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

IN THE MATTER OF THE SEARCHES OF: THE RESIDENCE LOCATED AT: [redacted] [redacted] MOTORCYCLE WITH PENNSYLVANIA PLATE [redacted] AND VEHICLE IDENTIFICATION NUMBER [redacted]	Magistrate No. 23-747 **[UNDER SEAL]** Magistrate No. 23-748 **[UNDER SEAL]**

AFFIDAVIT BY TELEPHONIC OR OTHER RELIABLE ELECTRONIC MEANS IN SUPPORT OF AN APPLICATION FOR SEARCH WARRANT

I, Grant Lee Polson, a Special Agent of the Federal Bureau of Investigation ("FBI"), being duly sworn, 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 residence located at [redacted] (hereinafter, the **"TARGET RESIDENCE"**), further described in Attachment A1, for the items described in Attachment B1, both of which are appended to this affidavit and incorporated herein by reference.

2. Also, 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 [redacted] motorcycle with Pennsylvania license plate [redacted] and Vehicle Identification Number [redacted] (hereinafter, the **"THE MOTORCYCLE"**), further described in Attachment A2, for the items described in Attachment B2, both of which are appended to this affidavit and incorporated herein by reference.

AGENT BACKGROUND

3. I am a Special Agent of the FBI and have been so employed since February 2022. I was previously employed by the Federal Air Marshal Service as a Federal Air Marshal starting in 2016. As a Special Agent with the FBI, 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 Title 18, United States Code, Section 2516.

4. I am currently assigned to the Joint Terrorism Task Force ("JTTF") in the FBI's Pittsburgh Division. In this capacity, I am charged with investigating possible violations of federal criminal law. By virtue of my FBI employment, I perform and have performed a variety of investigative tasks, including functioning as a case agent on domestic terrorism investigations. I have received training and have gained experience in the conduct of counterterrorism investigations, the execution of federal search warrants and seizures, interviewing and interrogation techniques, and the identification and collection of evidence, including mobile device computer-related evidence.

5. The purpose of this Application is to search for and seize evidence, fruits, and instrumentalities, more particularly described in Attachment B, of violations of Title 18, United States Code, Section 231(a)(3) (civil disorder) (hereinafter, the **"TARGET OFFENSE"**).

6. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, law enforcement officers, and witnesses. Since this Affidavit is being submitted for the limited purpose of securing this search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that subjects

[redacted] (hereinafter, **"B.D."**) and [redacted] (hereinafter **"K.D."**) committed violations of the **TARGET OFFENSE** and that evidence, fruits, and instrumentalities of these violations will be found in the **TARGET RESIDENCE** and **THE MOTORCYCLE.**

ACCESS TO LOCKED MOBILE DEVICES LOCATED AT THE TARGET RESIDENCE

7. This application seeks permission to search for records that might be found at the **TARGET RESIDENCE**, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

8. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being

used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

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

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a

file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs

may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating

criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

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

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

10. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the

warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises.

However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

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

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

a. 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 and facial 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.

b. 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.

c. 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, Apple offers a facial recognition feature called "Face ID." During the Face ID registration process, the user holds the device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

d. 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.

e. As discussed in this affidavit, based on my training and experience I 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 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.

f. 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 4 hours *and* the passcode or password has not been entered in the last 156 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.

g. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying

information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found at the Subject Premises and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features in the same manner as discussed above.

h. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the **TARGET RESIDENCE** and reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device; (2) hold the device in front of the face of those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

PROBABLE CAUSE

13. The FBI Pittsburgh JTTF has been investigating **B.D.** and **K.D.** for violations of the **TARGET OFFENSE**. As set forth in detail below, the **TARGET RESIDENCE** is the residence of **B.D.** and **K.D.**, who are husband and wife. The investigation revealed that **B.D.** and **K.D.** share the **TARGET RESIDENCE.**

14. On Tuesday, April 18, 2023, The University of Pittsburgh hosted guest speaker Michael Knowles to speak on "Womanhood and Transgenderism" at the O'Hara Student Center located at 4024 O'Hara Street, Pittsburgh, Pennsylvania 15213. The event was scheduled to begin at 7:30 p.m. At approximately 6:30 p.m. on that date, a group of approximately 300-350 protesters began to gather in the vicinity of the O'Hara Student Center. At approximately 7:01 p.m., one (1) cardboard effigy displaying a depiction of Michael Knowles' face was burned on O'Hara Street

using a red road flare (See Figure 1). At approximately that same time, a smoke bomb type of device, contained in a glass jar, was ignited and placed on the ground among the persons who were lined up to attend the Knowles event. Approximately 12 minutes later, a second similar device was ignited and placed in and among the lined up attendees and the University of Pittsburgh Police (hereinafter "UPP") officers who were there to maintain order for the event. The smoke bomb devices caused the lined-up attendees to scatter in different directions, and the police officers to rush to secure the barricades protecting attendees entering the event. (See Figures 2 and 3.)

