

# **Exhibit A**

for the  
District of Colorado

Case No.

more fully described in Attachment A, attached hereto, to include all out-buildings and vehicles located thereon and to include the person of KLETE DERIK KELLER, if he is present at the time of the search warrant execution.

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 there is now concealed on the following person or property located in the State and District of Colorado (identify the person or describe property to be searched and give its location):

*Printed name and title*

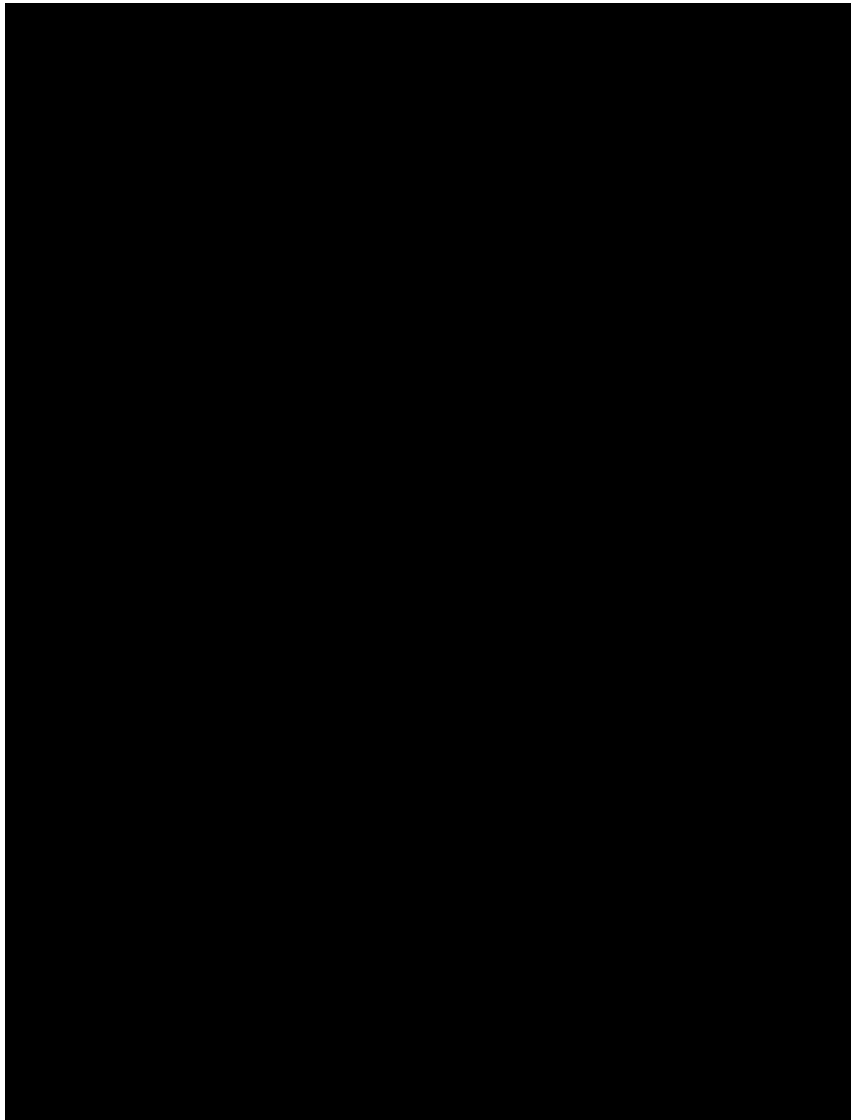
**ATTACHMENT A**

**DESCRIPTION OF LOCATION TO BE SEARCHED**

The Subject Premises is located at [REDACTED]

[REDACTED]. The location consists of the subject residence, surrounding property, and all outbuildings located thereon. The place to be searched includes the person of KLETE DERIK KELLER, if he is present on the subject premises at the time of the search warrant execution.

Photographs of the front and side of the Subject Premises are below:



## **ATTACHMENT B**

### **DESCRIPTION OF ITEMS TO BE SEIZED AND SEARCHED**

The following items, located at the Subject Premises that constitute evidence of the commission of, contraband, the fruits of crime, or instrumentalities of violations of 18 U.S.C. § 231(a)(3); 18 U.S.C. 1752(a)(1),(2); and 40 U.S.C. § 5104(e)(2) (the “Subject Offenses”), including the following:

1. Records and information relating to KLETE DERIK KELLER’s travel to the Washington D.C. area, on or around January 6, 2021;
2. Distinctive articles of clothing which would identify KLETE DERIK KELLER as the person in the videos of the Rotunda on January 6, 2021, including the USA Olympic jacket, the bandana or face covering, and the backpack which he appears to be wearing in the photos included with the affidavit in support of this search warrant;
3. Records and information which tend to establish ownership or use of digital devices and ownership or use of any Internet service accounts accessed to commit the Subject Offenses, to include credit card bills, telephone bills, correspondence and other identification documents;
4. Records and items that show dominion and control of the property searched, to include utility bills, telephone bills, correspondence, rental agreements and other identification documents.
5. Computers, which include all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices capable of performing logical, arithmetic, or storage functions, any physical object upon which computer data can be recorded, including desktop and laptop computers, computer hardware, computer software, volatile data, cellular telephones, tablets, server computers, gaming devices, network hardware, hard disk drives, RAM, floppy disks, flash memory, CDs, DVDs, and other magnetic or optical storage media, as well as, computer related documentation, computer passwords and data security devices, digital communications devices, cameras, videotapes, video recording devices, video recording players, and video display monitors, digital input and output devices such as keyboards, mouse(s), scanners, printers, monitors, electronic media and network equipment, modems, routers, connection and power cords, and external or connected devices used for accessing computer storage media that was used to commit or facilitate commissions of the Subject Offenses (collectively hereinafter, “COMPUTER”).

