

UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	
	:	CASE NO. 21-CR-204 (BAH)
v.	:	
	:	
MATTHEW BLEDSOE,	:	
	:	
Defendant	:	

**GOVERNMENT’S OPPOSITION TO DEFENDANT’S  
MOTION TO SUPPRESS EVIDENCE OBTAINED PURSUANT  
TO SEARCH WARRANT**

Matthew Bledsoe traveled from his home in Cordova, Tennessee, to Washington, D.C., where he joined a mob outside of the U.S. Capitol on January 6, 2021. Bledsoe was part of the group that illegally entered the U.S. Capitol on January 6 after a mob forced its way through, up and over the barricades and officers, then forced entry into the Capitol Building. His journey was documented through photos and videos, and a video compilation was posted to his Instagram account—theessentialmattbledsoe.

In a matter of days, Bledsoe was fully identified. The FBI obtained a search warrant for Bledsoe’s home to search for and seize evidence of his participation in the Capitol breach. Agents searched his home on January 15, 2021, and they seized two iPhones, among other items.

Bledsoe now moves to suppress evidence—including derivative evidence—from the cell phones seized. ECF 183. Bledsoe ignores facts from the affidavit<sup>1</sup> to boldly assert that probable cause was lacking. The Court should deny Bledsoe’s motion. First, the warrant described the electronic devices subject to seizure with sufficient particularity. Second, the search warrant

---

<sup>1</sup> The Search Warrant was issued in the United States District Court for the Western District of Tennessee in case number 21-SW-019. A copy of the Search Warrant and Search Warrant Application are attached as Exhibit A.

affidavit provided a sufficient nexus to establish the likelihood that the cell phones contained evidence of Bledsoe’s participation in the January 6 breach of the United States Capitol. Further, even if there is any reason to question the existence of probable cause—and there is not—law enforcement objectively, reasonably, and in good faith, relied upon the magistrate’s authorizations. Quite simply, the evidence should not be suppressed.

### **I. STATEMENT OF RELEVANT FACTS**

Bledsoe, a resident of Cordova, Tennessee, traveled to Washington, D.C. in advance of a joint session of the United States Congress, which was convened at the United States Capitol on January 6, 2021, to certify the vote count of the Electoral College of the 2020 Presidential Election.

A mass of individuals gathered outside of the United States Capitol on January 6. The Capitol, including the exterior plaza, was closed to members of the public. Exhibit A, Affidavit of FBI Task Force Office Kenneth Hale in Support of Search Warrant Application (“Hale Aff.”), ¶¶ 5–6. The Capitol doors and windows were locked or otherwise secured. Hale Aff., ¶ 9. Shortly after 2:00 p.m., while the joint session was underway, individuals in the crowd forced entry into the United States Capitol. Hale Aff., ¶ 9. Within minutes the joint session was suspended and Vice President Mike Pence and others evacuated the chambers. Hale Aff., ¶ 10. After the Capitol building was breached, Bledsoe found his way inside. Bledsoe’s trip to Washington, D.C. on January 6 was documented through photographs and videos which were posted to his Instagram account, “theessentialmattbledsoe”. Hale Aff., ¶¶ 13–16.

In the aftermath of the Capitol breach, the FBI was flooded with tips about the identities of individuals who entered the United States Capitol. One of those tips named Bledsoe as part of

a group that illegally entered the Capitol building on January 6. Agents followed up on the tip and were given the video compilation posted to Bledsoe’s Instagram account. Hale Aff., ¶ 12.

Agents watched the video compilation, which included several selfie photographs of Bledsoe and some video clips. The video compilation documented a crowd approaching the United States Capitol Building, a photograph of individuals scaling walls outside the Capitol Building, and clips of Bledsoe and his companions immediately outside an exterior door of the Capitol building while an alarm is blaring in the background, among other things. Hale Aff., ¶¶ 13–16. Bledsoe seemed to be walking and talking with a mobile device while videotaping his entry into the United States Capitol and a march through its halls. Hale Aff., ¶ 12.

In the very early stages of its investigation into Bledsoe, FBI agents were also alerted to a Facebook post by Bledsoe’s wife. Hale Aff., ¶ 19. The post asserted that her husband, Matt Bledsoe, was at the United States Capitol. Hale Aff., ¶ 19. Not only was he there, “he was one of the first.” Hale Aff., ¶ 19. She stated, “[w]e have lots of pictures and videos.” Hale Aff., ¶ 19.

On January 14, 2021, an FBI agent applied for a search warrant to search Bledsoe’s home in Cordova, Tennessee for evidence of Bledsoe’s alleged violations of unlawfully entering into the United States Capitol building and restricted grounds, and violent entry and disorderly conduct on Capitol Grounds. *See generally* Exhibit A. Based upon the information FBI agents learned about Bledsoe’s probable use of a mobile device to document his January 6 journey—and his wife’s post that they “have lots of pictures and videos”—the agent sought permission to search for information stored on “a computer’s hard drive or other storage media, including cell phones.” The agent articulated further reasons to justify a search of any “computer or storage medium, including a cell phone, found in Bledsoe’s home:

Individuals who engage in criminal activity, including violations of 18 U.S.C. § 1752(a) (Knowingly Entering or Remaining in any Restricted Building or Grounds without Lawful Authority) and 40 U.S.C. § 5014(e)(2) (Violent Entry and Disorderly Conduct on Capitol Grounds), use digital devices, like cell phones or computers, to access websites to facilitate illegal activity and to communicate with co-conspirators online; to store on digital devices, like cell phones or computers, documents and records relating to their illegal activity, which can include logs of online chats with co-conspirators; social media posting information; ... I also know that individuals who are involved in criminal conduct similar to what is described herein often use electronic devices, cellular telephones and computers to record activity and also to post recordings to social media. Individuals engaging in the conduct described herein usually keep their electronic devices close to their person or stored in their residence.