15. At approximately 7:28 p.m., protesters began walking South on University Place to the rear of the O'Hara Student Center, away from the police officers, and some attempted to gain access to the alleyway to the rear of O'Hara Student Center. This side of the building had windows to the second floor room where Knowles' presentation was about to begin. Upon seeing the protesters' movement to the rear of the building, the UPP officers moved quickly to that area to create a law enforcement personnel barrier separating the protesters from the building.

16. At approximately 7:31 p.m., a protester tossed an ignited firework into the group of approximately twelve (12) UPP officers in the rear of the building. The firework exploded, causing injuries to several officers, three of which received on-scene evaluation by paramedics from Pittsburgh Bureau of Emergency Medical Services, and one who sought additional care at Forbes Hospital. Officers reported being burned, bruised, suffering from hearing loss, and possible concussions as a result of the explosion. (See Figure 4)

Figure 1

Figure 2

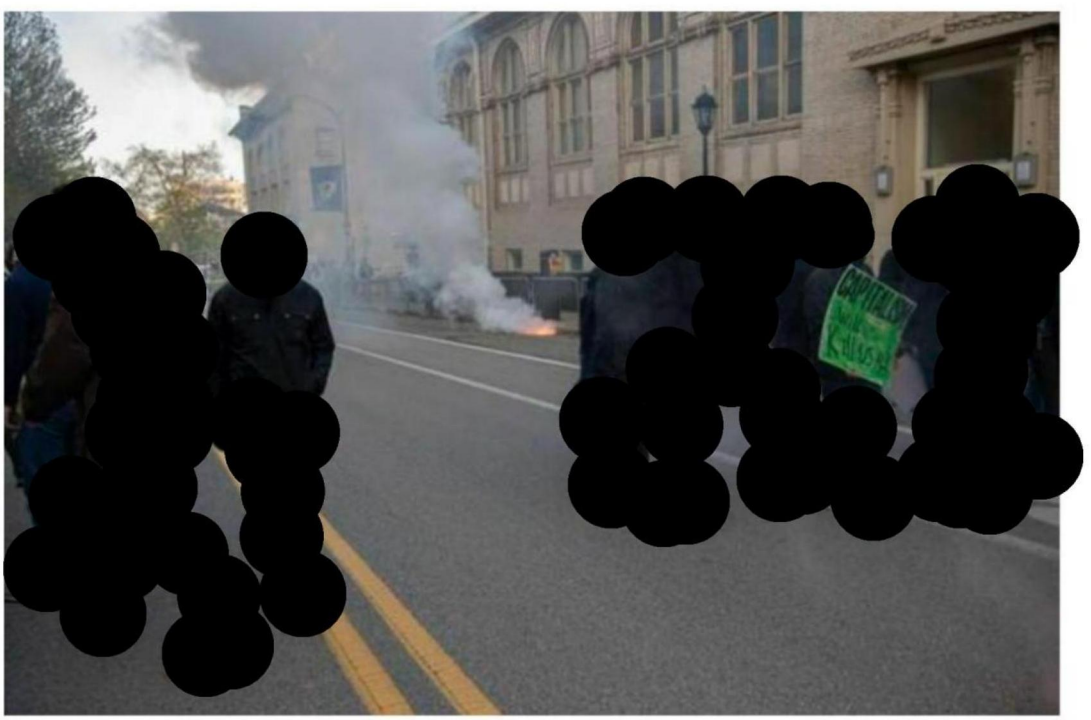


Figure 3

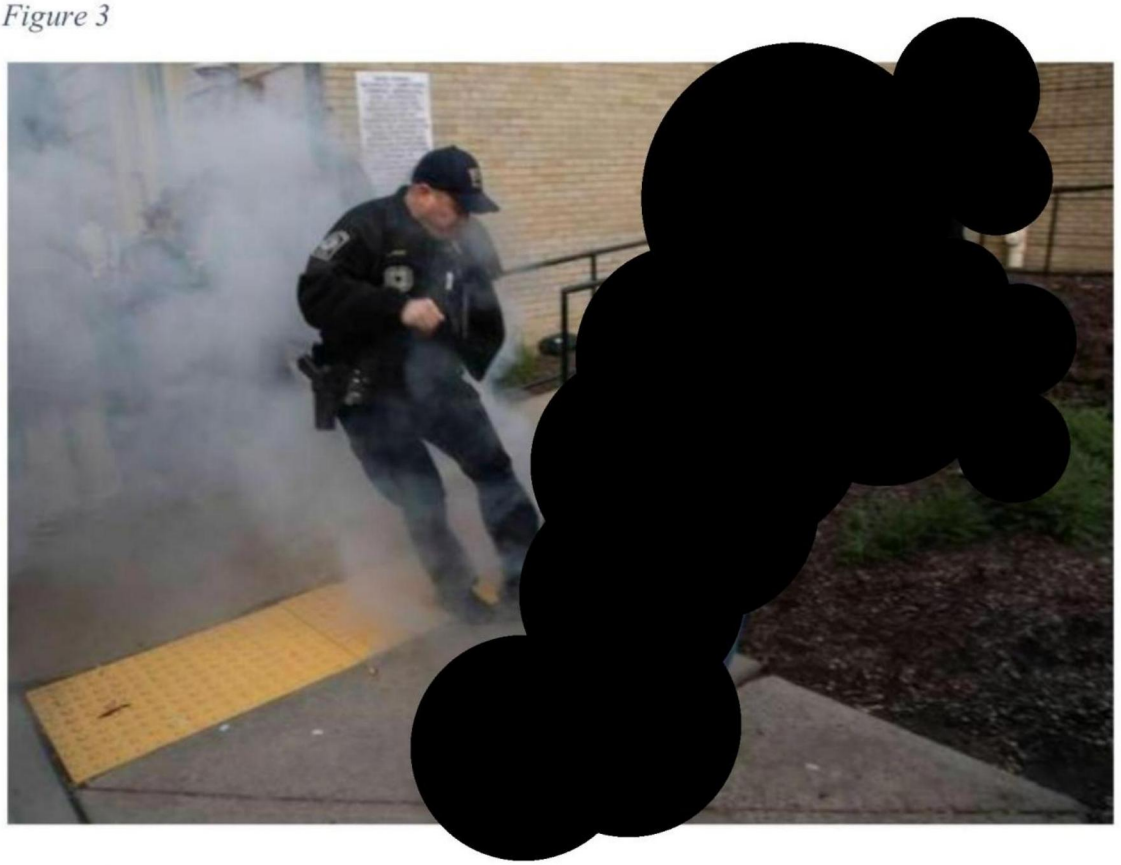


Figure 4

17. As a result of the above-described conduct of some of the protesters, UPP had to implement several security measures. At approximately 7:00 p.m., protesters had gathered near the front entrance of O'Hara Student Center, effectively preventing vehicles from traveling along O'Hara street. O'Hara Street serves as the main access road to UPMC Presbyterian Hospital. UPP issued an emergency alert via the University's Emergency Notification System (ENS), notifying students of a public safety emergency on O'Hara Street. As a