For any COMPUTER or storage medium whose seizure is otherwise authorized by this warrant, and any COMPUTER or storage medium that contains or in which is stored records or information that is otherwise called for by the warrant:

- a. Evidence of who used, owned, or controlled the COMPUTER at the time the items described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, calendars, browsing history, user profiles, e-mail, e-mail contacts, “chat” or instant messaging logs, photographs, and correspondence;
- b. Evidence of software that may allow others to control the COMPUTER, 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 lack of such malicious software;
- d. Evidence indicating how and when the COMPUTER was accessed or used to determine the chronological context of COMPUTER access, use, and events relating to the Subject Offense(s) and to the computer user;
- e. Evidence indicating the computer user’s state of mind as it relates to the Subject Offense(s);
- f. Evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. Evidence of the times the COMPUTER was used;
- i. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. Documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. Records of or information about the COMPUTER’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;
- l. Contextual information necessary to understand the evidence described in this attachment;
- m. Information about usernames or any online accounts or email addresses, including Instagram handle “██████,” Facebook account ██████, and Twitter;
- n. Volatile data necessary to preserve evidence prior to powering-off and unplugging a running computer;

- o. Information, notes, software, documents, records, or correspondence, in any format and medium, pertaining to the Subject Offense(s);
- p. Items otherwise described above in paragraphs of this Attachment B.

If KLETE DERIK KELLER is present at the time of the search warrant execution, executing law enforcement personnel are authorized to depress the fingerprints and/or thumbprints of KLETE DERIK KELLER onto the Touch ID or fingerprint sensor of any Apple iPhone, iPad, or other Apple brand device, or other device that has a fingerprint sensor, in order to gain access to the contents of any such device. Law enforcement personnel may also hold the device(s) found at the Subject Premises in front of the face of KLETE DERIK KELLER to activate the facial recognition feature; and/or (3) hold the device(s) found at the Subject Premises in front of the face of KLETE DERIK KELLER to activate the iris recognition feature, for the purpose of unlocking the device(s) in order to search the contents as authorized by this warrant.

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.

#### DEFINITIONS:

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, 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, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

## **AFFIDAVIT**

I, Brandon Kimble, being duly sworn, hereby depose and state that the following is true to the best of my information, knowledge, and belief:

### **INTRODUCTION AND AGENT BACKGROUND**

1. I am employed as a Special Agent of the Federal Bureau of Investigation (FBI) and have been so employed since 2016. Currently, I am assigned to a squad that investigates Domestic Terrorism matters as part of the FBI Denver Field Office. The focus of my Domestic Terrorism efforts has been investigating anti-government extremism. My squad is based at the Denver Field Office. As a Special Agent, I am authorized to investigate violations of laws of the United States and am authorized to execute warrants issued under the authority of the United States. My duties with the FBI include but are not limited to the investigation of Domestic Terrorism matters.
2. This affidavit is submitted in support of an application for a search warrant for the place described in Attachment A (hereinafter "Subject Premises"), and the computer(s) located therein, there being probable cause to believe that located in the place described in Attachment A are items described in Attachment B, being evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 231(a)(3), Obstructing Law Enforcement Engaged in Official Duties Incident to Civil Disorder; 18 U.S.C. 1752(a)(1),(2), Knowing 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 (the "Subject Offenses").
3. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of the Subject Offenses are presently located at the Subject Premises.
4. The information contained within the affidavit is based on my training and experience, as well as information imparted to me by other law enforcement officers involved in this investigation.

### **TECHNICAL TERMS**

5. Based on my training and experience, I use the following technical terms to convey the following meanings:
6. In this affidavit, the terms "computers" or "digital storage media" or "digital storage devices" may be used interchangeably, and are intended to include all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices capable of performing logical, arithmetic, or storage functions, any physical object upon which computer data can be recorded, including desktop and laptop computers, computer hardware, computer software, volatile data, cellular telephones, tablets, server computers,

gaming devices, network hardware, hard disk drives, RAM, floppy disks, flash memory, CDs, DVDs, and other magnetic or optical storage media, as well as, computer related documentation, computer passwords and data security devices, digital communications devices, cameras, videotapes, video recording devices, video recording players, and video display monitors, digital input and output devices such as keyboards, mouse(s), scanners, printers, monitors, electronic media and network equipment, modems, routers, connection and power cords, and external or connected devices used for accessing computer storage media that was used to commit or facilitate commissions of the Subject Offense(s) (collectively hereinafter, “computers”).