Hale Aff., ¶ 27(1).

A magistrate judge authorized the search warrant the same day. It permitted law enforcement to search Bledsoe's home and seize items related to the alleged crimes, including "[c]ellular telephones and other mobile devices, including tablets, cameras, mobile video cameras, and other mobile electronic devices," among other things. *See* Ex. A, p. 27 (Att. B).

Agents searched Bledsoe's home on the morning of January 15, barely more than a week after his trip to Washington, D.C. and the United States Capitol. Among the items seized were two iPhones—one in a black case and one in a green case. Ex. A, p. 31 (Return).

## **II. APPLICABLE LEGAL PRINCIPLES**

In evaluating probable cause, the assessment should be a "practical, common-sense decision whether, when given all the circumstances set forth in the affidavit ... there is a fair probability that contraband or evidence of a crime will be found in a particular place." *United States v. Cardoza*, 713 F.3d 656, 659 (D.C. Cir. 2013) (citing *Illinois v. Gates*, 462 U.S. 213 (1983)). The sufficiency of the showing underlying the issuance of a search warrant requires



“not a prima facie showing” but only a “fair probability.” *Gates*, 462 U.S. at 235. In *District of Columbia v. Wesby*, the Supreme Court recently further reaffirmed that:

Because probable cause deals with probabilities and depends on the totality of the circumstances, it is a fluid concept that is not readily, or even usefully, reduced to a neat set of legal rules. It requires only a probability or substantial chance of criminal activity, not an actual showing of such activity.

538 U.S. \_\_\_, 138 S. Ct. 577, 586 (2018) (citations and punctuation omitted).

As articulated by the Court, “[p]robable cause is not a high bar.” *Id.* Probable cause is satisfied when the search warrant application provides (1) a substantial basis for concluding that a search will uncover evidence of wrongdoing from a particular location, and (2) that a nexus exists between the item seized and criminal behavior. *United States v. Griffith*, 867 F.3d 1265, 1721 (D.C. Cir. 2017) (citations and punctuation omitted).

Moreover, “[u]nder *United States v. Leon*, [468 U.S. 897 (1984)] suppression of evidence is usually not required when officers conduct a search in reasonable reliance on a search warrant issued by a detached and neutral magistrate.” *Cardoza*, 713 F.3d at 658 (citing *Leon*, 468 U.S. at 913).

### **III. ARGUMENT**

This Court should deny Bledsoe’s Motion to Suppress data—and derivative evidence and information—recovered from the searches of cell phones seized from his home during execution of a search warrant.

#### **A. The search warrant application described the cell phones subject to seizure and search with sufficient particularity.**

The search warrant satisfied the constitutional requirement to describe the cell phones with particularity when it expressly authorized agents to search for and seize “cellular telephones and other mobile devices, ...” The Fourth Amendment requires that warrants “particularly

describe[e]” the “things to be seized.” U.S. Const. amend. IV. This requirement ensures that a search is “carefully tailored” to avoid a “wide-ranging exploratory search.” *Griffith*, 867 F.3d at 1275 (citing *Maryland v. Garrison*, 480 U.S. 79, 84 (1987)). However, the requirement of particularity does not preclude a general description of an object—such as a cell phone—when there is probable cause to seize it but specific information about the object is lacking. *Id.* at 1276. The court in *Griffith* described such a situation: “police might learn a suspect uses a phone through an informant” but “have no ability to describe the specific characteristics of any phone belonging to him.” *Id.* In this situation, in order to determine relevance to the investigation, devices fitting the general description of objects subject to seizure would need to “be examined, at least cursorily.” *Id.* (quoting *Andresen v. Maryland*, 427 U.S. 463, 482 n. 11 (1976)). Thus, greater latitude is preserved to search and seize electronic devices for which probable cause exists.

*United States v. Smith*, 2021WL 2982144 (D.D.C. July 15, 2021) (Howell, C.J.) exemplifies this principle. Officers investigating sexual assault allegations sought a warrant to seize electronic devices from the defendant’s home and search them for evidence of the crime. *Id.* at \*1. The officers did not have specific descriptions of the devices that may contain evidence, and only general language was included in the affidavit. The defendant argued that because the government could not readily identify the device it was seeking that allegedly contained evidence of his crimes, the scope of the warrant lacked particularity and was overbroad, requiring suppression of the evidence. *Id.* at \*7. This Court disagreed, finding that the defendant cited no authority requiring a precise description of the phone that may contain evidence of the crime. *Id.*

The hypothetical scenario described in *Griffith* is analogous to the reality of Bledsoe's case—the affiant had reason to believe that Bledsoe was in possession of mobile devices, including cell phones, containing evidence of the crimes under investigation, although the affiant was unable to describe the mobile devices with particularity. For instance, the video compilation posted on Bledsoe's Instagram, "theessentialmattbledsoe," included selfie-style photographs and videos that appeared to have been taken with a mobile device. Hale Aff., ¶ 12. And a post by Bledsoe's wife on her Facebook page boasting "[w]e have lots of pictures and videos" supported the conclusion that multiple devices in the home may contain evidence of Bledsoe's crimes. Hale Aff., ¶ 19. These factual predicates were sufficient to justify a search for "cell phones and other mobile devices" in Bledsoe's home. *Griffith*, 867 F.3d at 1276 ("with searches of lawful objects", "a broader sweep" may be allowed "when a reasonable investigation cannot produce a more particular description" of the items seized).

