

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of
*(Briefly describe the property to be searched
or identify the person by name and address)*
5583 Leigh Run Ct., Columbus, OH 43228

)
)
)
)

Case No. 2:23-mj-678

APPLICATION FOR A SEARCH WARRANT

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

located in the Southern District of Ohio, 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:

<i>Code Section</i>	<i>Offense Description</i>
18 USC 111; 231; 1752(a)(2); 40 USC 5104(e)(2)(D)	assaulting, resisting, or impeding certain officers; civil disorder; disorderly and disruptive conduct in a restricted building or grounds; disorderly or disruptive conduct in the Capitol Buildings; entering or remaining on restricted buildings
18 USC 1752(a)(1)	

The application is based on these facts:

See attached affidavit.

- Continued on the attached sheet.
- Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Bradley R. Hajdin

Applicant's signature

Bradley R. Hajdin

Printed name and title

Sworn to before me and signed in my presence.

Date: Dec. 7, 2023

City and state: Columbus, OH

Kimberly A. Johnson

Kimberly A. Johnson
United States Magistrate Judge



UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF:
5583 Leigh Run Ct., Columbus, OH 43228
UNDER RULE 41

SW No. 2:23-mj-678

UNDER SEAL

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

I, Bradley Hajdin, 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 warrant to search the premises known as 5583 Leigh Run Ct., Columbus, OH 43228, hereinafter “PREMISES,” further described in Attachment A, for the things 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. I am a Special Agent with the Federal Bureau of Investigation (FBI). I have been in this position since December 2022. I am currently assigned to the Joint Terrorism Task Force

(JTTF) in the FBI Cincinnati Division, Columbus Resident Agency. I have spent most of my FBI career investigating, managing, and supporting international and domestic terrorism investigations which often involve violations of Title 18 of the United States Code. I have conducted or participated in physical surveillance, assisted in the execution of search warrants, debriefed informants and reviewed other pertinent records. Currently, I am tasked with investigating criminal activity in and around the Capitol grounds on January 6, 2021. As such, I am an “investigative or law enforcement officer” of the United States within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Section 2516 of Title 18, United States Code.

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

6. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that violations of 18 U.S.C. §§ 111 (assaulting, resisting, or impeding certain officers); 231 (civil disorder), 1752(a)(1) (entering or remaining in restricted buildings or grounds), 1752(a)(2) (disorderly and disruptive conduct in a restricted building or grounds) and 40 U.S.C. §§ 5104(e)(2)(D)(disorderly or disruptive conduct in the Capitol Buildings) (the “TARGET OFFENSES”) have been committed by KYLE ANDREW CAMPBELL (“the Subject”) and other identified and unidentified persons, including others who may have been aided and abetted by, or conspiring with, the Subject, as well as others

observed by the Subject. There is also probable cause to search the PREMISES, further described in Attachment A, for the things described in Attachment B.

PROBABLE CAUSE

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

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

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

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

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

11. On January 6, 2021, a joint session of the United States Congress convened at the U.S. Capitol. During the joint session, elected members of the United States House of Representatives and the United States Senate were meeting in separate chambers of the U.S. Capitol to certify the vote count of the Electoral College of the 2020 Presidential Election, which took place on November 3, 2020 (“Certification”). The joint session began at approximately 1:00 p.m. Eastern Standard Time (EST). Shortly thereafter, by approximately 1:30 p.m. EST, 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.

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

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

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

15. Media reporting showed a group of individuals outside of the Capitol chanting, “Hang Mike Pence.” I know from this investigation that some individuals believed that Vice

President Pence possessed the ability to prevent the certification of the presidential election and that his failure to do so made him a traitor.

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

17. Beginning shortly after 2:00 p.m. EST, individuals in the crowd forced entry into the U.S. Capitol, including by breaking windows and by assaulting members of law enforcement, as others in the crowd encouraged and assisted those acts. Publicly available video footage shows an unknown individual saying to a crowd outside the Capitol building, “We’re gonna fucking take this,” which your affiant believes was a reference to “taking” the U.S. Capitol.