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

7. As described above and in Attachment B, I submit that if computers are found at the Subject Premises, there is probable cause to search and seize those items for the reasons stated below. Some of these electronic records might take the form of files, documents, and other data that is user-generated. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis. They may be seized and searched on-scene, and/or searched off-scene in a controlled environment.
8. For example, based on my knowledge, training, and experience, I know that a powered-on computer maintains volatile data. Volatile data can be defined as active information temporarily reflecting a computer’s current state including registers, caches, physical and virtual memory, network connections, network shares, running processes, disks (floppy, tape and/or CD-ROM), and printing activity. Collected volatile data may contain such information as opened files, connections to other computers, passwords used for encryption, the presence of anti-forensic tools, or the presence of programs loaded in memory that would otherwise go unnoticed. Volatile data and its corresponding evidentiary value is lost when a computer is powered-off and unplugged.
9. 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. 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.
10. Also, again based on my training and experience, wholly apart from user-generated files, computer storage media contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation,



file system data structures, virtual memory “swap” or paging files, and shadow copies of previous versions of systems or files, 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. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted, edited, moved, or show a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). 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.

11. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for evidence that establishes how computers were used, why they were used, the purpose of their use, and the purposes to which they were put, who used them, the state of mind of the user(s), and when they were used.
12. The monitor and printer show the nature and quality of the images or files that the system can produce. In addition, the analyst needs all assisting software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instructional manuals or other documentation and security devices. Moreover, searching computerized information for evidence or instrumentalities of crime commonly requires the seizure of the entire computer’s input/output periphery devices (including related documentation, passwords and security devices) so that a qualified expert can accurately retrieve the system’s data in a controlled environment.
13. The computer and its storage devices, the mouse, the monitor, keyboard, printer, modem and other system components are also used as instrumentalities of the crime to operate the computer to commit the offenses discussed in this affidavit. Devices such as modems and routers can contain information about dates, IP addresses, MAC addresses, frequency, and computer(s) used to access the Internet or to otherwise commit the crimes described herein. The computer equipment may also have fingerprints on them indicating the user of the computer and its components.
14. Similarly, information or files related to the crimes described herein are often obtained from the Internet or the cellular data networks using application software which often leaves files, logs or file remnants which would tend to show the identity of the person engaging in the conduct as well as the method of location or creation of the images, search terms used, exchange, transfer, distribution, possession or origin of the files. Files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.” The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

15. "User attribution" evidence can also be found on a computer and 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, "chat," instant messaging logs, photographs, videos, 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 computer or storage medium at a relevant time. 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.
16. Your Affiant knows from training and experience that digital software or hardware exists that allows persons to share digital access over wired or wireless networks allowing multiple persons to appear on the Internet from the same IP address. Examination of these items can reveal information about the authorized or unauthorized use of Internet connection at the residence.
17. Searching computer(s) for the evidence described in the attachment may require a range of data analysis techniques. For example, information regarding user attribution or Internet use is located in various operating system log files that are not easily located or reviewed. Or, a person engaged in criminal activity will attempt to conceal evidence of the activity by "hiding" files or giving them deceptive names. As explained above, because the warrant calls for records of how a computer has been used, what it has been used for, and who has used it, it is exceedingly likely that it will be necessary to thoroughly search storage media to obtain evidence, including evidence that is not neatly organized into files or documents. Just as a search of a premises for physical objects requires searching the entire premises for those objects that are described by a warrant, a search of this premises for the things described in this warrant will likely require a search among the data stored in storage media for the things (including electronic data) called for by this warrant. Additionally, it is possible that files have been deleted or edited, but that remnants of older versions are in unallocated space or slack space. This, too, makes it exceedingly likely that in this case it will be necessary to use a multitude of techniques, both on and off-scene, including more thorough techniques.
18. Based upon my knowledge, training and experience, I know that a thorough search for information stored in digital storage media requires a variety of techniques that often includes both on-site seizure and search as well as a more thorough review off-site review in a controlled environment. This variety of techniques is required, and often agents must seize most or all storage media to be searched on-scene and/or later in a controlled environment. These techniques are 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.

19. For example, the search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following on-site techniques (the following is a non-exclusive list, as other on-site search procedures may be used):
- A. On-site triage of computer systems to determine what, if any, peripheral devices or digital storage units have been connected to such computer systems, a preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or potential victims, and a scan for encryption software;
  - B. On-site copying and analysis of volatile memory, which is usually lost if a computer is powered down, and may contain information about how the computer is being used, by whom, when, and may contain information about encryption, virtual machine software (virtual operating systems that are lost if the computer is powered down or encrypted);
  - C. On-site forensic imaging of any computers may be necessary for computers or devices that may be partially or fully encrypted, in order to preserve unencrypted electronic data that may, if not immediately imaged on-scene, become encrypted and accordingly unavailable for any examination.
20. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include off-site techniques since it is often necessary that some computer equipment, peripherals, instructions, and software be seized and examined off-site and in a controlled environment. This is true because of the following:
- A. The nature of the evidence. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how, when and why a computer has been used, by whom, what it has been used for, requires considerable time, and taking that much time on premises could be unreasonable. Also, because computer evidence is extremely vulnerable to tampering and destruction (both from external sources and from code embedded in the system as a “booby-trap”), the controlled environment of a laboratory may be essential to its complete and accurate analysis. Searching for and attempting to recover any deleted, hidden, or encrypted data may be required to determine whether data falls within the list of items to be seized as set forth herein (for example, data that is encrypted and unreadable may not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of child exploitation offenses).
  - B. The volume of evidence and time required for an examination. Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the

stored data to determine which particular files are evidence or instrumentalities of crime. 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. Reviewing 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.