Bledsoe relies heavily on the reasoning in *Griffith* to justify suppression of evidence in his case. Even a cursory glance of *Griffith* highlights the flaws in this logic. First, *Griffith* involved the seizure of all electronic devices found in a residence when there was no evidence that the defendant used or owned a phone, much less any other electronic device. *Id.* at 1272. In fact, the defendant had been incarcerated for nearly a year prior to the search, a circumstance, the Court reasoned, that made it less likely the defendant owned or had ongoing access to a cell phone. *Id.* at 1273. The facts in Bledsoe's case stand in stark contrast. The post to his Instagram account approximately one week prior to the search supported the conclusion that he possessed a mobile device and used it to document his crimes.

Second, the affidavit supporting the search warrant in *Griffith* was void of a basis to believe that any phone would contain evidence of the crime. *Id.* at 1274. Such evidence is not

lacking in Bledsoe's case. The evidence in the affidavit was that a mobile device was used to record Bledsoe's participation in criminal acts then post photos and videos on the internet. Additionally, Bledsoe's wife boasted on her social media account that they kept evidence of Bledsoe's participation in the events of January 6, indicating she, too had access to a mobile device and incriminating evidence sought by the warrant.

**B. The search warrant application established a clear nexus between the cell phones and his criminal behavior.**

The search warrant also demonstrated "a nexus" between the evidence targeted by the warrant and the alleged "criminal behavior." *Griffith*, 867 F.3d at 1271 (citing *Groh*, 540 U.S. at 568); *Warden v. Hayden*, 387 U.S. 294, 307 (1967)). In evaluating whether a sufficient nexus exists, the judge is required to make "a practical common sense decision whether, given all the circumstances set forth in the affidavit ... there is a fair probability that [ ] evidence of a crime will be found in a particular place." *United States v. Ribeiro*, 397 F.3d 43, 48 (1st Cir. 2005) (quoting *Gates*, 462 U.S. at 238). "[T]he nature of the item and the normal inferences of where one would likely keep such evidence" may establish a nexus. *United States v. Anderson*, 851 F.2d 727, 729 (4th Cir. 1988); *see also Ribeiro*, 397 F.3d at 48.

The affidavit in this case set forth compelling facts and circumstances to support the reasonable conclusion that mobile devices, including cell phones, would contain evidence of Bledsoe's crimes. By way of example, the affidavit describes a video in which Bledsoe is standing immediately outside an exterior door of the Capitol and an alarm is heard blaring in the background. Hale Aff., ¶ 14. Bledsoe records himself as he enters the Capitol Building, and even announces his location: "In the Capitol. This is our house. We pay for this shit. Where's those pieces of shit at?" Hale Aff., ¶¶ 14–16. The compilation video posted to his Instagram account is seemingly a play-by-play of his movements to, on and through the Capitol Building



and grounds on January 6. The logical inference is that the photos and videos that made up the compilation posted to “theessentialmattbledsoe” were captured by a mobile device. Coupled with a post on his wife’s facebook account that “we have lots of pictures and videos” lends more than a “fair probability” that evidence would be found on the cell phones seized from Bledsoe’s home approximately one week from the Capitol breach.

C. **Even if probable cause was lacking—it is not—agents’ reasonably relied on the search warrant issued by the magistrate.**

Even assuming, *arguendo*, that the Court were to find that the warrant somehow lacked probable cause, the good faith reliance exception precludes the Court from applying the exclusionary rule to evidence recovered from the cell phone searches. *United States v. Leon*, 468 U.S. 897, 919 (1984) (“evidence obtained from a search should be suppressed only if it can be said that the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional under the Fourth Amendment”). Here, there is no evidence, argument or proffer put forth by Bledsoe that the affiant knew or should have known that the affidavit would not have passed constitutional muster. *Id.* at 916-17 (“[W]e discern no basis, and are offered none, for believing that exclusion of evidence seized pursuant to a warrant will have a significant deterrent effect on the issuing judge or magistrate ... Judges and magistrates are not adjuncts to the law enforcement team; as neutral judicial officers, they have no stake in the outcome of particular criminal prosecutions.”). Therefore, the warrant falls within the good faith reliance exception. *Id.* at 920 (finding that the exclusionary rule should not apply “when an officer acting with objective good faith has obtained a search warrant from a judge or magistrate and acted within its scope”). “In the ordinary case, an officer cannot be expected to question the magistrate’s probable-cause determination or his judgment that the form of the warrant is technically sufficient.” *United States v. Washington*, 775 F.3d 405, 407 (D.C.



Cir. 2014 (quoting *Leon*). In this case, the court’s probable-cause determination was technically sound and the agents were entitled to rely on it. “[W]e ordinarily do not suppress evidence seized pursuant to a search warrant unless the warrant affidavit was ‘so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable.’” *Cardoza*, 713 F.3d at 659. Bledsoe selectively ignores facts from the affidavit to argue that probable cause justifying the search of the cell phones found in Bledsoe’s residence was wholly absent—and he is wrong. There is nothing about the facts of this case or the facts contained in the warrant that would render law enforcement’s procedure—adhering to a lawfully issued warrant—unreasonable.

#### IV. CONCLUSION

For the foregoing reasons, the defendant’s motion to suppress evidence (ECF 183) should be denied.