result, buildings in the area were placed on a "soft lockdown" A soft lockdown secures all doors to card access only, and restricts access to only Police, facilities management, information technology, and integrated security department. Buildings and places in this soft lockdown include: Graduate School of Public Health, Thackeray Hall, Allen Hall, Gardner Steel Conference Center, Thaw Hall, Space Research Coordination Center, University Club, Benedum Hall, Nordenberg Hall and William Pitt Union. At approximately 10:22 p.m., UPP issued an alert via ENS that the prior public safety emergency was resolved and O'Hara Street was again accessible to traffic.

18. Investigators, including your Affiant, reviewed security video footage after these events. The videos show that, at approximately 4:30 p.m., individuals began gathering on Soldiers and Sailors Lawn, which is part of the Soldiers and Sailors property adjacent to the O'Hara Student Center. Most of these individuals were similarly dressed, many wearing all dark clothing with face coverings. As time passed, the group gathering at Soldiers and Sailors lawn grew larger. Shortly before 7:00 p.m., the group had amassed approximately 300-350 people and began to move North on University Place toward the O'Hara Student Center, where the Michael Knowles event was being held. By this time, UPPD had already placed bike racks in front of the O'Hara Student Center so that an orderly line for attendees could be created as well as a barricade between the attendees and the protesters. As attendees began to enter the event venue, the crowd of protesters

gathered around the entrance to the Student Center on O'Hara Street, mostly on the other side of the bike rack barrier.