- C. 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-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- D. 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.
- E. Need to review evidence over time and to maintain entirety of evidence. Your Affiant recognizes the prudence requisite in reviewing and preserving in its original form only such records applicable to the violations of law described in this Affidavit and in Attachment B in order to prevent unnecessary invasion of privacy and overbroad searches. Your Affiant advises it would be impractical and infeasible for the Government to review the mirrored images of digital devices that are copied as a result of a search warrant issued pursuant to this Application during a single analysis. Your Affiant has learned through practical experience that various pieces of evidence retrieved from digital devices in investigations of this sort often have unknown probative value and linkage to other pieces of evidence in the investigation until they are considered within the fluid, active, and ongoing investigation of the whole as it develops. In other words, the weight of each individual piece of the data fluctuates based upon additional investigative measures undertaken, other documents under review, and incorporation of evidence into a consolidated whole. Analysis is content-relational, and the importance of any associated data may grow whenever further analysis is performed. In the past, your Affiant has reviewed activity and data on digital devices pursuant to search warrants in the course of ongoing criminal investigations. Your affiant has learned from that experience, as well as other investigative efforts, that multiple reviews of the data at different times are necessary to understand the full value of the information contained therein, and to determine whether it is within the scope of the items sought in Attachment B. In order to obtain the full picture and meaning of the data from the information sought in Attachment B of this application, the Government would need to

maintain access to all of the resultant data, as the completeness and potential for probative value of the data must be assessed within the full scope of the investigation. As such, your Affiant respectfully requests the ability to maintain the whole of the data obtained as a result of the search warrant, and to maintain and to review the data in the control and custody of the Government and law enforcement at times deemed necessary during the investigation. As with all evidence, the Government will maintain the evidence and mirror images of the evidence in its custody and control, without alteration, amendment, or access by persons unrelated to the investigation.

21. Based on the foregoing, and consistent with Rule 41(e)(2)(B), when persons executing the warrant conclude that it would be impractical to review the media on-site, the warrant I am applying for permits both on-site seizing, imaging and searching, and off-site imaging and searching of storage media that reasonably appear to contain some or all of the evidence described in the warrant, thus permitting its later and perhaps repeated examination consistent with the warrant. The examination 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.
22. Because several people may share the Subject Premises as a residence, it is possible that the Subject Premises will contain computers that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the items 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.
23. Your Affiant knows from training and experience that digital storage devices can be very large in capacity, yet very small in physical size. Additionally, your Affiant knows from training and experience that those who are in possession of such devices also tend to keep them on their persons, especially when they may contain contraband or other evidence of a crime. The storage capacity of such devices can be as large as tens of gigabytes in size as further described below, which allows for the storage of thousands of images and videos as well as other digital information such as calendars, contact lists, programs and text documents. Such storage devices can be smaller than a postage stamp in size, which allows them to be easily hidden in a person's pocket. KELLER is known to have a personal cell phone, telephone number [REDACTED] 9333. Sprint Corporation is the service provider for this telephone number. Keller is also featured showing what is believed to be an android cellular phone in an August 27, 2021 news video. Keller's phone has the app "Wag" pulled up on the screen with a notification icon for Facebook visible.<sup>1</sup>
24. 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

---

<sup>1</sup> This video is publicly accessible on the Internet at the following URL: <https://www.fox21news.com/news/local/dog-sitting-gone-wild-owner-comes-home-to-find-shirtless-men-lube-in-living-room/>

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.

25. 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 fingerprints authorized to access the particular device are a part of the security settings of the device and will allow access to the device in lieu of entering a numerical passcode or longer alpha-numerical password, whichever the device is configured by the user to require.
26. The Touch ID feature only permits up to five attempts with a fingerprint before the device will require the user to enter a passcode. Furthermore, if the device is equipped with an operating system that is earlier than version 9.3, the Touch ID feature will not substitute for the use of a passcode or password if more than 48 hours have passed since the device has been unlocked; in other words, if more than 48 hours have passed since the device was accessed, the device will require the passcode or password programmed by the user and will not allow access to the device based on a fingerprint alone. If the operating system is version 9.3 or later, that time frame shrinks to 8 hours.
27. Similarly, Touch ID will not allow access if the device has been turned on or restarted, if the device has received a remote lock command, or if five attempts to match a fingerprint have been unsuccessful. For these reasons, it is necessary to use the fingerprints and thumbprints of any device’s users to attempt to gain access to any Apple devices found at the Subject Premises while executing the search warrant. The government may not be able to obtain the contents of the Apple devices if those fingerprints are not used to access the Apple devices by depressing them against the Touch ID button. Although I do not know which of the ten finger or fingers are authorized to access on any given Apple device and only five attempts are permitted, I know based on my training and experience that it is common for people to use one of their thumbs or index fingers for Touch ID, and in any event, all that would result from successive failed attempts is the requirement to use the authorized passcode or password.
28. In addition, I know from my training and experience that many other mobile device manufactures have their own version of Touch ID—that is, a fingerprint recognition feature that the device’s user can program and use to unlock the device. For instance, I know that Google Pixel phones and Google Pixel XL phones have a fingerprint sensor that can be used to unlock the device. Similarly, Samsung, LG, HTC, and other manufacturers also have devices with fingerprint sensors.