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

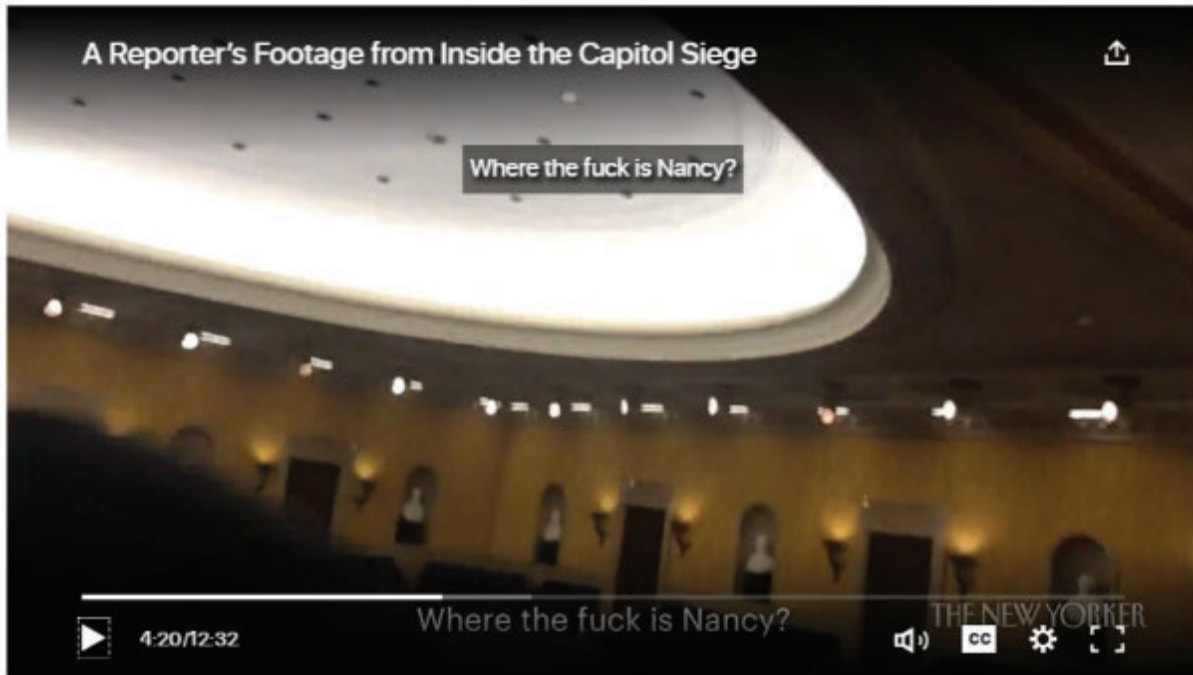
19. Between approximately 2:10 p.m, EST and 2:30 p.m. EST, Vice President Pence evacuated the Senate Chamber, and the Senate and House of Representatives were locked down and went into recess. Both the Senate and the House of Representatives Chamber were evacuated.

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

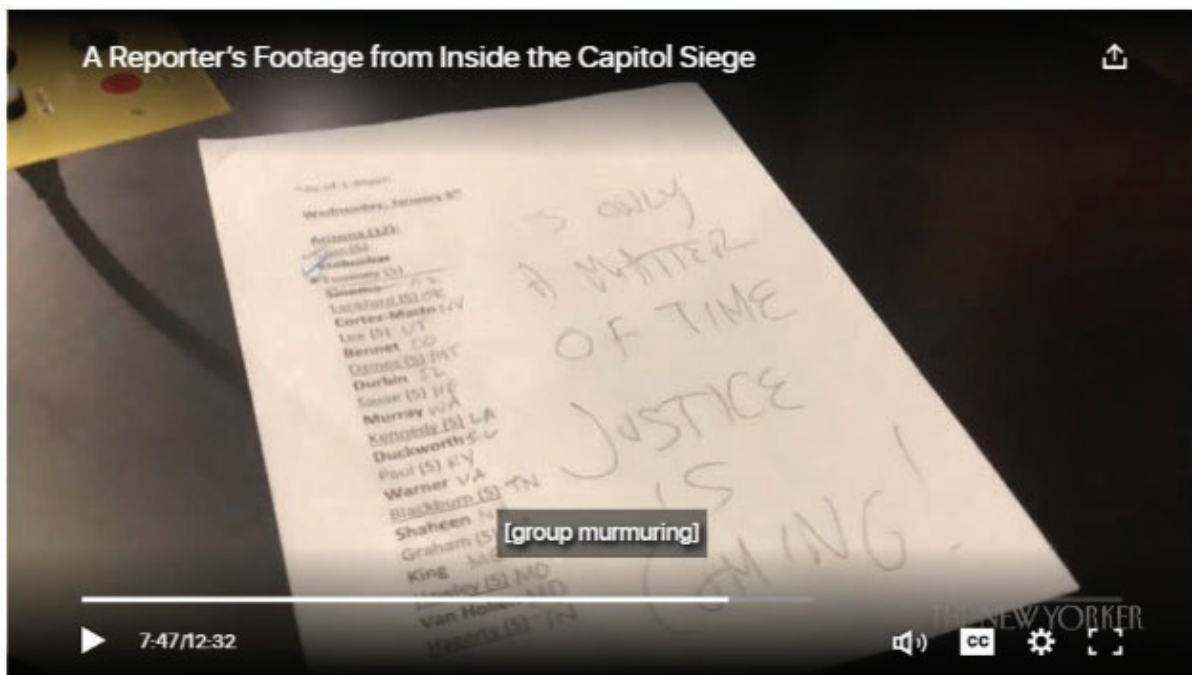
21. At around 2:47 p.m. EST, subjects broke into the Senate Chamber not long after I had been evacuated. Publicly available video shows an individual asking, “Where are they?” as they opened up the door to the Senate Chamber. Based upon the context, law enforcement believes that the word “they” is in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



