfield Jackson
27 International Airport (ATL) at 6:57 a.m. on January 5, 2021.

6 “Boy, that escalated quickly” is a reference from the 2004 film “Anchorman: The Legend of Ron Burgundy” to a fight that got out of hand, resulting in serious injury and death to some participants.

- 1 - Delta flight number 1411, departing from ATL at 8:05 a.m. on January 5, 2021,
2 arriving at Baltimore-Washington International Airport (BWI) at 9:46 a.m. on
3 January 5, 2021.
- 4 - Delta flight number 1411, departing BWI at 11:01 a.m. on January 7, 2021,
5 arriving at ATL at 12:55 p.m. on January 7, 2021.
- 6 - Delta flight number 2123, departing ATL at 1:40 p.m. on January 7, 2021, arriving
7 at SEA at 4:05 p.m. on January 7, 2021.

THE TARGET DEVICE

8 51. As described above, there is evidence that STICKNEY had in his possession
9 a digital device while at the U.S. Capitol on January 6, 2021. In addition, based on photos
10 and videos of the offenses that date, numerous persons committing the TARGET
11 OFFENSES possessed digital devices that they used to record and post photos and videos
12 of themselves and others committing those offenses.

13 52. Further, based on the investigation, numerous persons committing the
14 TARGET OFFENSES possessed digital devices to plan their attendance in Washington
15 D.C. on January 6, 2021, to coordinate with other participants at the gatherings there that
16 day, to take, send, and receive photographs and videos relating to events at the U.S. Capitol
17 and in Washington D.C. on January 6; and to communicate and post on social media and
18 digital forums about the events of January 6 after they occurred. This information can: (i)
19 reflect the preparation for, arrangement of, and commission of the TARGET OFFENSES;
20 (ii) identify the subject's presence at locations relevant to the TARGET OFFENSES; (iii)
21 reflect the ownership and use of the cellular telephones by persons involved in the
22 commission of the TARGET OFFENSES; (iv) document meetings and communications
23 between associates and co-conspirators; (v) demonstrate the subject's planning,
24 preparation, motive, and intent regarding the TARGET OFFENSES.

25 53. Moreover, it is well-known that virtually all adults in the United States use
26 mobile digital devices. In a fact sheet from June 12, 2019, The Pew Research Center for
27 Internet & Technology estimated that 96% of Americans owned at least one cellular phone,

1 and that that same 2019 report estimated that 81% of Americans use at least one
2 smartphone. See Mobile Fact Sheet, [https://www.pewresearch.org/internet/fact-](https://www.pewresearch.org/internet/fact-sheet/mobile/)
3 [sheet/mobile/](https://www.pewresearch.org/internet/fact-sheet/mobile/) (last visited Jan. 9, 2021).

4 54. I also know, based on my training and experience, that cell phones are
5 expensive, and people routinely retain their cell phones for many months or years. I also
6 know that, when individuals obtain new mobile phones, they often transfer their data from
7 their old phone to their new phone.

8 55. Based on my training and experience, individuals often carry cellular
9 telephones on their persons.

10 56. Based on my training and experience, and on conversations I have had with
11 other law enforcement officers, I also know that some individuals who participate in
12 activities aimed at disrupting or interfering with governmental and/or law enforcement
13 operations have been known to use anonymizing services and/or applications capable of
14 encrypting communications to protect their identity and communications. By using such
15 tools, in some cases, the only way to see the content of these conversations is on the
16 electronic device that had been used to send or receive the communications.

17 57. In my training and experience, individuals frequently post messages to social
18 media sites, like Facebook and Instagram, using a cellular telephone. Many subjects who
19 committed offenses at the U.S. Capitol on January 6, 2021 documented their offenses on
20 social media.

21 58. I know that any Device(s) belonging to STICKNEY may have location
22 services that could show STICKNEY's location on January 6, 2021, and his travels to and
23 from Washington D.C. Based on my experience, I know that subjects sometimes delete
24 their location data in an attempt to conceal their prior movements. However, I also know
25 that deleted items may be recoverable if they still reside in the digital device's storage. Any
26 Devices belonging to STICKNEY are likely to contain other types of location information,
27 including but not limited to geolocation data associated with photographs, which my

1 identify a user's location during a specific time period relevant to the TARGET
2 OFFENSES, such as during the breach of the U.S. Capitol.

3 59. Based on my training and experience, and conversations I have had with
4 other law enforcement officers, it is common for individuals to back up or preserve copies
5 of digital media (such as photographs or videos) across multiple devices to prevent loss.

6 60. Your affiant knows that cellular telephones contain valuable information and
7 evidence relating to violations of the TARGET OFFENSES. Such information consists of,
8 but is not limited to: call logs, phone books, photographs, voice mail messages, text
9 messages, images and video, Global Positioning System data, and any other stored
10 electronic data. This information can: (i) reflect the preparation for, arrangement of, and
11 commission of violations of the TARGET OFFENSES; (ii) identify locations relevant to
12 the TARGET OFFENSES; (iii) reflect the ownership and use of the cellular telephones by
13 persons involved in the commission of the TARGET OFFENSES; (iv) document meetings
14 and communications between associates, and co-conspirators of violations of the TARGET
15 OFFENSES.

16 61. Additionally, evidence from the TARGET DEVICE may yield ownership
17 information of the TARGET DEVICE(s). All of the aforementioned information would
18 further constitute evidence of the commission of the TARGET OFFENSES.

19 62. The warrant I am applying for would permit law enforcement to obtain from
20 certain individuals the display of physical biometric characteristics (such as fingerprint,
21 thumbprint, or facial characteristics) in order to unlock devices subject to search and
22 seizure pursuant to this warrant. I seek this authority based on the following:

23 a. I know from my training and experience, as well as from
24 information found in publicly available materials published by device manufacturers, that
25 many electronic devices, particularly newer mobile devices and laptops, offer their users
26 the ability to unlock the device through biometric features in lieu of a numeric or
27 alphanumeric passcode or password. These biometric features include fingerprint

1 scanners and facial recognition features. Some devices offer a combination of these
2 biometric features, and the user of such devices can select which features they would like
3 to utilize.

4 b. If a device is equipped with a fingerprint scanner, a user may enable
5 the ability to unlock the device through his or her fingerprints. For example, Apple offers
6 a feature called “Touch ID,” which allows a user to register up to five fingerprints that
7 can unlock a device. Once a fingerprint is registered, a user can unlock the device by
8 pressing the relevant finger to the device’s Touch ID sensor, which is found in the round
9 button (often referred to as the “home” button) located at the bottom center of the front of
10 the device. The fingerprint sensors found on devices produced by other manufacturers
11 have different names but operate similarly to Touch ID.

12 c. If a device is equipped with a facial recognition feature, a user may
13 enable the ability to unlock the device through his or her face, iris, or retina. For example,
14 Apple offers a facial recognition feature called “Face ID.” During the Face ID
15 registration process, the user holds the device in front of his or her face. The device’s
16 camera then analyzes and records data based on the user’s facial characteristics. The
17 device can then be unlocked if the camera detects a face with characteristics that match
18 those of the registered face. Facial recognition features found on devices produced by
19 other manufacturers have different names but operate similarly to Face ID.