19. At approximately 7:01 p.m., a cardboard effigy displaying a picture of Michael Knowles on its face was set on fire using a burning red flare on O'Hara Street, near the corner of Thackery Avenue (See Figure 1). Pittsburgh Bureau of Fire was able to contain and extinguish the fire shortly thereafter, as they were already on scene. Pittsburgh Bureau of Fire was in the process of responding to an earlier fire alarm being pulled at Benedum Hall when the fire on O'Hara Street began. Law enforcement later recovered an empty package of Orion emergency road flares (3-pack) from the scene. At approximately this same time, the first "smoke bomb," referenced above, was ignited and was rolled under the police barricades in front of the Gardner Steel Building located on O'Hara Street (See Figure 2). Video footage and photographs shows a male dressed in green shoes, black pants, blue "Carhartt" jacket, black face mask, glasses and carrying a black satchel bag (male later identified as **B.D.**) as the individual responsible for rolling the device with his right hand. At approximately 7:13 p.m., the second device emitting smoke and fire was thrown over a police barricade, towards UPP officers and ticketholders as they were lined up and entering the O'Hara Student Center (Figure 3). Video footage and photographs show **B.D.** throwing this second device as well. As the second smoke bomb was still burning and emitting smoke, **B.D.** can be seen grabbing and shaking police barricades, appearing to attempt to defeat the barricades and rush the entrance of O'Hara Student Center. UPP officers gave verbal commands telling protesters to get back, as protesters began rushing the entrance to the O'Hara Student Center. Protesters then moved around the corner of the O'Hara Student Center toward the rear entrance of O'Hara Student Center. At Approximately 7:31 p.m., the explosive firework was thrown and detonated into a group of twelve (12) UPP officers who had rushed to that area in response to the movements of the

protesters. Video footage and photographs show **B.D.** igniting the device while hiding behind a female dressed in white face mask and glasses and wearing black shoes, black pants, a white "puffy" jacket, and red scarf (female later identified as **K.D.**). After the explosion, the protesters in this rear area of the O'Hara Student Center were seen running away from the explosion. At approximately 7:34 p.m., a University of Pittsburgh Emergency Notification Service (ENS) Alert was issued to the community stating, "There is a public safety emergency at O'Hara Street. Stay away from the area."

20. Knowles' event nevertheless took place and ended at approximately 9:00 p.m. Pittsburgh Bureau of Police (PBP) issued three dispersal warnings over a loudspeaker at approximately 9:42 p.m. The crowd lingered for a couple of minutes and eventually dispersed without incident. At approximately 10:21 p.m. a final ENS Alert was issued stating, "The prior emergency on O'Hara Street was resolved. All clear. Buildings returning to normal operations."

21. Intercollegiate Studies Institute (ISI) is a non-profit 501(c)(3) educational organization funded by thousands of individuals and dozens of charitable foundations in Pennsylvania and around the country. ISI is headquartered in Wilmington, Delaware. Their mission is to provide access to speakers and presenters for college students around the country. They focus on the freedom of speech and the right to peacefully assemble. ISI was responsible for organizing and paying for the speaking event on April 18, 2023, at the University of Pittsburgh featuring Michael Knowles and Brad Polumbo. ISI paid approximately $10,000 each to Michael Knowles and Brad Polumbo to have them speak at the event, and approximately $2,500 to the moderator, Leah Libresco Sargeant. There were two components scheduled to take place on April 18, 2023. These included a 90-minute organized debate and a 60-minutes Very Important Persons (VIP) meet and greet with ISI staff, students, and Michael Knowles. Due to safety concerns arising

from the activity outside of the O'Hara Student Center on the night of April 18, 2023, UPP made the decision to end the event at approximately 9:00 p.m., thereby cancelling the promised "Meet and Greet" that was supposed to occur afterward. Consequently, ISI paid the speakers and moderator a total of $22,500 plus travel and lodging expenses for a service that was not fulfilled to the extent of the terms agreed upon. In addition, ISI incurred security costs totaling approximately $27,796.04 for the following services: $16,925.16 to the University of Pittsburgh for 28 UPP officers and 11 UPP supervisors for six (6) hours; $3,006.25 to a private security company called RIP Security; and $7,864.63 to Michael Knowle's private security, to include travels and lodging expenses. Despite the total security costs, protection was not adequate enough to maintain a safe enough environment in order to conduct the event as planned.