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



23. 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.”



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





25. At around 2:48 p.m. EST, DC Mayor Muriel Bowser announced a citywide curfew beginning at 6:00 p.m. 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 building had been secured. Vice President Pence remained in the United States Capitol from the time he was evacuated from the Senate Chamber until the session resumed.

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

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

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

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

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

35. Many subjects seen on news footage in the area of the U.S. Capitol are using a cell phone in some capacity. It appears some subjects were recording the events occurring in and around the U.S. Capitol and others appear to be taking photos, to include photos and video of themselves after breaking into the U.S. Capitol itself, including photos of themselves damaging

and stealing property. As reported in the news media, others inside and immediately outside the U.S. Capitol live-streamed their activities, including those described above as well as statements about these activities.

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



1

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



2

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



Facts Specific to This Application

37. As part of its investigation of United States Capitol video footage, the FBI Washington Field Office's Violent Crimes Task Force identified an unknown male (SUBJECT 1) who was wearing a black jacket with a fur-trimmed hood amongst rioters who were attempting to overwhelm officers by breaching a police barricade on the Lower West Terrace of the Capitol on January 6, 2021. SUBJECT 1 (circled in red) can be seen pushing officers in multiple instances throughout video footage collected at the Capitol (see figures 1-4 below).

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



Figure 1

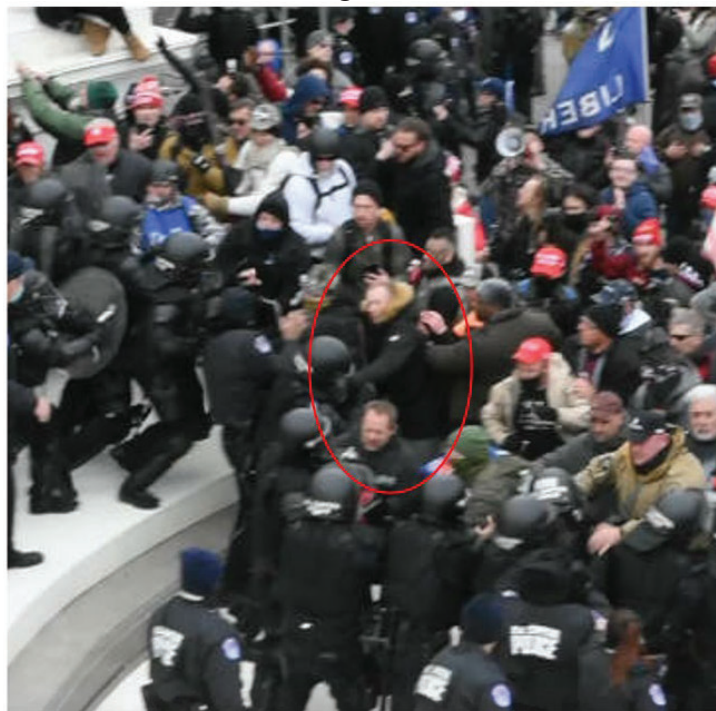


Figure 2



Figure 3



Figure 4

38. Seeking the public's assistance in identifying those who made unlawful entry into the Capitol, the FBI created bolos utilizing images of unknown subjects compiled from the footage. Bolo 521-AFO was created using images of SUBJECT 1 (Figure 5).



Figure 5

39. The FBI sought to identify SUBJECT 1 using open-source research and a pay-for-use facial comparison tool. Possible matches were made to the images below (see figures 6-7 below). These images were linked with identifiers related to an individual known as KYLE ANDREW CAMPBELL. The FBI subsequently searched law enforcement databases for KYLE ANDREW CAMPBELL, and identified a driver's license photo (Figure 8) which FBI personnel believed matched the photo of SUBJECT 1.