20 d. While not as prolific on digital devices as fingerprint and facial-
21 recognition features, both iris and retina scanning features exist for securing devices/data.
22 The human iris, like a fingerprint, contains complex patterns that are unique and stable.
23 Iris recognition technology uses mathematical pattern-recognition techniques to map the
24 iris using infrared light. Similarly, retina scanning casts infrared light into a person’s eye
25 to map the unique variations of a person’s retinal blood vessels. A user can register one
26 or both eyes to be used to unlock a device with these features. To activate the feature, the
27 user holds the device in front of his or her face while the device directs an infrared light

1 toward the user's face and activates an infrared sensitive camera to record data from the
2 person's eyes. The device is then unlocked if the camera detects the registered eye.

3 e. In my training and experience, users of electronic devices often
4 enable the aforementioned biometric features because they are considered to be a more
5 convenient way to unlock a device than by entering a numeric or alphanumeric passcode
6 or password. Moreover, in some instances, biometric features are considered to be a more
7 secure way to protect a device's contents. This is particularly true when the users of a
8 device are engaged in criminal activities and thus have a heightened concern about
9 securing the contents of a device.

10 f. As discussed in this affidavit, based on my training and experience I
11 believe that one or more digital devices will be found during the search. The passcode or
12 password that would unlock the device(s) subject to search under this warrant is not
13 known to law enforcement. Thus, law enforcement personnel may not otherwise be able
14 to access the data contained within the device(s), making the use of biometric features
15 necessary to the execution of the search authorized by this warrant.

16 g. I also know from my training and experience, as well as from
17 information found in publicly available materials including those published by device
18 manufacturers, that biometric features will not unlock a device in some circumstances
19 even if such features are enabled. This can occur when a device has been restarted,
20 inactive, or has not been unlocked for a certain period of time. For example, Apple
21 devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed
22 since the device was last unlocked or (2) when the device has not been unlocked using a
23 fingerprint for 4 hours *and* the passcode or password has not been entered in the last 156
24 hours. Biometric features from other brands carry similar restrictions. Thus, in the event
25 law enforcement personnel encounter a locked device equipped with biometric features,
26 the opportunity to unlock the device through a biometric feature may exist for only a
27 short time.

1 h. In my training and experience, the person who is in possession of a
2 device or has the device among his or her belongings at the time the device is found is
3 likely a user of the device. However, in my training and experience, that person may not
4 be the only user of the device, and may not be the only individual whose physical
5 characteristics are among those that will unlock the device via biometric features.
6 Furthermore, while physical proximity is an important factor in determining who is the
7 user of a device, it is only one among many other factors that may exist.

8 i. Due to the foregoing, I request that if law enforcement personnel
9 encounter a device that is subject to search and seizure pursuant to this warrant and may
10 be unlocked using one of the aforementioned biometric features, and if law enforcement
11 reasonably suspects [any individual located at the Subject Premises] [Name of Target(s)]
12 is a user of the device, then – for the purpose of attempting to unlock the device in order
13 to search the contents as authorized by this warrant – law enforcement personnel shall be
14 authorized to:(1) press or swipe the fingers (including thumbs) of [the individuals] [Name
15 of Target] to the fingerprint scanner of the device; and/or (2) hold the device in front of
16 the face and open eyes of [those same individuals] [Name of Target] and activate the
17 facial, iris, or retina recognition feature.

18 j. In pressing or swiping an individual’s thumb or finger onto a device
19 and in holding a device in front of an individual’s face and open eyes, law enforcement
20 may not use excessive force, as defined in *Graham v. Connor*, 490 U.S. 386 (1989);
21 specifically, law enforcement may use no more than objectively reasonable force in light
22 of the facts and circumstances confronting them.

23 **TECHNICAL TERMS**

24 63. Based on my training and experience, and information acquired from other
25 law enforcement officials with technical expertise, I know the terms described below have
26 the following meanings or characteristics:
27

1 a. “Digital device,” as used herein, includes the following three terms
2 and their respective definitions:

3 1) A “computer” means an electronic, magnetic, optical, or other
4 high speed data processing device performing logical or storage functions, and includes
5 any data storage facility or communications facility directly related to or operating in
6 conjunction with such device. *See* 18 U.S.C. § 1030(e)(1). Computers are physical units of
7 equipment that perform information processing using a binary system to represent
8 information. Computers include, but are not limited to, desktop and laptop computers,
9 smartphones, tablets, smartwatches, and binary data processing units used in the operation
10 of other products like automobiles.

11 2) “Digital storage media,” as used herein, means any information
12 storage device in which information is preserved in binary form and includes electrical,
13 optical, and magnetic digital storage devices. Examples of digital storage media include,
14 but are not limited to, compact disks, digital versatile disks (“DVDs”), USB flash drives,
15 flash memory cards, and internal and external hard drives.

16 3) “Computer hardware” means all equipment that can receive,
17 capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic,
18 magnetic, or similar computer impulses or data. Computer hardware includes any data-
19 processing devices (including, but not limited to, central processing units, internal and
20 peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and
21 diskettes, and other memory storage devices); peripheral input/output devices (including,
22 but not limited to, keyboards, printers, video display monitors, modems, routers, scanners,
23 and related communications devices such as cables and connections), as well as any
24 devices, mechanisms, or parts that can be used to restrict access to computer hardware
25 (including, but not limited to, physical keys and locks).

26 b. “Wireless telephone” (or mobile telephone, or cellular telephone), a
27 type of digital device, is a handheld wireless device used for voice and data communication

1 at least in part through radio signals and also often through “wi-fi” networks. When
2 communicating via radio signals, these telephones send signals through networks of
3 transmitters/receivers, enabling communication with other wireless telephones, traditional
4 “land line” telephones, computers, and other digital devices. A wireless telephone usually
5 contains a “call log,” which records the telephone number, date, and time of calls made to
6 and from the phone. In addition to enabling voice communications, wireless telephones
7 offer a broad range of applications and capabilities. These include, variously: storing names
8 and phone numbers in electronic “address books”; sending, receiving, and storing text
9 messages, e-mail, and other forms of messaging; taking, sending, receiving, and storing
10 still photographs and video; storing and playing back audio files; storing dates,
11 appointments, and other information on personal calendars; utilizing global positioning
12 system (“GPS”) locating and tracking technology, and accessing and downloading
13 information from the Internet.

14 c. A “tablet” is a mobile computer, typically larger than a wireless phone
15 yet smaller than a notebook, that is primarily operated by touch-screen. Like wireless
16 phones, tablets function as wireless communication devices and can be used to access the
17 Internet or other wired or wireless devices through cellular networks, “wi-fi” networks, or
18 otherwise. Tablets typically contain programs called applications (“apps”), which, like
19 programs on both wireless phones, as described above, and personal computers, perform
20 many different functions and save data associated with those functions.