29. Similarly, in my training and experience I know that some applications loaded onto mobile devices or other electronic devices may be secured by the user with a thumbprint or fingerprint. Common among these types of applications are applications such as mobile banking apps or other financial applications, password storage applications, and secure communications apps, among others.
30. Further, 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.
31. Similarly, 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.
32. 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.
33. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices 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.
34. Due to the foregoing, I am informing the Court that if law enforcement personnel encounter any Device(s) that are subject to seizure pursuant to the requested warrants and may be unlocked using one of the aforementioned biometric features, law enforcement personnel intends to obtain from KLETE DERIK KELLER 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 KLETE DERIK KELLER to the fingerprint scanner of the Device(s) found at the Subject Premises; (2) hold the Device(s) found at the Subject Premises in front of the face of KLETE DERIK KELLER to activate the facial recognition feature; and/or (3) hold the Device(s) found at the Subject Premises in front of the face of KLETE DERIK KELLER to activate the iris recognition feature, for the purpose of unlocking the Device(s) in order to search the contents as authorized by this warrant.

35. Your Affiant knows from training and experience that search warrants of residences involved in computer or digitally related criminal activity usually produce items that tend to establish ownership or use of digital devices and ownership or use of any Internet service accounts accessed to commit the crimes described in this affidavit, to include credit card bills, telephone bills, correspondence and other identification documents.
36. Your Affiant knows from training and experience that search warrants of residences usually reveal items that tend to show dominion and control of the property searched, to include utility bills, telephone bills, correspondence, rental agreements and other identification documents.
37. Your Affiant knows from training and experience that seized computers may contain communications to/from an attorney. If the government identifies seized communications to/from an attorney, the investigative team will discontinue review until a filter team of one or more government attorneys and other government personnel, as needed, is established. The filter team will have no previous or future involvement in the investigation of this matter. The filter team will identify and segregate communications to/from attorneys, which may or may not be subject to attorney-client privilege. At no time will the filter team advise the investigative team of the substance of any of the communications to/from attorneys. The filter team then will provide all communications that do not involve an attorney to the investigative team, and the investigative team may resume its review. If the filter team believes that any of the communications to/from attorneys are not actually privileged (e.g., the communication includes a third party), and if the investigation is not covert, the filter team will first seek to obtain agreement from the appropriate defense counsel before providing these attorney communications to the investigative team. If consulting with defense counsel is not possible or does not produce an agreement, the filter team will obtain a court order before providing these attorney communications to the investigative team.

### **INVESTIGATION**

38. The United States Capitol (the Capitol), which is located at First Street, SE, in Washington, D.C., is secured 24 hours a day by United States Capitol Police (Capitol Police). Restrictions around the Capitol include permanent and temporary security barriers and posts manned by Capitol Police. Only authorized people with appropriate identification are allowed access inside the Capitol. On January 6, 2021, the exterior plaza of the Capitol was closed to members of the public.
39. On January 6, 2021, a joint session of the United States Congress convened at the 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 Capitol to certify the vote count of the Electoral College of the 2020 Presidential Election, which had taken place on November 3, 2020. The joint session began at approximately 1:00 p.m. Shortly thereafter, by approximately 1:30 p.m., the House and Senate adjourned to separate chambers to resolve a particular objection. Vice President of the United States Michael R. Pence was present and presiding, first in the joint session, and then in the Senate chamber.

40. As the proceedings continued in both the House and the Senate, and with Vice President Pence present and presiding over the Senate, a large crowd gathered outside of the Capitol. As noted above, temporary and permanent barricades were in place around the exterior of the Capitol building, and Capitol Police were present and attempting to keep the crowd away from the Capitol building and the proceedings underway inside.
41. At approximately 2:00 p.m., certain individuals in the crowd forced their way through, up, and over the barricades and Capitol Police officers, and 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 Capitol Police Officers or other authorized security officials.
42. At such time, the certification proceedings were still underway, and the exterior doors and windows of the Capitol were locked or otherwise secured. Capitol Police officers attempted to maintain order and keep the crowd from entering the Capitol; however, shortly after 2:00 p.m., individuals in the crowd forced entry into the Capitol, including by breaking windows and by assaulting members of the Capitol Police, as others in the crowd encouraged and assisted those acts.
43. Shortly thereafter, at approximately 2:20 p.m., members of the House and Senate, including Vice President Pence serving as the President of the Senate, were instructed to—and did—evacuate the chambers. Accordingly, all proceedings of the United States Congress, including the joint session, were effectively suspended until shortly after 8:00 p.m. the same day.
44. In light of the dangerous circumstances caused by the unlawful entry to the Capitol, including the danger posed by individuals who had entered the Capitol without any security screening or weapons check, Congressional proceedings could not resume until after every unauthorized occupant had left the Capitol, and law enforcement could confirm the building had been secured. The proceedings resumed at approximately 8:00 p.m. 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.
45. 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 Capitol building without authority to be there.