Figure 6



Figure 7

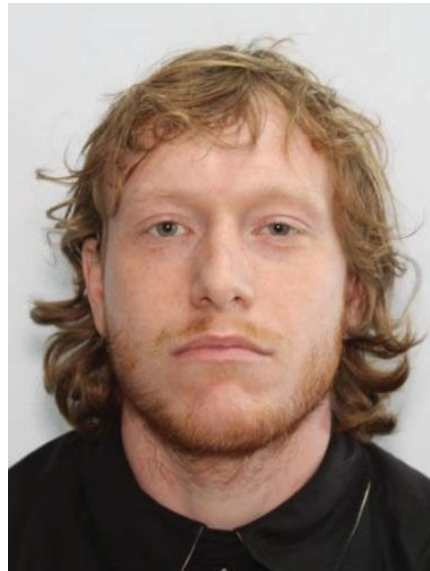


Figure 8

40. On or about April 8, 2022, a concerned citizen (C-1) provided a tip to the FBI regarding the potential identity and employment of SUBJECT 1. C-1 identified SUBJECT 1 as KYLE CAMPBELL who was employed by Allstate Insurance in Columbus, Ohio. C-1 also provided an image of CAMPBELL (Figure 9).

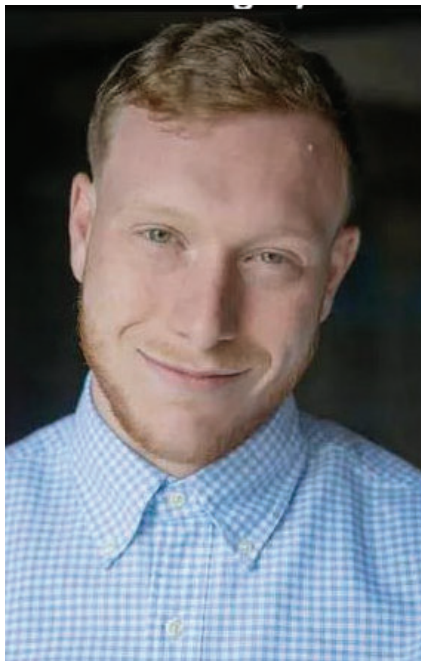


Figure 9

41. On or about April 15, 2022, a concerned citizen (C-2) provided a tip to the FBI identifying SUBJECT 1 as KYLE ANDREW CAMPBELL of Columbus, Ohio. C-2 noted that the coat worn by SUBJECT 1 on January 6 was identical to one worn by CAMPBELL on his social media accounts. C-2 provided identifying information for CAMPBELL, including his employment at the Frank A. Lengal Jr. Allstate Insurance office in Columbus, Ohio.

42. In May 2022, the FBI opened an investigation of CAMPBELL based on the multiple tips it received regarding him being involved with the events at the U.S. Capitol on January 6, 2021. As part of its investigation, the FBI conducted a facial recognition query of an image of CAMPBELL against archived open-source footage from January 6, 2021. The queries

yielded several photos of CAMPBELL (circled in yellow) outside the U.S. Capitol building on January 6, 2021, including photos of CAMPBELL moving past snow fencing erected by U.S. Capitol Police as part of the Restricted Perimeter around the U.S. Capitol (see figures 10-12 below).



Figure 10



Figure 11



Figure 12

43. In connection with its investigation, on or about February 3, 2023, the FBI interviewed CAMPBELL regarding his activities at the U.S. Capitol on January 6, 2021.

CAMPBELL advised that he did travel with an associate to the U.S. Capitol on January 6, 2021. CAMPBELL stated that he was close to the police line before he was pushed into it from behind, causing the police to push him back. He stated that he was not the aggressor in this situation and moved aside after getting sprayed by police. Once the police line had broken, CAMPBELL and his associate walked toward the Capitol building and milled around for approximately 45 minutes, after which the pair returned to Columbus, Ohio.

44. On November 22, 2022, FBI agents conducted surveillance at CAMPBELL's place of employment at the Frank A. Lengal Jr. Allstate Insurance office at 2000 Bethel Road in Columbus, OH. A vehicle registered to CAMPBELL was present in the office's parking lot. Agents positively identified CAMPBELL entering the vehicle, which they followed back to the residence.

45. FBI agents conducted surveillance at the PREMISES nine additional times between November 2022 and November 2023. On all of these occasions, the vehicle registered to CAMPBELL was parked outside of the residence. CAMPBELL was positively identified leaving the residence on five of instances.

46. Additionally, when CAMPBELL was interviewed in connection with the investigation by FBI agents on February 3, 2023, his interview took place at the PREMISES.