21 d. A “GPS” navigation device, including certain wireless phones and
22 tablets, uses the Global Positioning System (generally abbreviated “GPS”) to display its
23 current location, and often retains records of its historical locations. Some GPS navigation
24 devices can give a user driving or walking directions to another location, and may contain
25 records of the addresses or locations involved in such historical navigation. The GPS
26 consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely
27 accurate clock. Each satellite repeatedly transmits by radio a mathematical representation

1 of the current time, combined with a special sequence of numbers. These signals are sent
2 by radio, using specifications that are publicly available. A GPS antenna on Earth can
3 receive those signals. When a GPS antenna receives signals from at least four satellites, a
4 computer connected to that antenna can mathematically calculate the antenna's latitude,
5 longitude, and sometimes altitude with a high level of precision.

6 e. "Computer passwords and data security devices" means information
7 or items designed to restrict access to or hide computer software, documentation, or data.
8 Data security devices may consist of hardware, software, or other programming code. A
9 password (a string of alpha-numeric characters) usually operates as a digital key to
10 "unlock" particular data security devices. Data security hardware may include encryption
11 devices, chips, and circuit boards. Data security software of digital code may include
12 programming code that creates "test" keys or "hot" keys, which perform certain pre-set
13 security functions when touched. Data security software or code may also encrypt,
14 compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well
15 as reverse the progress to restore it.

16 f. "Computer software" means digital information which can be
17 interpreted by a computer and any of its related components to direct the way they work.
18 Computer software is stored in electronic, magnetic, or other digital form. It commonly
19 includes programs to run operating systems, applications, and utilities.

20 g. Internet Protocol ("IP") Address is a unique numeric address used by
21 digital devices on the Internet. An IP address, for present purposes, looks like a series of
22 four numbers, each in the range 0-255, separated by periods (*e.g.*, 149.101.1.32). Every
23 computer attached to the Internet must be assigned an IP address so that Internet traffic
24 sent from and directed to that computer may be directed properly from its source to its
25 destination. Most Internet service providers control a range of IP addresses. Some
26 computers have static—that is, long-term—IP addresses, while other computers have
27 dynamic—that is, frequently changed—IP addresses.

1 h. The “Internet” is a global network of computers and other electronic
2 devices that communicate with each other using numerous specified protocols. Due to the
3 structure of the Internet, connections between devices on the Internet often cross state and
4 international borders, even when the devices communicating with each other are in the
5 same state.

6 i. “Internet Service Providers,” or “ISPs,” are entities that provide
7 individuals and businesses access to the Internet. ISPs provide a range of functions for their
8 customers, including access to the Internet, web hosting, e-mail, remote storage, and co-
9 location of computers and other communications equipment. ISPs can offer a range of
10 options in providing access to the Internet, including via telephone-based dial-up and
11 broadband access via digital subscriber line (“DSL”), cable, dedicated circuits, fiber-optic,
12 or satellite. ISPs typically charge a fee based upon the type of connection and volume of
13 data, called bandwidth, which the connection supports. Many ISPs assign each subscriber
14 an account name, a user name or screen name, an e-mail address, an e-mail mailbox, and a
15 personal password selected by the subscriber. By using a modem, the subscriber can
16 establish communication with an ISP and access the Internet by using his or her account
17 name and password.

18 j. A “modem” translates signals for physical transmission to and from
19 the ISP, which then sends and receives the information to and from other computers
20 connected to the Internet.

21 k. A “router” often serves as a wireless Internet access point for a single
22 or multiple devices, and directs traffic between computers connected to a network (whether
23 by wire or wirelessly). A router connected to the Internet collects traffic bound for the
24 Internet from its client machines and sends out requests on their behalf. The router also
25 distributes to the relevant client inbound traffic arriving from the Internet. A router usually
26 retains logs for any devices using that router for Internet connectivity. Routers, in turn, are
27 typically connected to a modem.

1 l. “Domain Name” means the common, easy-to-remember names
2 associated with an IP address. For example, a domain name of “www.usdoj.gov” refers to
3 the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric
4 characters, with each level delimited by a period. Each level, read backwards – from right
5 to left – further identifies parts of an organization. Examples of first-level, or top-level
6 domains are typically .com for commercial organizations, .gov for the governmental
7 organizations, .org for organizations, and .edu for educational organizations. Second-level
8 names will further identify the organization, for example usdoj.gov further identifies the
9 United States governmental agency to be the Department of Justice. Additional levels may
10 exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov
11 identifies the World Wide Web server located at the United States Department of Justice,
12 which is part of the United States government.

13 m. “Cache” means the text, image, and graphic files sent to and
14 temporarily stored by a user’s computer from a website accessed by the user in order to
15 allow the user speedier access to and interaction with that website in the future.

16 n. “Peer to Peer file sharing” (P2P) is a method of communication
17 available to Internet users through the use of special software, which may be downloaded
18 from the Internet. In general, P2P software allows a user to share files on a computer with
19 other computer users running compatible P2P software. A user may obtain files by opening
20 the P2P software on the user’s computer and searching for files that are currently being
21 shared on the network. A P2P file transfer is assisted by reference to the IP addresses of
22 computers on the network: an IP address identifies the location of each P2P computer and
23 makes it possible for data to be transferred between computers. One aspect of P2P file
24 sharing is that multiple files may be downloaded at the same time. Another aspect of P2P
25 file sharing is that, when downloading a file, portions of that file may come from multiple
26 other users on the network to facilitate faster downloading.

27

1 i. When a user wishes to share a file, the user adds the file to shared
2 library files (either by downloading a file from another user or by copying
3 any file into the shared directory), and the file’s hash value is recorded by the
4 P2P software. The hash value is independent of the file name; that is, any
5 change in the name of the file will not change the hash value.

6 ii. Third party software is available to identify the IP address of a
7 P2P computer that is sending a file. Such software monitors and logs Internet
8 and local network traffic.

9 o. “VPN” means a virtual private network. A VPN extends a private
10 network across public networks like the Internet. It enables a host computer to send and
11 receive data across shared or public networks as if they were an integral part of a private
12 network with all the functionality, security, and management policies of the private
13 network. This is done by establishing a virtual point-to-point connection through the use
14 of dedicated connections, encryption, or a combination of the two. The VPN connection
15 across the Internet is technically a wide area network (WAN) link between the sites. From
16 a user perspective, the extended network resources are accessed in the same way as
17 resources available from a private network-hence the name “virtual private network.” The
18 communication between two VPN endpoints is encrypted and usually cannot be intercepted
19 by law enforcement.

20 p. “Encryption” is the process of encoding messages or information in
21 such a way that eavesdroppers or hackers cannot read it but authorized parties can. In an
22 encryption scheme, the message or information, referred to as plaintext, is encrypted using
23 an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with
24 the use of an encryption key, which specifies how the message is to be encoded. Any
25 unintended party that can see the ciphertext should not be able to determine anything about
26 the original message. An authorized party, however, is able to decode the ciphertext using
27

1 a decryption algorithm that usually requires a secret decryption key, to which adversaries
2 do not have access.