Respectfully submitted,

MATTHEW M. GRAVES  
United States Attorney  
D.C. Bar No. 481052

By: /s/ Melanie L. Alsworth  
MELANIE L. ALSWORTH  
AR Bar No. 2002095  
Trial Attorney, Detailee  
601 D Street, NW  
Washington, DC 20530  
(202) 598-2285  
Melanie.Alsworth2@usdoj.gov

Jamie Carter  
Assistant United States Attorney  
D.C. Bar No. 1027970  
601 D Street, N.W.  
Washington, DC 20530  
(202) 252-6741  
Jamie.Carter@usdoj.gov

# **Exhibit A**

UNITED STATES DISTRICT COURT

for the
Western District of Tennessee

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



Case No. 21-SW-019

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

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

SEE ATTACHMENT A

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

SEE ATTACHMENT B

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

- Evidence of a crime;
Contraband, fruits of crime, or other items illegally possessed;
Property designed for use, intended for use, or used in committing a crime;
A person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Table with 2 columns: Code Section, Offense Description. Includes 18 USC 1752 (a)(1)-(2) and 40 USC 5104(e)(2)(D),(G).

The application is based on these facts:

SEE Attached AFFIDAVIT OF FBI TFO KENNETH HALE

- 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.

Handwritten signature of Kenneth Hale

Applicant's signature

KENNETH HALE, FBI TFO

Printed name and title

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

Date: January 14, 2021

Handwritten signature of Tu M. Pham

Judge's signature

City and state: MEMPHIS, TN

TU M. PHAM, CHIEF U.S. MAGISTRATE JUDGE

Printed name and title

# UNITED STATES DISTRICT COURT

for the  
Western District of Tennessee

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



)  
)  
)  
)  
)  
)

Case No. 21-SW-019

## WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

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

SEE ATTACHMENT A which is attached hereto and fully 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 which is attached hereto and fully incorporated herein by reference

**YOU ARE COMMANDED** to execute this warrant on or before 1/28/2021 *(not to exceed 14 days)*  
 in the daytime 6:00 a.m. to 10:00 p.m.  at any time in the day or night because good cause has been established.

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

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Tu M. Pham  
*(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: January 14, 2021 1:30 pm

*Judge's signature*

City and state: Memphis, TN

TU M. PHAM, Chief U.S. Magistrate Judge  
*Printed name and title*

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

**Return**Case No.:  
21-SW-019

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

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

**Certification**

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

Date: \_\_\_\_\_

\_\_\_\_\_  
*Executing officer's signature*\_\_\_\_\_  
*Printed name and title*



IN THE UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF TENNESSEE

IN THE MATTER OF THE SEARCH OF:





Case No. 21-SW-019

**STATEMENT IN SUPPORT OF AN  
APPLICATION UNDER RULE 41 FOR A  
WARRANT TO SEARCH AND SEIZE**

I, **Kenneth Hale**, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as   
 (“PREMISES”), further described in Attachment A, for the things described in Attachment B.

2. I am a federal deputized Task Force Officer (“TFO”) with the Federal Bureau of Investigation (“FBI”), and I have been a TFO since May 2019. Between November 2003 and May 2019, I served as an officer and detective with the Memphis Police Department. My training and experiences include the preparation of numerous criminal affidavits. I am currently assigned to the Joint Terrorism Task Force (“JTTF”) of the FBI Field Office, in Memphis, Tennessee. As a TFO, I have been involved in investigations of both international and domestic terrorism. During the course of these investigations, I have conducted or participated in physical and electronic

surveillance, assisted in the execution of search warrants, debriefed informants, and reviewed other pertinent records. Through my training, education, and experience, I have become familiar with the efforts of persons involved in criminal activity to avoid detection by law enforcement.

3. I am familiar with the facts and circumstances of this investigation, both from my own investigative activities and from information obtained from other law-enforcement officers and others with personal knowledge of the facts set forth in this affidavit. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this Affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1752(a), Knowingly Entering or Remaining in any Restricted Building or Grounds Without Lawful Authority, and 40 U.S.C. §5104(e)(2), Violent Entry and Disorderly Conduct on Capitol Grounds, have been committed by Mathew Bledsoe (“Bledsoe”). As explained below, there is also probable cause to search the **PREMISES**, described in Attachment A, for evidence of these crimes, instrumentalities of these crimes and contraband or fruits of these crimes, as described in Attachment B.

**PROBABLE CAUSE**

5. The U.S. Capitol, which is located at First Street, SE, in Washington, D.C., 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 are allowed access inside the U.S. Capitol.

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

7. On January 6, 2021, a joint session of the United States Congress convened at the United States Capitol. During the joint session, elected members of the United States House of Representatives and the United States Senate were meeting in separate chambers of the 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. Vice President Mike Pence was presiding in the Senate chamber.

8. With the joint session underway and with Vice President Mike Pence presiding, a large crowd gathered outside the U.S. Capitol. Temporary and permanent barricades surround the exterior of the U.S. Capitol Building. U.S. Capitol police were present and attempting to keep the crowd away from the Capitol buildings and the proceedings underway inside.

9. At approximately 2:00 p.m., certain individuals in the crowd forced their way through, up, and over the barricades and officers of the U.S. Capitol Police, and the crowd advanced to the exterior façade of the building. At such time, the joint session was 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. Shortly after 2:00 p.m., however, individuals in the crowd forced entry into the U.S. Capitol, including by breaking windows.

10. Shortly thereafter, at approximately 2:20 p.m., members of the United States House of Representatives and the 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 session resumed.

11. 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.