46. A search of open sources revealed a video credited to Townhall Media, a political news organization, depicting various events that occurred at the Capitol on January 6, 2021.<sup>2</sup> At approximately twelve minutes and fifty-two seconds into the video, an individual (PERSON 1) is visible in the United States Capitol Rotunda (the Rotunda), wearing a dark-colored jacket with the markings “USA” in white printed letters on the back. PERSON 1 can be seen in the bottom-center of the screenshot of the video below with a red oval around him:



47. Beginning at approximately thirteen minutes and six seconds, law enforcement officers attempt to remove individuals from the Rotunda and continue to do so for the next several minutes of the video. At approximately fourteen minutes and thirty-eight seconds, PERSON 1 is still in the Rotunda, and the back of his jacket is again visible. PERSON 1 stands taller than a number of individuals around him and can clearly be seen as law enforcement officers repeatedly attempt to remove him and others from the Rotunda.
48. At fourteen minutes and forty-one seconds, law enforcement officers appear to push PERSON 1 from behind. PERSON 1 can be seen standing in the Rotunda still wearing the dark-colored USA jacket, which also appears to bear a Nike logo on the front right side and a red and white Olympic patch on the front left side, as depicted in the below screenshot:

---

<sup>2</sup> This video is publicly accessible on the Internet at the following URL: [https://www.youtube.com/watch?v=YzxvVi8wkrU&feature=emb\\_title](https://www.youtube.com/watch?v=YzxvVi8wkrU&feature=emb_title). The video is also available with dialogue from the individual who recorded the video at the following URL: <https://townhall.com/tipsheet/juliorosas/2021/01/11/watch-townhalls-frontline-video-of-capitol-building-riot-n2582910>.



49. Below is a photograph of what appears to be the red and white Olympic patch on the front left side of PERSON 1's jacket:



50. Continuing through the video, at fourteen minutes and fifty-three seconds, law enforcement officers continue to try and remove PERSON 1, among other individuals, from the Rotunda. PERSON 1's bearded face is clearly visible on the left side of the video in the below screenshot depicted in the red oval:



51. Additional open-source research revealed that media outlets such as SwimSwam, a news organization that covers competitive swimming and other related sports, identified this individual as possibly KLETE DERIK KELLER. Your affiant has confirmed this identification.
52. First, a search of Colorado's Department of Motor Vehicles returned KLETE DERIK KELLER's August 2019 driver's license photograph. By comparing this photograph to the image of PERSON 1, your affiant reasonably believes that PERSON 1 is identical to KLETE DERIK KELLER. The photograph affiliated with KLETE DERIK KELLER's driver's license is below:



53. Second, Colorado state records and publicly available information list KELLER's height at 6 feet, 6 inches tall, and PERSON 1 appears to be one of the tallest individuals in the video depicting individuals in the Rotunda.

54. Third, open-source research revealed that KELLER is a three-time Olympic athlete and Olympic Gold Medalist, and PERSON 1 appears to be wearing a United States Olympic Team jacket in the video showing him in the Rotunda.
55. Your affiant observed KELLER's registered vehicle at the Subject Premises on January 11, 2021, and interior lights were observed on inside the Subject Premises. Publicly available commercial databases and government records state that KELLER's residence is the Subject Premises. Therefore, it is likely KELLER would store his clothing there, and normally would have his cellular phone on his person or in his residence. KELLER has been aware of a potential investigation into these violations since at least January 11, 2021, when media outlets contacted KELLER's employer to inquire about the video of KELLER in the U.S. Capitol on January 6, 2021, and it is possible KELLER has disposed of or moved the clothing he was wearing or his cellular phone. Agents have been informed by at least one person that KELLER may have left his cell phone and jacket in D.C., but your affiant has not been able to confirm that.
56. Open source information and publicly available search engines show KELLER had social media accounts, to include Instagram, Facebook, and Twitter, prior to the commission of the subject offenses. Your affiant is aware such accounts included an Instagram account with the handle "[REDACTED]" and a Facebook account with user ID "[REDACTED]". KELLER has since deleted his Instagram and Facebook accounts. Law enforcement officers identified that the accounts had been deleted on or prior to approximately January 11, 2021. As observed in the August 2018 video, KELLER had several applications installed on his cellular phone, including Facebook.<sup>3</sup> The New York Times spoke with coaches and former teammates of KELLER for an article dated January 12, 2021. The New York Times reported that, "Few of the people who recognized Mr. Keller in the video expressed surprise at his presence in Washington. His deleted social media accounts, several of them said, had in recent years included a stream of pro-Trump messaging."<sup>4</sup> Participants of the storming of the U.S. Capitol on January 6, 2021, utilized social media platforms, including Facebook and Twitter to recruit, organize, and encourage people to travel to Washington D.C. for January 6, 2021, to prevent Congress from certifying the results of the 2020 Presidential Election. Therefore, KELLER's social media accounts should show that KELLER accessed information and messages related to the January 6, 2021, demonstration in Washington DC; how KELLER conducted his planning and preparation to attend and participate in the demonstration; and, perhaps, what his intentions were regarding the alleged offenses.
57. KELLER's travel to Washington D.C. for the events of January 6, 2021, would have been arranged using either airfare or traveling a distance of approximately 1,600 miles via ground transportation. Purchasing airfare would require the use of either a computer or a cellular phone to find and pay for the ticket. Additionally, many travelers use electronic

---

<sup>3</sup> <https://www.fox21news.com/news/local/dog-sitting-gone-wild-owner-comes-home-to-find-shirtless-men-lube-in-living-room/>.