3 q. “Malware,” short for malicious (or malevolent) software, is software
4 used or programmed by attackers to disrupt computer operations, gather sensitive
5 information, or gain access to private computer systems. It can appear in the form of code,
6 scripts, active content, and other software. Malware is a general term used to refer to a
7 variety of forms of hostile or intrusive software.

8 **COMPUTERS, ELECTRONIC/MAGNETIC STORAGE, AND FORENSIC**
9 **ANALYSIS**

10 64. As described above and in Attachment B, this application seeks permission
11 to search for evidence, fruits, contraband, instrumentalities, and information that might be
12 found within the Device, in whatever form they are found. One form in which such items
13 might be found is data stored on one or more digital devices. Such devices are defined
14 above and include any electronic system or device capable of storing or processing data in
15 digital form, including central processing units; desktop computers, laptop computers,
16 notebooks, and tablet computers; personal digital assistants; wireless communication
17 devices, such as telephone paging devices, beepers, mobile telephones, and smart phones;
18 digital cameras; peripheral input/output devices, such as keyboards, printers, scanners,
19 plotters, monitors, and drives intended for removable media; related communications
20 devices, such as modems, routers, cables, and connections; storage media, such as hard
21 disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic
22 tapes used to store digital data (excluding analog tapes such as VHS); and security devices.
23 Thus, the warrant applied for would authorize the seizure of digital devices or, potentially,
24 the copying of stored information, all under Rule 41(e)(2)(B). Based on my knowledge,
25 training, and experience, as well as information related to me by agents and others involved
26 in this investigation and in the forensic examination of digital devices, I respectfully submit
27

1 that there is probable cause to believe that the records and information described in
2 Attachment B will be stored in the Device for at least the following reasons:

3 65. Individuals who engage in criminal activity, including the TARGET
4 OFFENSES use digital devices, like the Device(s), to access websites to facilitate illegal
5 activity and to communicate with co-conspirators online; to store on digital devices, like
6 the Device(s), documents and records relating to their illegal activity, which can include
7 logs of online chats with co-conspirators; email correspondence; text or other “Short
8 Message Service” (“SMS”) messages; contact information of co-conspirators, including
9 telephone numbers, email addresses, identifiers for instant messaging and social medial
10 accounts; call logs, phone books, photographs, voice mail messages, images and video,
11 Global Positioning System data, and any other stored electronic data. This information can:
12 (i) reflect the preparation for, arrangement of, and commission of violations of the
13 TARGET OFFENSES; (ii) identify locations relevant to the TARGET OFFENSES; (iii)
14 reflect the ownership and use of the cellular telephones by persons involved in the
15 commission of the TARGET OFFENSES; (iv) document meetings and communications
16 between associates, and co-conspirators of violations of the TARGET OFFENSES.

17 a. Individuals who engage in the foregoing criminal activity, in the event
18 that they change digital devices, will often “back up” or transfer files from their old digital
19 devices to that of their new digital devices, so as not to lose data, including that described
20 in the foregoing paragraph, which would be valuable in facilitating their criminal activity.

21 b. Digital device files, or remnants of such files, can be recovered months
22 or even many years after they have been downloaded onto the medium or device, deleted,
23 or viewed via the Internet. Electronic files downloaded to a digital device can be stored for
24 years at little or no cost. Even when such files have been deleted, they can be recovered
25 months or years later using readily-available forensics tools. When a person “deletes” a file
26 on a digital device such as a home computer, a smart phone, or a memory card, the data
27 contained in the file does not actually disappear; rather, that data remains on the storage

1 medium and within the device unless and until it is overwritten by new data. Therefore,
2 deleted files, or remnants of deleted files, may reside in free space or slack space – that is,
3 in space on the digital device that is not allocated to an active file or that is unused after a
4 file has been allocated to a set block of storage space – for long periods of time before they
5 are overwritten. In addition, a digital device’s operating system may also keep a record of
6 deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the
7 Internet are automatically downloaded into a temporary Internet directory or “cache.” The
8 browser typically maintains a fixed amount of electronic storage medium space devoted to
9 these files, and the files are only overwritten as they are replaced with more recently viewed
10 Internet pages. Thus, the ability to retrieve “residue” of an electronic file from a digital
11 device depends less on when the file was downloaded or viewed than on a particular user’s
12 operating system, storage capacity, and computer, smart phone, or other digital device
13 habits.

14 66. As further described in Attachment B, this application seeks permission to
15 locate not only electronic evidence or information that might serve as direct evidence of
16 the crimes described in this affidavit, but also for forensic electronic evidence or
17 information that establishes how the digital device(s) were used, the purpose of their use,
18 who used them (or did not), and when. Based on my knowledge, training, and experience,
19 as well as information related to me by agents and others involved in this investigation and
20 in the forensic examination of digital devices, I respectfully submit there is probable cause
21 to believe that this forensic electronic evidence and information will be in any of the
22 Device(s) at issue here because:

23 a. Although some of the records called for by this warrant might be
24 found in the form of user-generated documents or records (such as word processing,
25 picture, movie, or texting files), digital devices can contain other forms of electronic
26 evidence as well. In particular, records of how a digital device has been used, what it has
27 been used for, who has used it, and who has been responsible for creating or maintaining

1 records, documents, programs, applications, and materials contained on the digital
2 device(s) are, as described further in the attachments, called for by this warrant. Those
3 records will not always be found in digital data that is neatly segregable from the hard
4 drive, flash drive, memory card, or other electronic storage media image as a whole. Digital
5 data stored in the Device(s), not currently associated with any file, can provide evidence of
6 a file that was once on the storage medium but has since been deleted or edited, or of a
7 deleted portion of a file (such as a paragraph that has been deleted from a word processing
8 file). Virtual memory paging systems can leave digital data on a hard drive that show what
9 tasks and processes on a digital device were recently used. Web browsers, e-mail programs,
10 and chat programs often store configuration data on a hard drive, flash drive, memory card,
11 or memory chip that can reveal information such as online nicknames and passwords.
12 Operating systems can record additional data, such as the attachment of peripherals, the
13 attachment of USB flash storage devices, and the times a computer, smart phone, or other
14 digital device was in use. Computer, smart phone, and other digital device file systems can
15 record data about the dates files were created and the sequence in which they were created.
16 This data can be evidence of a crime, indicate the identity of the user of the digital device,
17 or point toward the existence of evidence in other locations. Recovery of this data requires
18 specialized tools and a controlled laboratory environment, and also can require substantial
19 time.

20 b. Forensic evidence on a digital device can also indicate who has used or
21 controlled the device. This “user attribution” evidence is analogous to the search for
22 “indicia of occupancy” while executing a search warrant at a residence. For example,
23 registry information, configuration files, user profiles, e-mail, e-mail address books, chats,
24 instant messaging logs, photographs, the presence or absence of malware, and
25 correspondence (and the data associated with the foregoing, such as file creation and last-
26 accessed dates) may be evidence of who used or controlled the digital device at a relevant
27 time, and potentially who did not.