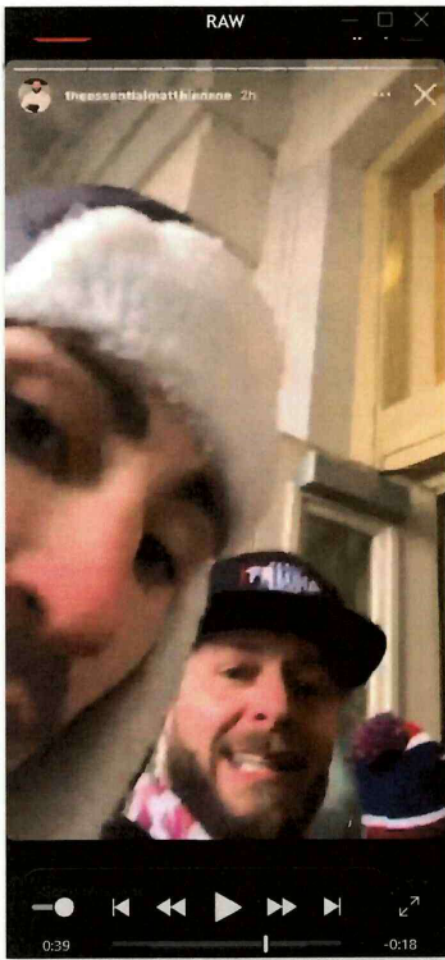
12. During the investigation into the events at the U.S. Capitol, FBI Agents received a tip that Matthew Bledsoe had been part of the group that illegally entered the U.S. Capitol. Upon following up, they received a video compilation that was posted to his Instagram account—theessentialmattbledsoe—which included several selfie photographs of Mr. Bledsoe throughout the day and some videos clips. These images appear to be captured by Mr. Bledsoe on a mobile device.

13. A video compilation posted on theessentialmattbledsoe Instagram account shows the crowd approaching the U.S. Capitol building. Another photo in the same video shows people climbing the walls of the building; it appears the person who took that photograph was located on top of the wall. This is followed by a selfie of an individual who appears to be Bledsoe, wearing a baseball hat with the words “TRUMP 2020.” All of these photographs appear to be from a mobile device.



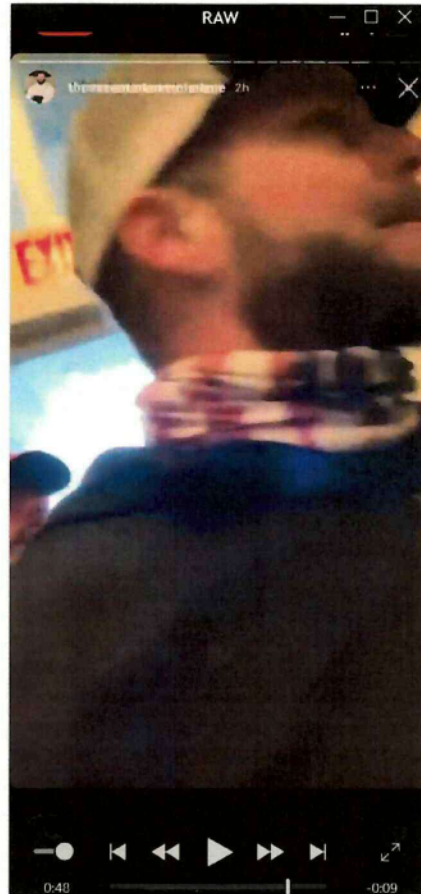
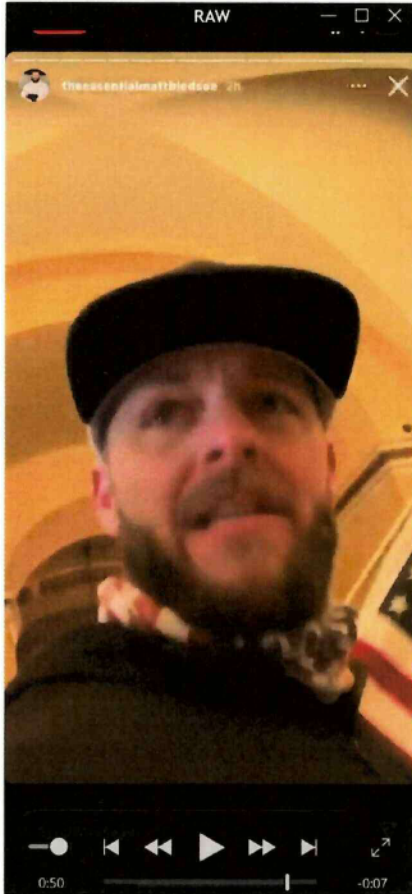


14. The compilation video on Bledsoe's Instagram account contains a clip of Mr. Bledsoe and his companions immediately outside an exterior door of the Capitol. An alarm can be heard blaring in the background. His companion says, "We're going in!" Mr. Bledsoe turns the camera from what appears to be a mobile device so that the camera shows the door, and he then says, "In the Capitol. This is our house. We pay for this shit. Where's those pieces of shit at?" As Mr. Bledsoe is walking and talking with what appears to be a mobile device, he continues to videotape while passing through the outer door and into the hallway. The two screenshots below show Mr. Bledsoe prior to entry.