<sup>4</sup> <https://www.nytimes.com/2021/01/12/us/olympic-gold-medalist-swimmer-raided-the-capitol-in-his-usa-jacket.html>,

boarding passes instead of paper boarding passes and/or access their itinerary on their cell phone. Alternatively, ground transportation would have required logistical planning necessitating the use of a computer and/or cellular phone. Such logistical planning would included, among other things: driving directions, making hotel reservations, and finding places to eat or get gas.

### **CONCLUSION**

58. I submit that this affidavit supports probable cause for a warrant to search the Subject Premises described in Attachment A, and seize the items described in Attachment B.

I declare under penalty of perjury that the foregoing is true and correct to the best of my information, knowledge, and belief.

s/Brandon Kimble

Brandon Kimble, Special Agent  
Federal Bureau of Investigation

SUBSCRIBED and SWORN to by reliable electronic means me this 14th day of January 2021.

---

HON. MICHAEL E. HEGARTY  
UNITED STATES MAGISTRATE JUDGE  
DISTRICT OF COLORADO


Application for search warrant was reviewed and is submitted by Peter McNeilly, Assistant United States Attorney.



## UNITED STATES DISTRICT COURT

for the  
District of Colorado

In the Matter of the Search of:

 more fully  
 described in Attachment A, attached hereto, to include  
 all out-buildings and vehicles located thereon and to  
 include the person of KLETE DERIK KELLER, if he  
 is present at the time of the search warrant execution.

)  
) Case No.  
)  
)  
)  
)  
)  
)

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

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

SEE "ATTACHMENT A" attached hereto and incorporated by reference

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

SEE "ATTACHMENT B" attached hereto and incorporated by reference

I find that the affidavit(s), or any recorded testimony, establishes probable cause to search and seize the person or property.

**YOU ARE COMMANDED** to execute this warrant on or before January 28, 2021 (not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10 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 Michael E. Hegarty  
(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: \_\_\_\_\_

\_\_\_\_\_  
Judge's signatureCity and state: Denver, CO

Hon. Michael E. Hegarty, U.S. Magistrate Judge  
Printed name and title

<b>Return</b>		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:		
<b>Certification</b>		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <div style="display: flex; justify-content: space-between; align-items: flex-end;"> <div style="width: 30%;"> <p>Date: _____</p> </div> <div style="width: 65%;"> <div style="text-align: center; margin-bottom: 10px;"> <p>_____</p> <p><i>Executing officer's signature</i></p> </div> <div style="text-align: center;"> <p>_____</p> <p><i>Printed name and title</i></p> </div> </div> </div>		