47. I know, based on my training and experience, that people routinely re-wear clothing and accessories, store these items in their homes, and keep them for an extended period. Clothing and accessories consistent with those worn by KYLE ANDREW CAMPBELL on January 6, 2021 constitute evidence of the commission of the offenses discussed herein, in that KYLE ANDREW

CAMPBELL can be visually identified as the individual in the photos and videos discussed above, in part through the distinct attire and accessories worn that day.

48. I also know, based on my training and experience, that cell phones are expensive, and people routinely retain their cell phones for many months or years.

49. Your affiant also knows that hundreds of people have been arrested in connection to the riot that occurred at the U.S. Capitol on January 6, 2021. During searches of many those people's homes, from early 2021 through present, in multiple jurisdictions, law enforcement has recovered clothing, paraphernalia, tools, and devices that were worn, used, or carried on January 6, 2021.

50. For example, on June 29, 2022, the home and adjacent barn of a defendant in the District of Rhode Island was searched, and agents recovered two handheld radios consistent with the radio that the defendant was photographed holding in Washington, D.C. on January 6, 2021. On January 13, 2023, a search conducted in the Eastern District of Virginia yielded a subject's cell phone used on January 6 and several items believed to be worn on January 6—including a backpack, a neck gaiter, a tricorne hat, and body armor. On February 1, 2023, the homes of two suspected rioters were searched in the Eastern District of Michigan. In one home, officers located clothing worn by the individual at the Capitol on January 6. In the other home, agents discovered both clothing as well as the stick/club this individual took into the Capitol as well as a protest sign he displayed that day. On April 11, 2023 in the Western District of Texas, an American flag neck gaiter, black pants, and a fleece-lined leather winter hat worn by a suspected rioter on January 6 were recovered in his home. On April 12, in the District of New Mexico, officers searched the home of a suspected rioter and recovered the chrome-colored goggles he wore on January 6. On

April 27, the homes of two suspected rioters were searched in the Middle District of Pennsylvania. In one home, officers recovered the blue Yamaha jacket the individual wore at the Capitol on January 6. In the other home, officers recovered a blue Trump hat the individual wore at the Capitol that day. On October 30, 2023, in the Eastern District of Missouri, two separate searches of two separate defendants successfully recovered items of clothing defendants wore to the Capitol on January 6 in addition to a cell phone and laptop with information related to January 6.

51. CAMPBELL has been observed wearing the black puffer jacket with a fur collar while under FBI surveillance as recently as November 29, 2023.

52. Records obtained from Verizon related to telephone number 937-510-4427 indicated that KYLE CAMPBELL was an authorized user on the account associated with this number. These records also showed that this number was associated with a 128 GB red Apple iPhone SE 20 during the billing period extending from December 22, 2020 to January 21, 2021.

53. Toll records obtained from Verizon revealed that the aforementioned telephone number was involved in approximately 27 calls on January 6, 2021. With each of these calls, the location of the number's device was logged. At approximately 5:03 am, the device logged its location as Columbus, OH when receiving a voicemail. At around 1:19 pm, an incoming call was received, with the device location being Washington, D.C. When interviewed by the FBI, CAMPBELL stated that he arrived in Washington around noon on January 6, 2021. Five other calls were noted in the records that indicated that the device was located in Washington, D.C., the latest of which was received at 3:59 pm. Additionally, a call was received at 11:43 pm that placed the device in Hebron, OH, a town approximately 30 miles east of Columbus. When interviewed, CAMPBELL stated that he arrived back to Columbus around 12:00 or 1:00 am on January 7.

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

55. Further, based on the investigation, numerous persons committing the TARGET OFFENSES possessed digital devices to communicate with other individuals to plan their attendance in Washington D.C. on January 6, 2021, to coordinate with other participants at the gatherings there that day, and to communicate and post on social media and digital forums about the events of January 6 after they occurred.

56. Moreover, it is well-known that virtually all adults in the United States use mobile digital devices. In a fact sheet from April 7, 2021, The Pew Research Center for Internet & Technology estimated that 97% of Americans owned at least one cellular phone, and that that same 2021 report estimated that 85% of Americans use at least one smartphone. *See* Mobile Fact Sheet, <https://www.pewresearch.org/internet/fact-sheet/mobile/> (last visited November 27, 2023).

57. In addition, in my training and experience, it is common for individuals to back up or preserve copies of digital media (such as photos and videos) across multiple devices to prevent loss. Indeed, some companies provide services that seamlessly sync data across devices, such as Apple devices and the Apple iCloud service. Thus, there is reason to believe that evidence of the offense that originally resided on the Subject's cell phone may also be saved to other digital devices within the PREMISES.