1 c. A person with appropriate familiarity with how a digital device works
2 can, after examining this forensic evidence in its proper context, draw conclusions about
3 how such digital devices were used, the purpose of their use, who used them, and when.

4 d. The process of identifying the exact files, blocks, registry entries,
5 logs, or other forms of forensic evidence on a digital device that are necessary to draw an
6 accurate conclusion is a dynamic process. While it is possible to specify in advance the
7 records to be sought, digital device evidence is not always data that can be merely reviewed
8 by a review team and passed along to investigators. Whether data stored on digital devices
9 is evidence may depend on other information stored on the devices and the application of
10 knowledge about how the devices behave. Therefore, contextual information necessary to
11 understand other evidence also falls within the scope of the warrant.

12 e. Further, in finding evidence of how a digital device was used, the
13 purpose of its use, who used it, and when, sometimes it is necessary to establish that a
14 particular thing is not present on the device. For example, the presence or absence of
15 counter-forensic programs, anti-virus programs (and associated data), and malware may be
16 relevant to establishing the user's intent and the identity of the user.

17 **METHODS TO BE USED TO SEARCH DIGITAL DEVICES**

18 67. Based on my knowledge, training, and experience, as well as information
19 related to me by agents and others involved in this investigation and in the forensic
20 examination of digital devices, I know that:

21 a. Searching digital devices can be an extremely technical process, often
22 requiring specific expertise, specialized equipment, and substantial amounts of time, in part
23 because there are so many types of digital devices and software programs in use today.
24 Digital devices – whether, for example, desktop computers, mobile devices, or portable
25 storage devices – may be customized with a vast array of software applications, each
26 generating a particular form of information or records and each often requiring unique
27 forensic tools, techniques, and expertise. As a result, it may be necessary to consult with

1 specially trained personnel who have specific expertise in the types of digital devices,
2 operating systems, or software applications that are being searched, and to obtain
3 specialized hardware and software solutions to meet the needs of a particular forensic
4 analysis.

5 b. Digital data is particularly vulnerable to inadvertent or intentional
6 modification or destruction. Searching digital devices can require the use of precise,
7 scientific procedures that are designed to maintain the integrity of digital data and to
8 recover “hidden,” erased, compressed, encrypted, or password-protected data. Recovery of
9 “residue” of electronic files from digital devices also requires specialized tools and often
10 substantial time. As a result, a controlled environment, such as a law enforcement
11 laboratory or similar facility, is often essential to conducting a complete and accurate
12 analysis of data stored on digital devices.

13 c. Further, as discussed above, evidence of how a digital device has been
14 used, the purposes for which it has been used, and who has used it, may be reflected in the
15 absence of particular data on a digital device. For example, to rebut a claim that the owner
16 of a digital device was not responsible for a particular use because the device was being
17 controlled remotely by malicious software, it may be necessary to show that malicious
18 software that allows someone else to control the digital device remotely is not present on
19 the digital device. Evidence of the absence of particular data or software on a digital device
20 is not segregable from the digital device itself. Analysis of the digital device as a whole to
21 demonstrate the absence of particular data or software requires specialized tools and a
22 controlled laboratory environment, and can require substantial time.

23 d. Digital device users can attempt to conceal data within digital devices
24 through a number of methods, including the use of innocuous or misleading filenames and
25 extensions. For example, files with the extension “.jpg” often are image files; however, a
26 user can easily change the extension to “.txt” to conceal the image and make it appear as
27 though the file contains text. Digital device users can also attempt to conceal data by using

1 encryption, which means that a password or device, such as a “dongle” or “keycard,” is
2 necessary to decrypt the data into readable form. Digital device users may encode
3 communications or files, including substituting innocuous terms for incriminating terms or
4 deliberately misspelling words, thereby thwarting “keyword” search techniques and
5 necessitating continuous modification of keyword terms. Moreover, certain file formats,
6 like portable document format (“PDF”), do not lend themselves to keyword searches. Some
7 applications for computers, smart phones, and other digital devices, do not store data as
8 searchable text; rather, the data is saved in a proprietary non-text format. Documents
9 printed by a computer, even if the document was never saved to the hard drive, are
10 recoverable by forensic examiners but not discoverable by keyword searches because the
11 printed document is stored by the computer as a graphic image and not as text. In addition,
12 digital device users can conceal data within another seemingly unrelated and innocuous
13 file in a process called “steganography.” For example, by using steganography, a digital
14 device user can conceal text in an image file that cannot be viewed when the image file is
15 opened. Digital devices may also contain “booby traps” that destroy or alter data if certain
16 procedures are not scrupulously followed. A substantial amount of time is necessary to
17 extract and sort through data that is concealed, encrypted, or subject to booby traps, to
18 determine whether it is evidence, contraband, or instrumentalities of a crime.

19 e. Analyzing the contents of mobile devices, including tablets, can be very
20 labor intensive and also requires special technical skills, equipment, and software. The
21 large, and ever increasing, number and variety of available mobile device applications
22 generate unique forms of data, in different formats, and user information, all of which
23 present formidable and sometimes novel forensic challenges to investigators that cannot be
24 anticipated before examination of the device. Additionally, most smart phones and other
25 mobile devices require passwords for access. For example, even older iPhone 4 models,
26 running IOS 7, deployed a type of sophisticated encryption known as “AES-256
27 encryption” to secure and encrypt the operating system and application data, which could

1 only be bypassed with a numeric passcode. Newer cell phones employ equally
2 sophisticated encryption along with alpha-numeric passcodes, rendering most smart
3 phones inaccessible without highly sophisticated forensic tools and techniques, or
4 assistance from the phone manufacturer. Mobile devices used by individuals engaged in
5 criminal activity are often further protected and encrypted by one or more third party
6 applications, of which there are many. For example, one such mobile application, "Hide It
7 Pro," disguises itself as an audio application, allows users to hide pictures and documents,
8 and offers the same sophisticated AES-256 encryption for all data stored within the
9 database in the mobile device.

10 f. Based on all of the foregoing, I respectfully submit that searching any
11 digital device for the information, records, or evidence pursuant to this warrant may require
12 a wide array of electronic data analysis techniques and may take weeks or months to
13 complete. Any pre-defined search protocol would only inevitably result in over- or under-
14 inclusive searches, and misdirected time and effort, as forensic examiners encounter
15 technological and user-created challenges, content, and software applications that cannot
16 be anticipated in advance of the forensic examination of the devices. In light of these
17 difficulties, your affiant requests permission to use whatever data analysis techniques
18 reasonably appear to be necessary to locate and retrieve digital information, records, or
19 evidence within the scope of this warrant.

20 68. The volume of data stored on many digital devices will typically be so large
21 that it will be extremely impractical to search for data during the physical search of the
22 premises.