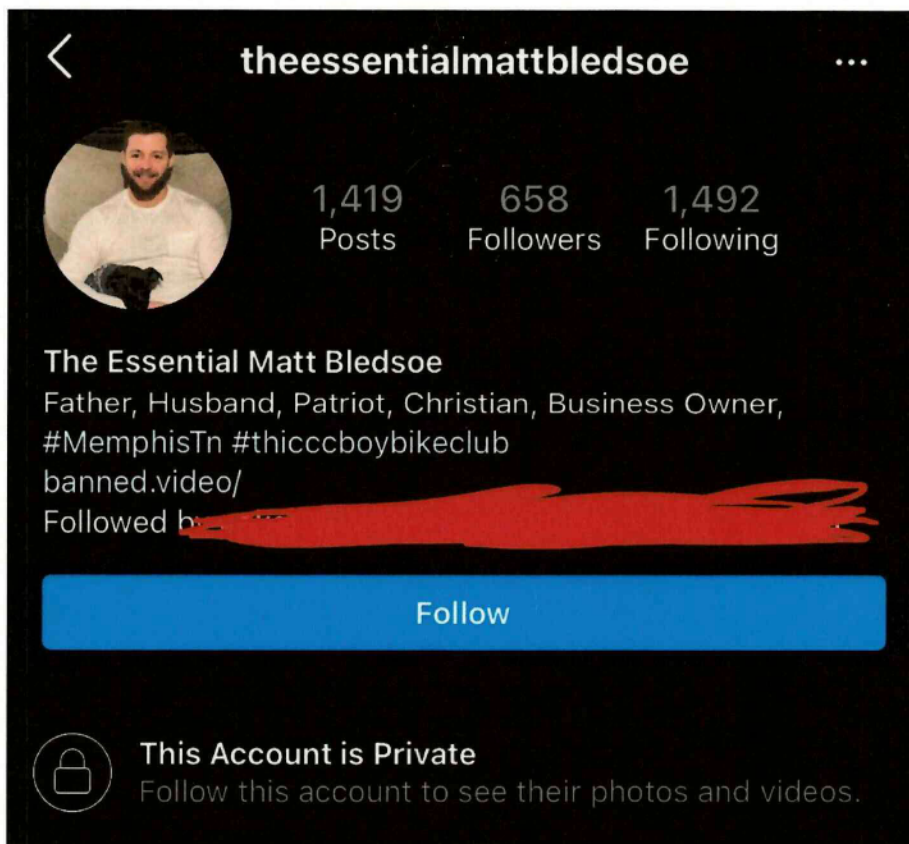


15. The following two photographs show him after entry into the U.S. Capitol:

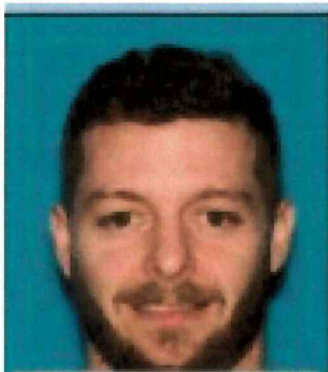


16. The video ends with another video clip captured by a person out of view of the camera where the crowd is chanting, "Stop the steal! Stop the steal!," as they march through the halls of the Capitol.

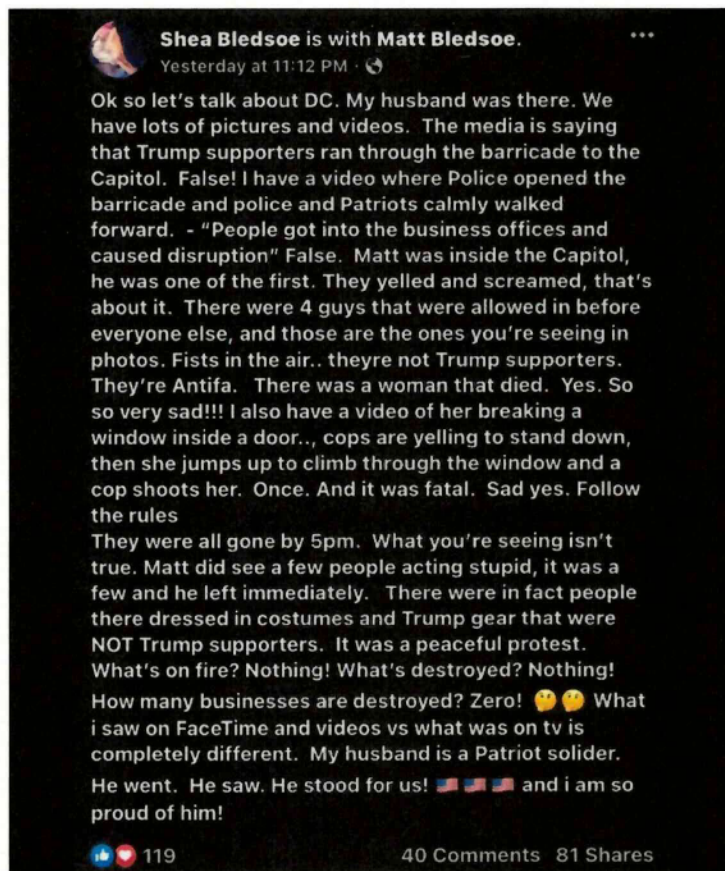
17. The FBI also received a screenshot of "theessentialmattbledsoe" Instagram home page from a confidential source who knows Bledsoe and who identified the Instagram account as belonging to Bledsoe. A copy of the screenshot of is below.



18. Mr. Bledsoe's identity was also checked against his driver's license photo, which shows him to be the same person shown in the video and photos above:



19. The source also led agents to a post by “Shea Bledsoe,” who is Mr. Bledsoe’s wife, in which Mrs. Bledsoe tags BLED SOE’s Facebook page. In the Facebook posting, Shea Bledsoe states, “Matt was inside the Capitol, he was one of the first.”