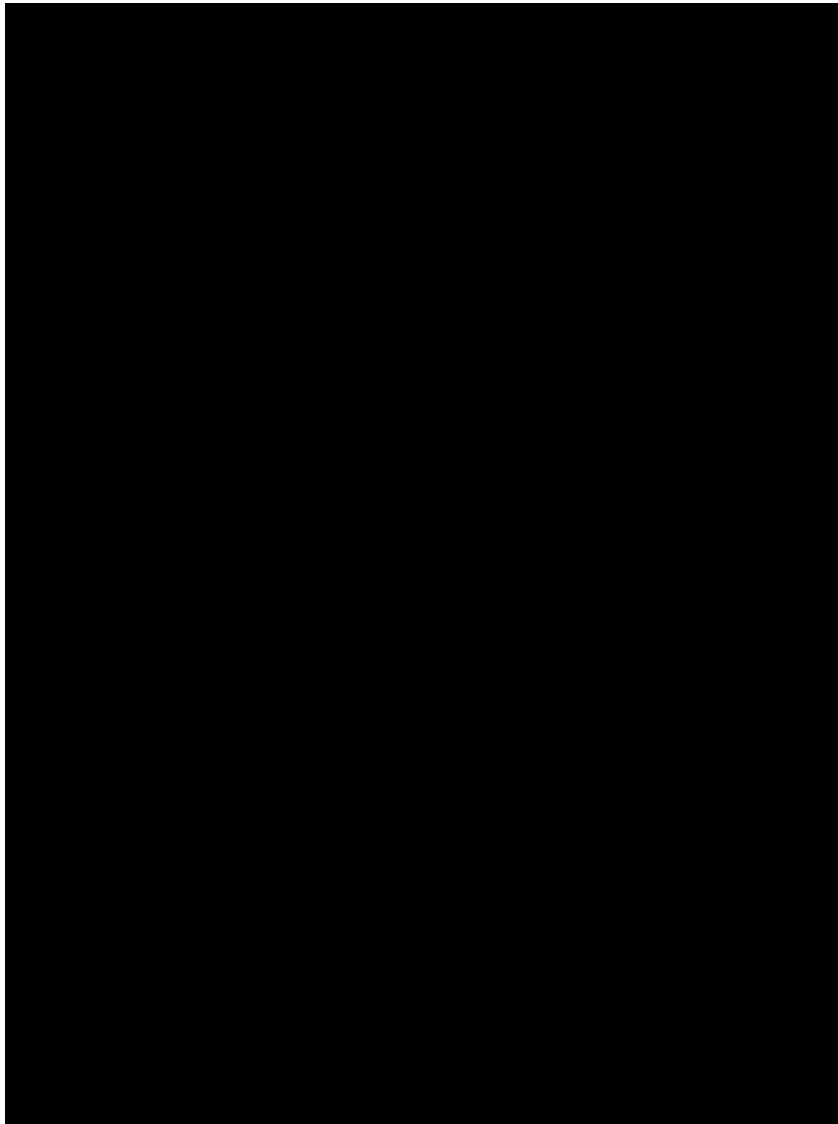
**ATTACHMENT A**

**DESCRIPTION OF LOCATION TO BE SEARCHED**

The Subject Premises is located at [REDACTED]

[REDACTED]. The location consists of the subject residence, surrounding property, and all outbuildings located thereon. The place to be searched includes the person of KLETE DERIK KELLER, if he is present on the subject premises at the time of the search warrant execution.

Photographs of the front and side of the Subject Premises are below:



## **ATTACHMENT B**

### **DESCRIPTION OF ITEMS TO BE SEIZED AND SEARCHED**

The following items, located at the Subject Premises that constitute evidence of the commission of, contraband, the fruits of crime, or instrumentalities of violations of 18 U.S.C. § 231(a)(3); 18 U.S.C. 1752(a)(1),(2); and 40 U.S.C. § 5104(e)(2) (the “Subject Offenses”), including the following:

1. Records and information relating to KLETE DERIK KELLER’s travel to the Washington D.C. area, on or around January 6, 2021;
2. Distinctive articles of clothing which would identify KLETE DERIK KELLER as the person in the videos of the Rotunda on January 6, 2021, including the USA Olympic jacket, the bandana or face covering, and the backpack which he appears to be wearing in the photos included with the affidavit in support of this search warrant;
3. Records and information which tend to establish ownership or use of digital devices and ownership or use of any Internet service accounts accessed to commit the Subject Offenses, to include credit card bills, telephone bills, correspondence and other identification documents;
4. Records and items that show dominion and control of the property searched, to include utility bills, telephone bills, correspondence, rental agreements and other identification documents.
5. Computers, which include all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices capable of performing logical, arithmetic, or storage functions, any physical object upon which computer data can be recorded, including desktop and laptop computers, computer hardware, computer software, volatile data, cellular telephones, tablets, server computers, gaming devices, network hardware, hard disk drives, RAM, floppy disks, flash memory, CDs, DVDs, and other magnetic or optical storage media, as well as, computer related documentation, computer passwords and data security devices, digital communications devices, cameras, videotapes, video recording devices, video recording players, and video display monitors, digital input and output devices such as keyboards, mouse(s), scanners, printers, monitors, electronic media and network equipment, modems, routers, connection and power cords, and external or connected devices used for accessing computer storage media that was used to commit or facilitate commissions of the Subject Offenses (collectively hereinafter, “COMPUTER”).

For any COMPUTER or storage medium whose seizure is otherwise authorized by this warrant, and any COMPUTER or storage medium that contains or in which is stored records or information that is otherwise called for by the warrant:

- a. Evidence of who used, owned, or controlled the COMPUTER at the time the items described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, calendars, browsing history, user profiles, e-mail, e-mail contacts, "chat" or instant messaging logs, photographs, and correspondence;
- b. Evidence of software that may allow others to control the COMPUTER, 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 lack of such malicious software;
- d. Evidence indicating how and when the COMPUTER was accessed or used to determine the chronological context of COMPUTER access, use, and events relating to the Subject Offense(s) and to the computer user;
- e. Evidence indicating the computer user's state of mind as it relates to the Subject Offense(s);
- f. Evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. Evidence of the times the COMPUTER was used;
- i. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. Documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. Records of or information about the COMPUTER'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;
- l. Contextual information necessary to understand the evidence described in this attachment;
- m. Information about usernames or any online accounts or email addresses, including Instagram handle "[REDACTED]," Facebook account "[REDACTED]," and Twitter;
- n. Volatile data necessary to preserve evidence prior to powering-off and unplugging a running computer;

- o. Information, notes, software, documents, records, or correspondence, in any format and medium, pertaining to the Subject Offense(s);
- p. Items otherwise described above in paragraphs of this Attachment B.

If KLETE DERIK KELLER is present at the time of the search warrant execution, executing law enforcement personnel are authorized to depress the fingerprints and/or thumbprints of KLETE DERIK KELLER onto the Touch ID or fingerprint sensor of any Apple iPhone, iPad, or other Apple brand device, or other device that has a fingerprint sensor, in order to gain access to the contents of any such device. Law enforcement personnel may also hold the device(s) found at the Subject Premises in front of the face of KLETE DERIK KELLER to activate the facial recognition feature; and/or (3) hold the device(s) found at the Subject Premises in front of the face of KLETE DERIK KELLER to activate the iris recognition feature, for the purpose of unlocking the device(s) in order to search the contents as authorized by this warrant.

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.

#### DEFINITIONS:

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, 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, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).