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

59. The property to be searched includes laptop computers, mobile phones, and/or tablets owned, used, or controlled by KYLE ANDREW CAMPBELL, including but not limited to a 128 GB red Apple iPhone SE 20, telephone number 937-510-4427, IMEI 356838111228220, IMSI 311480607714687, hereinafter the “Device(s).” Investigators have reason to believe that the Device(s) are currently located at PREMISES because it is CAMPBELL’s place of residence.

TECHNICAL TERMS

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

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

1) A “computer” means an electronic, magnetic, optical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e)(1). Computers are physical units of equipment that perform information

processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.

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

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

b. “Wireless telephone” (or mobile telephone, or cellular telephone), a type of digital device, is a handheld wireless device used for voice and data communication at least in part through radio signals and also often through “wi-fi” networks. When communicating via radio signals, these telephones send signals through networks of transmitters/receivers, enabling communication with other wireless telephones, traditional “land line” telephones, computers, and

other digital devices. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of applications and capabilities. These include, variously: storing names and phone numbers in electronic “address books”; sending, receiving, and storing text messages, e-mail, and other forms of messaging; taking, sending, receiving, and storing still photographs and video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; utilizing global positioning system (“GPS”) locating and tracking technology, and accessing and downloading information from the Internet.

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

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

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

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

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

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

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

COMPUTERS, ELECTRONIC/MAGNETIC STORAGE, AND FORENSIC ANALYSIS

60. As described above and in Attachment B, this application seeks permission to search for evidence, fruits, contraband, instrumentalities, and information that might be found on the PREMISES, in whatever form they are found. One form in which such items might be found is data stored on one or more digital devices. Such devices are defined above and include any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Thus, the warrant applied for would authorize the seizure of digital devices or, potentially, the copying

of stored information, all under Rule 41(e)(2)(B). Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that, if digital devices are found on the PREMISES, there is probable cause to believe that the items described in Attachment B will be stored in the Device(s) for at least the following reasons:

a. Individuals who engage in criminal activity, including trespassing at the U.S. Capitol on January 6, 2021, use digital devices like the Devices to save and share video and photographic evidence of their illegal activity in order to, among other things, garner credibility from like-minded individuals.

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

c. Digital device files, or remnants of such files, can be recovered months or even many years after they have been downloaded onto the medium or device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person “deletes” a file on a digital device such as a home computer, a smart phone, or a memory card, the data contained in the file does not actually disappear; rather, that data remains on the storage medium and within the device unless and until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the digital device that is not allocated to an active

file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a digital device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve “residue” of an electronic file from a digital device depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer, smart phone, or other digital device habits.

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

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

materials contained on the digital device(s) are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive, flash drive, memory card, or other electronic storage media image as a whole. Digital data stored in the Device(s), not currently associated with any file, 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 digital data on a hard drive that show what tasks and processes on a digital device were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on a hard drive, flash drive, memory card, or memory chip that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times a computer, smart phone, or other digital device was in use. Computer, smart phone, and other digital device file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

b. Forensic evidence on a digital device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, chats, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated

with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time, and potentially who did not.

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how such digital devices 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 digital device 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, digital device evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on digital devices is evidence may depend on other information stored on the devices and the application of knowledge about how the devices behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device 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 the device. For example, the presence or absence of counter-forensic programs, anti-virus programs (and associated data), and malware may be relevant to establishing the user's intent and the identity of the user.

METHODS TO BE USED TO SEARCH DIGITAL DEVICES

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

a. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time, in part because there are so many types of digital devices and software programs in use today. Digital devices – whether, for example, desktop computers, mobile devices, or portable storage devices – may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.

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

c. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else

to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a digital device is not segregable from the digital device itself. Analysis of the digital device as a whole to demonstrate the absence of particular data or software requires specialized tools and a controlled laboratory environment, and can require substantial time.

d. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear as though the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby thwarting “keyword” search techniques and necessitating continuous modification of keyword terms. Moreover, certain file formats, like portable document format (“PDF”), do not lend themselves to keyword searches. Some applications for computers, smart phones, and other digital devices, do not store data as searchable text; rather, the data is saved in a proprietary non-text format. Documents printed by a computer, even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography, a digital device user can conceal

text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband, or instrumentalities of a crime.

e. Analyzing the contents of mobile devices, including tablets, can be very labor intensive and also requires special technical skills, equipment, and software. The large, and ever increasing, number and variety of available mobile device applications generate unique forms of data, in different formats, and user information, all of which present formidable and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart phones and other mobile devices require passwords for access. For example, even older iPhone 4 models, running IOS 7, deployed a type of sophisticated encryption known as “AES-256 encryption” to secure and encrypt the operating system and application data, which could only be bypassed with a numeric passcode. Newer cell phones employ equally sophisticated encryption along with alpha-numeric passcodes, rendering most smart phones inaccessible without highly sophisticated forensic tools and techniques, or assistance from the phone manufacturer. Mobile devices used by individuals engaged in criminal activity are often further protected and encrypted by one or more third party applications, of which there are many. For example, one such mobile application, “Hide It Pro,” disguises itself as an audio application, allows users to hide pictures and documents, and offers the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.