20. In addition, the FBI received a screenshot of Bledsoe’s Facebook page, from a confidential source who knows Matt Bledsoe and who identified the Facebook account as belonging to Matthew Bledsoe. The screenshot has the same picture and self-description as “Father, Husband, Patriot, Business Owner, #MemphisTn #thicboybieclub” as Bledsoe’s Instagram account. A copy of the screenshot is below:



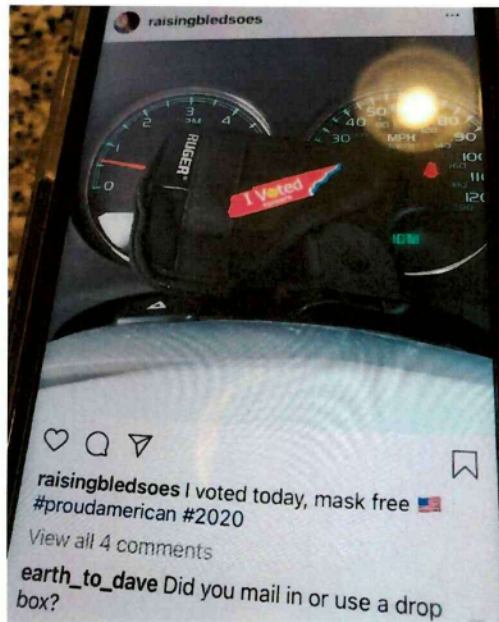
**Matt Bledsoe**

Father, Husband, Patriot, Business Owner,  
#MemphisTn #thicccboybikeclub

Add Friend

Owner and Founder at Primetime Movers

21. In addition, Mrs. Bledsoe previously posted the image below of a firearm on her Instagram account raisingbledsoes:





22. Since the above facts were obtained, all social media belonging to Matthew and Shea Bledsoe have been deleted.

23. On January 13, 2021, the FBI observed a dark-colored Ford F-250 parked in the drive-way of the residence located at the PREMISES. Based on FBI database checks, Bledsoe is the registered owner of a Ford F-250. The vehicle was backed into the drive-way so that a license tag could not be observed.

24. During the investigation, the FBI searched law-enforcement databases, which revealed that Matthew Bledsoe's physical address is the same as the PREMISES.

#### **TECHNICAL TERMS**

25. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.



- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

**COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

26. As described above and in Attachment B, this application seeks permission to search for records that might be found on the **PREMISES**, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media, including cell phones. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

27. *Probable cause.* I submit that if a computer or storage medium, including a cell phone, is found on the **PREMISES**, there is probable cause to believe that records related to Bledsoe's commission of the above-described offenses, and thus records that are evidence of these crimes, described in this statement will be stored on those electronic devices, for at least the following reasons:

- 1. Individuals who engage in criminal activity, including violations of 18 U.S.C. § 1752(a) (Knowingly Entering or Remaining in any Restricted Building or Grounds Without Lawful Authority) and 40 U.S.C. § 5104(e)(2) (Violent Entry and Disorderly Conduct on Capitol

Grounds), use digital devices, like cell phones or computers, to access websites to facilitate illegal activity and to communicate with co-conspirators online; to store on digital devices, like cell phones or computers, documents and records relating to their illegal activity, which can include logs of online chats with co-conspirators; social media posting information; email correspondence; text or other “Short Message Service” (“SMS”) messages; contact information of co-conspirators, including telephone numbers, email addresses, identifiers for instant messaging and social medial accounts; stolen financial and personal identification data, including bank account numbers, credit card numbers, and names, addresses, telephone numbers, and social security numbers of other individuals; and records of illegal transactions using stolen financial and personal identification data, to, among other things, (1) keep track of co-conspirator’s contact information; (2) keep a record of illegal transactions for future reference; (3) keep an accounting of illegal proceeds for purposes of, among other things, splitting those proceeds with co-conspirators; and (4) store stolen data for future exploitation. I also know that individuals who are involved in criminal conduct similar to what is described herein often use electronic devices, cellular phones and computers to record activity and also to post recordings to social media. Individuals engaging in the conduct described herein usually keep their electronic devices close to their person or stored in their residence.

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost.

Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

28. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files and/or mobile cellular data that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that

establishes how such devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the **PREMISES** because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet

history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline



information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing

is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

- f. I know that when an individual uses a computer to send or post messages over the Internet, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

29. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

30. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying digital devices and storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

31. I know from my training and experience, as well as from information found in publicly available materials, including those published by Apple, that some models of Apple devices, such as iPhones and iPads, offer their users the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, “fingerprint”) in lieu of a numeric or alphanumeric passcode or password. This feature is called Touch ID. Some models also allow users to unlock their devices by allowing the device to capture an image of the user’s face. The device then uses facial recognition software to unlock the device in lieu of a numeric or alphanumeric passcode or password. This feature is called Facial Recognition.

32. If a user enables Touch ID on a given Apple device, he or she can register up to 5 fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) found at the bottom center of the front of the device. In my training and experience, users of Apple devices that offer Touch ID often enable it because it is considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way

to protect the device's contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

33. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode or password must be used instead. These circumstances include: (1) when more than 48 hours has passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID in 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID exists only for a short time. Touch ID also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; and (3) five unsuccessful attempts to unlock the device via Touch ID are made.

34. The passcode or password that would unlock a target device is not known to law enforcement. Thus, it will likely be necessary to press the finger(s) of the user of the Apple iPhone to the device's Touch ID sensor, or to point the device's camera at Bledsoe's face, to activate Facial Recognition in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Attempting to unlock the target device in this manner is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

35. It is likely that Bledsoe is the user of the target device and thus that his fingerprints are among those that are able to unlock the device via Touch ID. Additionally, it is likely that Bledsoe's face would be able to unlock the device using Facial Recognition.



36. Although I do not know which of a given user's 10 fingerprints is capable of unlocking a particular device, based on my training and experience, I know that it is common for a user to unlock a Touch ID-enabled Apple device via the fingerprints on thumbs or index fingers. In the event that law enforcement is unable to unlock the Subject Device as described above within the five attempts permitted by Touch ID, this will simply result in the device requiring the entry of a password or passcode before it can be unlocked.

37. Due to the foregoing, I request that the Court authorize law enforcement to press the fingers (including thumbs) of Bledsoe to the Touch ID sensor of the device for the purpose of attempting to unlock the device via Touch ID in order to search the contents as authorized by this warrant.