23 a. Therefore, in searching for information, records, or evidence, further
24 described in Attachment B, law enforcement personnel executing this search warrant will
25 employ the following procedures:

26 i. Law enforcement personnel will, consistent with Rule 41(e)(2)(B) of
27 the Federal Rules of Criminal Procedure, transport the TARGET DEVICE to

1 an appropriate law enforcement laboratory or similar facility for review. For
2 all the reasons described above, it would not be feasible to conduct a complete,
3 safe, and appropriate search of any such digital devices at the PREMISES. The
4 digital devices, and/or any digital images thereof created by law enforcement
5 sometimes with the aid of a technical expert, in an appropriate setting, in aid
6 of the examination and review, will be examined and reviewed in order to
7 extract and seize the information, records, or evidence described in Attachment
8 B.

9 ii. The analysis of the contents of the digital devices may entail any or
10 all of various forensic techniques as circumstances warrant. Such techniques
11 may include, but shall not be limited to, surveying various file “directories”
12 and the individual files they contain (analogous to looking at the outside of a
13 file cabinet for the markings it contains and opening a drawer believed to
14 contain pertinent files); conducting a file-by-file review by “opening,”
15 reviewing, or reading the images or first few “pages” of such files in order to
16 determine their precise contents; “scanning” storage areas to discover and
17 possibly recover recently deleted data; scanning storage areas for deliberately
18 hidden files; and performing electronic “keyword” searches through all
19 electronic storage areas to determine whether occurrences of language
20 contained in such storage areas exist that are related to the subject matter of
21 the investigation.

22 iii. In searching the digital devices, the forensic examiners may examine
23 as much of the contents of the digital devices as deemed necessary to make a
24 determination as to whether the contents fall within the items to be seized as
25 set forth in Attachment B. In addition, the forensic examiners may search for
26 and attempt to recover “deleted,” “hidden,” or encrypted data to determine
27 whether the contents fall within the items to be seized as described in

Attachment B. Any search techniques or protocols used in searching the contents of the seized digital devices will be specifically chosen to identify the specific items to be seized under this warrant.

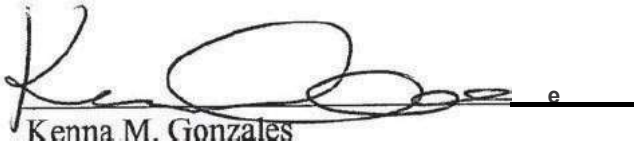
CONCLUSION

69. Based upon the above-referenced facts, your affiant asserts that there is probable cause to believe that the TARGET DEVICE contains evidence of the TARGET OFFENSE.

70. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to Federal Rule of Criminal Procedure 41.

71. I further request that the Court permit the search warrant to be executed at any time given that the TARGET DEVICE is contained on the premises of the Federal Bureau of Investigation.

Respectfully submitted,



Kenna M. Gonzales
Federal Bureau of Investigation

Affidavit submitted by email and attested to me as true and accurate by telephone, consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) this 15th day of December, 2023.

17J7

The Honorable Brian A. Tsuchida
United States Magistrate Judge

ATTACHMENT A

Property to be searched

The person to be searched is MATTHEW LAWRENCE STICKNEY (date of birth [REDACTED], 1989) (“STICKNEY” as pictured below, provided that such person is located within the Western District of Washington).



The property to be searched is any digital device which is capable of containing or reasonably could contain fruits, evidence, information, contraband, or instrumentalities described in paragraph 1 of Attachment B (the “Device(s)”), specifically including any smart phone(s) and/or cellular telephone(s) that law enforcement has reason to believe belong to STICKNEY.

ATTACHMENT B

Property to be seized

1
2
3 1. The items, information, and data to be seized are fruits, evidence, and
4 instrumentalities, in whatever form and however stored, of violations of 18 U.S.C. §
5 1752(a)(1) (entering or remaining in restricted buildings or grounds), 18 U.S.C. §
6 1752(a)(2) (disorderly and disruptive conduct in a restricted building or grounds), 40
7 U.S.C. § 5104(e)(2)(D) (disorderly or disruptive conduct in a Capitol building or grounds),
8 and 40 U.S.C. § 5104(e)(2)(G) (parading, demonstrating, or picketing in a Capitol building
9 or grounds) (the “TARGET OFFENSES”), as described in the search warrant affidavit,
10 including, but not limited to call logs, phone books, photographs, voice mail messages, text
11 messages, images and video, Global Positioning System data, and any other stored
12 electronic data that contain, constitute evidence of, document, establish, identify, or reflect:

13 a. Establishing or documenting the commission of the TARGET
14 OFFENSES;

15 b. Identifying locations where the individual committed the TARGET
16 OFFENSES, traveled to before and after the commission of the TARGET OFFENSES,
17 and in preparation for the TARGET OFFENSES;

18 c. Reflecting the ownership and use of the item identified in Attachment
19 A by the individual committing the TARGET OFFENSES;

20 d. Documenting meetings and communications between individuals
21 committing one or more of the TARGET OFFENSES;

22 e. Reflecting communications between the individual committing one or
23 more of the TARGET OFFENSES and other individuals, discussing the commission of
24 one or more of the TARGET OFFENSES;

25 f. Reflecting communications between the individual committing one or
26 more of the TARGET OFFENSES and other individuals who may have assisted or
27 provided support in the commission of one or more of the TARGET OFFENSES;

1 g. Containing photographs or video that would constitute evidence of a
2 violation of the TARGET OFFENSES;

3 h. Evidence of any conspiracy, planning, or preparation to commit the
4 TARGET OFFENSES;

5 i. Evidence concerning efforts after the fact to conceal evidence of the
6 TARGET OFFENSES, or to flee prosecution for the same;

7 j. Evidence concerning materials, devices, or tools that were used to
8 unlawfully commit the TARGET OFFENSES;

9 k. Evidence of communication devices used in relation to the TARGET
10 OFFENSES;

11 l. Evidence of the state of mind of the subject in committing the
12 TARGET OFFENSES, e.g., intent, absence of mistake, or evidence indicating preparation
13 or planning, or knowledge and experience, related to the criminal activity under
14 investigation;

15 m. Evidence concerning the identity of persons who either (i)
16 collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the
17 criminal activity under investigation; or (ii) communicated with the unlawful actors about
18 matters relating to the criminal activity under investigation, including records that help
19 reveal their whereabouts;

20 n. Evidence concerning planning to unlawfully enter the U.S. Capitol,
21 including any maps or diagrams of the building or its internal offices;

22 o. Evidence concerning unlawful entry into the U.S. Capitol, including
23 any property of the U.S. Capitol;

24 p. Evidence concerning the official proceeding that was to take place at
25 Congress on January 6, 2021, i.e., the certification process of the 2020 Presidential
26 Election;

1 q. Evidence concerning efforts to obstruct, impede, or disrupt the official
2 proceeding that was to take place at Congress on January 6, 2021, i.e., the certification
3 process of the 2020 Presidential Election;

4 r. Evidence concerning the breach and unlawful entry of the United
5 States Capitol on January 6, 2021;

6 s. Evidence concerning the riot and/or civil disorder at the United States
7 Capitol on January 6, 2021;