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

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

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

1. Upon securing the PREMISES, law enforcement personnel will, consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, seize any digital devices (that is, the Device(s)), within the scope of this warrant as defined above, deemed capable of containing the information, records, or evidence described in Attachment B and transport these items to an appropriate law enforcement laboratory or similar facility for review. For all the reasons described above, it would not be feasible to conduct a complete, safe, and appropriate search of any such digital devices at the PREMISES. The digital devices, and/or any digital images thereof created by law enforcement sometimes with the aid of a technical expert, in an appropriate setting,

in aid of the examination and review, will be examined and reviewed in order to extract and seize the information, records, or evidence described in Attachment B.

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

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

BIOMETRIC ACCESS TO DEVICE(S)

64. This warrant permits law enforcement agents to obtain from the person of KYLE ANDREW CAMPBELL (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 or facial characteristics) 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). The grounds for this request are as follows:

65. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

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

67. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called “Trusted Face.” During the Trusted Face registration process, the user holds the device in front of his or her face. The device’s front-facing camera then analyzes and records data based on the user’s facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Apple’s “Face ID”) have different names but operate similarly to Trusted Face.

68. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called “Windows Hello.” During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user’s face and activates an infrared-sensitive camera to record data based on patterns within the user’s irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

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

70. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices, the Device(s), will be found during the search. The passcode or password that would unlock the Device(s) subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the Device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

71. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

72. Due to the foregoing, if law enforcement personnel encounter any Device(s) that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to obtain from the aforementioned person(s) the display of any physical biometric characteristics (such as

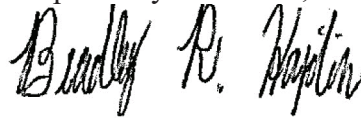
fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s), including to (1) press or swipe the fingers (including thumbs) of the aforementioned person(s) to the fingerprint scanner of the Device(s) found at the PREMISES; (2) hold the Device(s) found at the PREMISES in front of the face of the aforementioned person(s) to activate the facial recognition feature; and/or (3) hold the Device(s) found at the PREMISES in front of the face of the aforementioned person(s) to activate the iris recognition feature, for the purpose of attempting to unlock the Device(s) in order to search the contents as authorized by this warrant.

73. The proposed warrant does not authorize law enforcement to require that the aforementioned person(s) state or otherwise provide the password, or identify 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 proposed 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) would be permitted under the proposed warrant. 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.

CONCLUSION

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

Respectfully submitted,



Bradley R. Hajdin
Special Agent
Federal Bureau of Investigation

December 7, 2023



Kimberly A. Johnson
United States Magistrate Judge



ATTACHMENT A

Property to be searched

The property to be searched is 5583 Leigh Run Ct., Columbus, OH 43228 (the “PREMISES”), further described as a tan, two-story townhome located in the Edgemont Village community.





ATTACHMENT B

Property to be seized

1. The items to be seized are fruits, evidence, information, contraband, or instrumentalities, in whatever form and however stored, relating to violations of 111 (assaulting, resisting, or impeding certain officers); 231 (civil disorder), 1752(a)(1) (entering or remaining in restricted buildings or grounds); 1752(a)(2) (disorderly and disruptive conduct in a restricted building or grounds) and 40 U.S.C. §§ 5104(e)(2)(D)(disorderly or disruptive conduct in the Capitol Buildings) (the “TARGET OFFENSES”) that have been committed by KYLE ANDREW CAMPBELL (“the Subject”) and other identified and unidentified persons, as described in the search warrant affidavit; including, but not limited to:

- a. Evidence of the TARGET OFFENSES;
- b. Evidence concerning efforts after the fact to conceal evidence of those offenses, or to flee prosecution for the same;
- c. Evidence concerning materials, devices, or tools that were used to unlawfully commit the TARGET OFFENSES;
- d. Evidence of communication devices used in relation to the TARGET OFFENSES;
- e. Evidence concerning the identity of persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation; or (ii) communicated with the unlawful actors about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts.
- f. Evidence concerning planning to unlawfully enter the U.S. Capitol, including any maps or diagrams of the building or its internal offices;
- g. Evidence concerning unlawful entry into the U.S. Capitol, including any property of the U.S. Capitol;
- h. Evidence concerning the official proceeding that was to take place at Congress on January 6, 2021, i.e., the certification process of the 2020 Presidential Election;
- i. Evidence concerning efforts to obstruct, impede, or disrupt the official proceeding that was to take place at Congress on January 6, 2021, i.e., the certification process of the 2020 Presidential Election;
- j. Evidence concerning the breach and unlawful entry of the United States Capitol on January 6, 2021;

- k. Evidence concerning the riot and/or civil disorder at the United States Capitol on January 6, 2021;
- l. Evidence concerning the assaults of federal officers/agents and efforts to impede such federal officers/agents in the performance of their duties the United States Capitol on January 6, 2021;
- m. Evidence concerning damage to, or theft of, property at the United States Capitol on January 6, 2021;
- n. Evidence concerning awareness that the U.S. Capitol was closed to the public on January 6, 2021;
- o. Evidence of the defendant's presence at the U.S. Capitol on or around January 6, 2021;
- p. Evidence concerning the results of, challenges to, or questions about the legitimacy of the 2020 Presidential Election;
- q. Evidence regarding travel to Washington, D.C. in or around January 2021, motive and intent for travel to Washington, D.C. in or around January 2021, the planning of travel to and activity in Washington, D.C. on or about January 6, 2021, research about the U.S. Capitol, and mode of travel, travel expenses, and travel logistics on or about January 6, 2021.
- r. Evidence regarding the riot at the U.S. Capitol on January 6, 2021;
- s. Clothing and other items that reflect evidence of defendant's presence at the U.S. Capitol on January 6, 2021.

2. Records and information that constitute evidence of identity, including but not limited to:

- a. clothing worn by the subject, to include a black puffer jacket with a fur collar and black tennis shoes with white soles;
- b. clothing and other articles that reflect evidence of having participated in the unlawful activity at the U.S. Capitol, including evidence of pepper spray or other non-lethal crowd control remnants;

3. Address and/or telephone books and papers reflecting names, addresses and/or telephone numbers, which constitute evidence of conspirators and potential witnesses of violations of the TARGET OFFENSES.

4. Records and information—including but not limited to documents, communications, emails, online postings, photographs, videos, calendars, itineraries, receipts, and financial statements—relating to:

- a. Any records and/or evidence revealing the Subject's presence at the January 6, 2021, riot;
- b. Any physical records, such as receipts for travel, which may serve to prove evidence of travel of to or from Washington D.C. from November, 2020 through January, 2021;
- c. The Subject's (and others's) motive and intent for traveling to the U.S. Capitol on or about January 6, 2021; and
- d. The Subject's (and others's) activities in and around Washington, D.C., specifically the U.S. Capitol, on or about January 6, 2021.

5. Photographs, in particular photographs of the subject, co-conspirators, or events in Washington D.C. on January 6, 2021, which constitute evidence of the TARGET OFFENSES.

6. Evidence of relationships between members of a conspiracy, including evidence of identification and evidence of motivation to engage in TARGET OFFENSES.

7. Cellular telephones, SIM cards, computers, laptops, I-Pads, DVDs, hard drives, and electronic store devices, and receipts reflecting their ownership and use, which contain records of the commission of the TARGET OFFENSES.

8. Safes, both combination and key type, and their contents, which can contain evidence of the commission of the TARGET OFFENSES.

9. Indicia of ownership, including, receipts, invoices, bills, canceled envelopes, and keys, which provides evidence of identity as to individuals committing the TARGET OFFENSES; and

10. For any digital device which is capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities as described in the search warrant affidavit and above, hereinafter the “Device(s)”:

- a. evidence of who used, owned, or controlled the Device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, chat, instant messaging logs, photographs, and correspondence;
- b. evidence of software, or the lack thereof, that would allow others to control the Device(s), such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the attachment to the Device(s) of other storage devices or similar containers for electronic evidence;

- d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Device(s);
- e. evidence of the times the Device(s) was used;
- f. passwords, encryption keys, and other access devices that may be necessary to access the Device(s);
- g. documentation and manuals that may be necessary to access the Device(s) or to conduct a forensic examination of the Device(s);
- h. records of or information about Internet Protocol addresses used by the Device(s);
- i. records of or information about the Device(s)'s Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

During the execution of the search of the PREMISES described in Attachment A, law enforcement personnel are also specifically authorized to obtain from KYLE ANDREW CAMPBELL (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.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media

that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “digital devices” includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); security devices; and any other type of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions.

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.