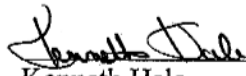
38. Because several people may share the **PREMISES** as a residence, it is possible that the **PREMISES** will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

39. Because electronic evidence can be accessed, destroyed, altered or manipulated remotely and without notice or indication of being accessed, authorization to execute this warrant as to any digital devices or other storage media recovered from the **PREMISES** at any time of the day or night is requested.

**CONCLUSION**

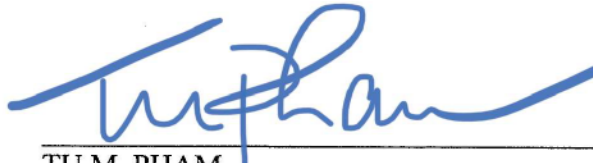
40. I submit that this affidavit supports probable cause for a warrant to search the **PREMISES** described in Attachment A and seize the items described in Attachment B.

AND FURTHER, AFFIANT SAITH NOT.



\_\_\_\_\_  
Kenneth Hale  
Task Force Officer  
Federal Bureau of Investigation

Attested to by the applicant in accordance with the requirements of Fed.R.Crim.P. 4.1 on January 14, 2021.



\_\_\_\_\_  
TU M. PHAM  
CHIEF UNITED STATES MAGISTRATE JUDGE  
WESTERN DISTRICT OF TENNESSEE

ATTACHMENT A



The property to be searched is [REDACTED] (“PREMISES”), including any outbuildings, appurtenances, storage areas, and vehicles found within the curtilage thereon.

**ATTACHMENT B**

*Property to be seized*

The items to be seized are fruits, evidence, or instrumentalities of and relating to violations of 18 U.S.C. § 1752(a), Knowingly Entering or Remaining in any Restricted Building or Grounds Without Lawful Authority; 40 U.S.C. §5104(e)(2), Violent Entry and Disorderly Conduct on Capitol Grounds:

This includes the following:

1. Cellular telephones and other mobile devices, including tablets, cameras, mobile video cameras, and other mobile electronic devices.
2. Clothing worn by Bledsoe on or around January 6, 2021, including a bandana or mask appearing to replicate an American flag, and a baseball hat with the words "TRUMP 2020."
3. ~~Information referring and relating to Bledsoe's state of mind from in and around December 2020 through January 2021, including information concerning violence.~~ TMP
4. Information referring and relating to the identity and location of perpetrators, aiders and abettors, coconspirators, and accessories after the fact.
5. Information referring and relating to any travel from in and around December 2020 through January 2021, including plans for travel, expenses, reservations, and other logistics.
6. Information referring and relating to any photographs and video concerning violence, incitement to riot, civil unrest, and the U.S. Capitol from in and around December 2020 through January 2021.
7. Information referring and relating to Bledsoe's activities in and around Washington, D.C., in or around January 2021.

8. Information referring and relating to the subject of the investigation and any co-conspirators, and criminal associates.

9. Information referring and relating to the offenses of 18 U.S.C. § 1752(a), Knowingly Entering or Remaining in any Restricted Building or Grounds Without Lawful Authority, and 40 U.S.C. §5104(e)(2), Violent Entry and Disorderly Conduct on Capitol Grounds.

10. Information referring and relating to Bledsoe's intentions for traveling to and from Washington, D.C., in or around January 6, 2021.

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

During the execution of the search of the PREMISES described in Attachment A, law enforcement personnel are also specifically authorized to obtain from BLEDSOE (but not any other individuals present at the PREMISES at the time of execution of the warrant) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint, facial characteristics, or iris display) necessary to unlock any Device(s) requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person(s)' physical biometric characteristics will unlock the Device(s), to



include pressing fingers or thumbs against and/or putting a face before the sensor, or any other security feature requiring biometric recognition of:

- (a) any of the Device(s) found at the PREMISES,
- (b) where the Device(s) are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,

for the purpose of attempting to unlock the Device(s)'s security features in order to search the contents as authorized by this warrant.

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

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

Original

Duplicate Original

# UNITED STATES DISTRICT COURT

for the  
Western District of Tennessee

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



Case No. 21-SW-019

## WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

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

SEE ATTACHMENT A which is attached hereto and fully 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 which is attached hereto and fully incorporated herein by reference

**YOU ARE COMMANDED** to execute this warrant on or before 1/28/2021 *(not to exceed 14 days)*  
 in the daytime 6:00 a.m. to 10:00 p.m.  at any time in the day or night because good cause has been established.

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

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Tu M. Pham  
*(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: January 14, 2021 1:30 pm

*Judge's signature*

City and state: Memphis, TN

TU M. PHAM, Chief U.S. Magistrate Judge  
*Printed name and title*

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

Return		
Case No.: 21-SW-019	Date and time warrant executed: 01/15/2021 @ 0600hrs	Copy of warrant and inventory left with: Kathryn S. Bledsoe
Inventory made in the presence of: Morgan Mitchell		
Inventory of the property taken and name(s) of any person(s) seized:		
<ol style="list-style-type: none"> <li>1. Silver HP laptop; model: 14-dk0002dk w/charger s/n 5C9931258C</li> <li>2. iPhone in black case</li> <li>3. iPhone in green case</li> <li>4. Trump hat</li> <li>5. Flag neck gaiter</li> <li>6. 1 black North Face Jacket; 1 Under Armour black quarter zip</li> </ol>		
Name: Matthew Bledsoe, <span style="background-color: black; color: black;">[REDACTED]</span> Arrested		
Certification		
I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.		
Date: 01/19/2021	<u>Kenneth Hale</u> <i>Executing officer's signature</i>	
	<u>Kenneth Hale / Task Force Officer</u> <i>Printed name and title</i>	