8 t. Evidence concerning the assaults of federal officers/agents and efforts
9 to impede such federal officers/agents in the performance of their duties the United States
10 Capitol on January 6, 2021;

11 u. Evidence concerning damage to, or theft of, property at the United
12 States Capitol on January 6, 2021;

13 v. Evidence concerning awareness that the U.S. Capitol was closed to
14 the public on January 6, 2021;

15 w. Evidence of the subject's presence at the U.S. Capitol on or around
16 January 6, 2021;

17 x. Evidence concerning the results of, challenges to, or questions about
18 the legitimacy of the 2020 Presidential Election;

19 y. Evidence regarding travel to Washington, D.C. in or around January
20 2021, motive and intent for travel to Washington, D.C. in or around January 2021, the
21 planning of travel to and activity in Washington, D.C. on or about January 6, 2021, research
22 about the U.S. Capitol, and mode of travel, travel expenses, and travel logistics on or about
23 January 6, 2021;

24 z. Evidence regarding the riot at the U.S. Capitol on January 6, 2021;

25 aa. Records and information related to the email addresses, phone
26 numbers, social media, account identifiers used by perpetrators, aiders and abettors, co-
27 conspirators, and accessories after the fact concerning the TARGET OFFENSE;

1 bb. Evidence of who used, owned, or controlled the Device(s) at the time
2 the things described in this warrant were created, edited, or deleted, such as logs, registry
3 entries, configuration files, saved usernames and passwords, documents, browsing history,
4 user profiles, email, email contacts, chat, instant messaging logs, photographs, and
5 correspondence;

6 cc. Evidence of software, or the lack thereof, that would allow others to
7 control the Device(s), such as viruses, Trojan horses, and other forms of malicious
8 software, as well as evidence of the presence or absence of security software designed to
9 detect malicious software;

10 dd. Evidence of the attachment to the Device(s) of other storage devices
11 or similar containers for electronic evidence;

12 ee. Evidence of counter-forensic programs (and associated data) that are
13 designed to eliminate data from the Device(s);

14 ff. Evidence of the times the Device(s) was used;

15 gg. Passwords, encryption keys, and other access devices that may be
16 necessary to access the Device(s);

17 hh. Records of or information about Internet Protocol addresses used by
18 the Device(s); and

19 ii. Records of or information about the Device(s)'s Internet activity,
20 including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite"
21 web pages, search terms that the user entered into any Internet search engine, and records
22 of user-typed web addresses.

23 2. During the execution of this search warrant as described in Attachment A,
24 if law enforcement encounters a smartphone or other electronic device equipped with a
25 biometric-unlock feature, and if law enforcement reasonably suspects Matthew Lawrence
26 Stickney is a user of the device, then – for the purpose of attempting to unlock the device
27 in order to search the contents as authorized by this warrant – law enforcement personnel

1 are authorized to: (1) press or swipe the fingers (including thumbs) of Matthew Lawrence
 2 Stickney to the fingerprint scanner of the device; and/or (2) hold the device in front of the
 3 face and open eyes of Matthew Lawrence Stickney and activate the facial, iris, or retina
 4 recognition feature. In pressing or swiping an individual’s thumb or finger onto a device
 5 and in holding a device in front of an individual’s face and open eyes, law enforcement
 6 may not use excessive force, as defined in *Graham v. Connor*, 490 U.S. 386 (1989);
 7 specifically, law enforcement may use no more than objectively reasonable force in light
 8 of the facts and circumstances confronting them.

9 While attempting to unlock the device by use of the compelled display of
 10 biometric characteristics pursuant to this warrant, law enforcement is not authorized to
 11 demand that the aforementioned person(s) state or otherwise provide the password or
 12 identify the specific biometric characteristics (including the unique finger(s) or other
 13 physical features), that may be used to unlock or access the Device(s). Nor does the
 14 warrant authorize law enforcement to use the fact that the warrant allows law
 15 enforcement to obtain the display of any biometric characteristics to compel the
 16 aforementioned person(s) to state or otherwise provide that information. However, the
 17 voluntary disclosure of such information by the aforementioned person(s) is permitted.
 18 To avoid confusion on that point, if agents in executing the warrant ask any of the
 19 aforementioned person(s) for the password to any Device(s), or to identify which
 20 biometric characteristic (including the unique finger(s) or other physical features) unlocks
 21 any Device(s), the agents will not state or otherwise imply that the warrant requires the
 22 person to provide such information, and will make clear that providing any such
 23 information is voluntary and that the person is free to refuse the request.

24
 25
 26
 27

UNITED STATES DISTRICT COURT

for the
Western District of Washington

In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address))
The Person of Matthew Lawrence Stickney,)
more fully described in Attachment A)
)

Case No. MJ23-600

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

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

The person of Matthew Lawrence Stickney, more fully described in Attachment A, incorporated herein 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, for list of items to be seized, incorporated herein by reference

YOU ARE COMMANDED to execute this warrant on or before December 29, 2023 (not to exceed 14 days)
 in the daytime 6:00 a.m. to 10:00 p.m. at any time in the day or night because good cause has been established.

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

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to any U.S. Magistrate Judge in this District.
(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: 12/15/2023 9:15 AM



Judge's signature

City and state: Seattle, Washington

Brian A. Tsuchida, United States Magistrate Judge

Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p>		
Date: _____	<p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Executing officer's signature</i></p> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Printed name and title</i></p>	

ATTACHMENT A

Property to be searched

1
2
3 The person to be searched is MATTHEW LAWRENCE STICKNEY (date of birth
4 [REDACTED], 1989) (“STICKNEY” as pictured below, provided that such person is located
5 within the Western District of Washington).



21 The property to be searched is any digital device which is capable of containing or
22 reasonably could contain fruits, evidence, information, contraband, or instrumentalities
23 described in paragraph 1 of Attachment B (the “Device(s)”), specifically including any
24 smart phone(s) and/or cellular telephone(s) that law enforcement has reason to believe
25 belong to STICKNEY.
26
27

ATTACHMENT B

Property to be seized

1
2
3 1. The items, information, and data to be seized are fruits, evidence, and
4 instrumentalities, in whatever form and however stored, of violations of 18 U.S.C. §
5 1752(a)(1) (entering or remaining in restricted buildings or grounds), 18 U.S.C. §
6 1752(a)(2) (disorderly and disruptive conduct in a restricted building or grounds), 40
7 U.S.C. § 5104(e)(2)(D) (disorderly or disruptive conduct in a Capitol building or grounds),
8 and 40 U.S.C. § 5104(e)(2)(G) (parading, demonstrating, or picketing in a Capitol building
9 or grounds) (the “TARGET OFFENSES”), as described in the search warrant affidavit,
10 including, but not limited to call logs, phone books, photographs, voice mail messages, text
11 messages, images and video, Global Positioning System data, and any other stored
12 electronic data that contain, constitute evidence of, document, establish, identify, or reflect:

13 a. Establishing or documenting the commission of the TARGET
14 OFFENSES;

15 b. Identifying locations where the individual committed the TARGET
16 OFFENSES, traveled to before and after the commission of the TARGET OFFENSES,
17 and in preparation for the TARGET OFFENSES;

18 c. Reflecting the ownership and use of the item identified in Attachment
19 A by the individual committing the TARGET OFFENSES;

20 d. Documenting meetings and communications between individuals
21 committing one or more of the TARGET OFFENSES;

22 e. Reflecting communications between the individual committing one or
23 more of the TARGET OFFENSES and other individuals, discussing the commission of
24 one or more of the TARGET OFFENSES;

25 f. Reflecting communications between the individual committing one or
26 more of the TARGET OFFENSES and other individuals who may have assisted or
27 provided support in the commission of one or more of the TARGET OFFENSES;

1 g. Containing photographs or video that would constitute evidence of a
2 violation of the TARGET OFFENSES;

3 h. Evidence of any conspiracy, planning, or preparation to commit the
4 TARGET OFFENSES;

5 i. Evidence concerning efforts after the fact to conceal evidence of the
6 TARGET OFFENSES, or to flee prosecution for the same;

7 j. Evidence concerning materials, devices, or tools that were used to
8 unlawfully commit the TARGET OFFENSES;

9 k. Evidence of communication devices used in relation to the TARGET
10 OFFENSES;

11 l. Evidence of the state of mind of the subject in committing the
12 TARGET OFFENSES, e.g., intent, absence of mistake, or evidence indicating preparation
13 or planning, or knowledge and experience, related to the criminal activity under
14 investigation;

15 m. Evidence concerning the identity of persons who either (i)
16 collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the
17 criminal activity under investigation; or (ii) communicated with the unlawful actors about
18 matters relating to the criminal activity under investigation, including records that help
19 reveal their whereabouts;

20 n. Evidence concerning planning to unlawfully enter the U.S. Capitol,
21 including any maps or diagrams of the building or its internal offices;

22 o. Evidence concerning unlawful entry into the U.S. Capitol, including
23 any property of the U.S. Capitol;

24 p. Evidence concerning the official proceeding that was to take place at
25 Congress on January 6, 2021, i.e., the certification process of the 2020 Presidential
26 Election;

27

1 q. Evidence concerning efforts to obstruct, impede, or disrupt the official
2 proceeding that was to take place at Congress on January 6, 2021, i.e., the certification
3 process of the 2020 Presidential Election;

4 r. Evidence concerning the breach and unlawful entry of the United
5 States Capitol on January 6, 2021;

6 s. Evidence concerning the riot and/or civil disorder at the United States
7 Capitol on January 6, 2021;

8 t. Evidence concerning the assaults of federal officers/agents and efforts
9 to impede such federal officers/agents in the performance of their duties the United States
10 Capitol on January 6, 2021;

11 u. Evidence concerning damage to, or theft of, property at the United
12 States Capitol on January 6, 2021;

13 v. Evidence concerning awareness that the U.S. Capitol was closed to
14 the public on January 6, 2021;

15 w. Evidence of the subject's presence at the U.S. Capitol on or around
16 January 6, 2021;

17 x. Evidence concerning the results of, challenges to, or questions about
18 the legitimacy of the 2020 Presidential Election;

19 y. Evidence regarding travel to Washington, D.C. in or around January
20 2021, motive and intent for travel to Washington, D.C. in or around January 2021, the
21 planning of travel to and activity in Washington, D.C. on or about January 6, 2021, research
22 about the U.S. Capitol, and mode of travel, travel expenses, and travel logistics on or about
23 January 6, 2021;

24 z. Evidence regarding the riot at the U.S. Capitol on January 6, 2021;

25 aa. Records and information related to the email addresses, phone
26 numbers, social media, account identifiers used by perpetrators, aiders and abettors, co-
27 conspirators, and accessories after the fact concerning the TARGET OFFENSE;

1 bb. Evidence of who used, owned, or controlled the Device(s) at the time
2 the things described in this warrant were created, edited, or deleted, such as logs, registry
3 entries, configuration files, saved usernames and passwords, documents, browsing history,
4 user profiles, email, email contacts, chat, instant messaging logs, photographs, and
5 correspondence;

6 cc. Evidence of software, or the lack thereof, that would allow others to
7 control the Device(s), such as viruses, Trojan horses, and other forms of malicious
8 software, as well as evidence of the presence or absence of security software designed to
9 detect malicious software;

10 dd. Evidence of the attachment to the Device(s) of other storage devices
11 or similar containers for electronic evidence;

12 ee. Evidence of counter-forensic programs (and associated data) that are
13 designed to eliminate data from the Device(s);

14 ff. Evidence of the times the Device(s) was used;

15 gg. Passwords, encryption keys, and other access devices that may be
16 necessary to access the Device(s);

17 hh. Records of or information about Internet Protocol addresses used by
18 the Device(s); and

19 ii. Records of or information about the Device(s)'s Internet activity,
20 including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite"
21 web pages, search terms that the user entered into any Internet search engine, and records
22 of user-typed web addresses.

23 2. During the execution of this search warrant as described in Attachment A,
24 if law enforcement encounters a smartphone or other electronic device equipped with a
25 biometric-unlock feature, and if law enforcement reasonably suspects Matthew Lawrence
26 Stickney is a user of the device, then – for the purpose of attempting to unlock the device
27 in order to search the contents as authorized by this warrant – law enforcement personnel

1 are authorized to: (1) press or swipe the fingers (including thumbs) of Matthew Lawrence
2 Stickney to the fingerprint scanner of the device; and/or (2) hold the device in front of the
3 face and open eyes of Matthew Lawrence Stickney and activate the facial, iris, or retina
4 recognition feature. In pressing or swiping an individual's thumb or finger onto a device
5 and in holding a device in front of an individual's face and open eyes, law enforcement
6 may not use excessive force, as defined in *Graham v. Connor*, 490 U.S. 386 (1989);
7 specifically, law enforcement may use no more than objectively reasonable force in light
8 of the facts and circumstances confronting them.

9 While attempting to unlock the device by use of the compelled display of
10 biometric characteristics pursuant to this warrant, law enforcement is not authorized to
11 demand that the aforementioned person(s) state or otherwise provide the password or
12 identify the specific biometric characteristics (including the unique finger(s) or other
13 physical features), that may be used to unlock or access the Device(s). Nor does the
14 warrant authorize law enforcement to use the fact that the warrant allows law
15 enforcement to obtain the display of any biometric characteristics to compel the
16 aforementioned person(s) to state or otherwise provide that information. However, the
17 voluntary disclosure of such information by the aforementioned person(s) is permitted.
18 To avoid confusion on that point, if agents in executing the warrant ask any of the
19 aforementioned person(s) for the password to any Device(s), or to identify which
20 biometric characteristic (including the unique finger(s) or other physical features) unlocks
21 any Device(s), the agents will not state or otherwise imply that the warrant requires the
22 person to provide such information, and will make clear that providing any such
23 information is voluntary and that the person is free to refuse the request.
24
25
26
27