IDENTIFICATION OF B.D.

22. On April 3, 2023, the UPPD received a tip via the Wufoo application indicating a group of anarchist extremists planned to engage in acts of violence in an effort to disrupt a planned debate regarding transgender issues which was scheduled for April 18, 2023, at the University of Pittsburgh O'Hara Student Center. Complainant advised that this group of anarchist extremists meet Thursday evenings at the [redacted] Bookstore at [redacted]. During one of these meetings, an individual referred to as "[redacted]" stated the speaker event "was not going to happen" and subsequently passed out "zines," or small printed booklets, to meeting participants which provided instruction on how to make incendiary devices for arson and Molotov cocktails.

23. Based upon the possible planning and preparation for the commission of acts of violence targeting the April 18, 2023 speaker event, the FBI Pittsburgh JTTF conducted surveillance of the [redacted] Bookstore on April 13, 2023. At approximately 9:02 p.m. on April 13,

2023, surveillance observed an individual arrive at the [redacted] Bookstore on a black and red [redacted] motorcycle. The individual departed the Bookstore on the same motorcycle at approximately 10:32 p.m. Through subsequent review of photographs, FBI Task Force Officer (TFO) David Derbish was able to identify **B.D.** as the likely operator of the motorcycle observed on April 13, 2023.

24. Review of video footage from April 18, 2023, identified a male believed to be **B.D.** donning a black face mask and glasses, and wearing green shoes, black pants, a black satchel bag, and a blue Carhartt jacket, accompanied by a female, believed to be **K.D.**, donning a white face mask and glasses and wearing black shoes, black pants, a white "puffy" jacket, and red scarf. The couple was observed on video on the outer edge of protesters gathered at the intersection of University Place and O'Hara Street at approximately 6:43 p.m. As the protest moved to the front of the O'Hara Student Center, the male was observed on video, at approximately 7:01 p.m., igniting the first of two "smoke bombs" and rolling it under police barricades. At approximately 7:13 p.m., the male can be seen on video igniting the second "smoke bomb" and ducking under a "Jews Say Never Again" banner. The unidentified banner holders appeared to lift the banner as the smoke device was released toward officers and the speaking event attendees. The couple, believed to be **B.D.** and **K.D.**, then went over to the metal barrier, at which time the male tried to knock it over, by grabbing it and shaking it.

25. The couple proceeded with other protesters to the rear exit of the O'Hara Student Center. At approximately 7:29 p.m., video showed the male bend over behind the female and ignite an explosive device, with the female appearing to step in front of him, shielding his activity from others. The male then threw the device over a small crowd and into approximately twelve (12) officers. The device struck one officer, fell to the ground and then exploded into flames and debris.

The flames and debris can be viewed on camera launching approximately three to four stories into the air and outwards into a crowd of people. As a result of the explosion, multiple police officers sustained injuries, to include burns, bruises, hearing loss, and possible concussions.

26. Subsequent review of video gathered by UPP in the days following the event confirmed that the above described couple, believed to be **B.D.** and **K.D.**, arrived in the Oakland area for the event at approximately 5:43 p.m. on April 18, 2023, on a [redacted] motorcycle, and eventually departed the area on the same motorcycle shortly after 8:00 p.m. Video further captured Pittsburgh Regional Transport (PRT) Bus #6449 traveling behind the motorcycle, at Fifth Avenue and Lytton Avenue. Video subsequently provided by PRT identified the motorcycle's PA license plate as [redacted]. Law enforcement database checks confirmed PA license plate [redacted] is registered to a [redacted] motorcycle owned by **B.D.**, the **THE MOTORCYCLE**. Checks further identified a [redacted] bearing PA license tag [redacted] is also registered to **B.D.** and **K.D.** The physical appearances of **B.D.** and **K.D.** are consistent with the physical appearances of the male and female who arrived and drove away from the vicinity of the incident on **THE MOTORCYCLE**. The residence of **B.D.** and **K.D.**, as described more fully below, displays a red and black diagonally divided flag hanging from the second story balcony of the residence. This flag is known to investigators as being associated with anarchists.

27. Law enforcement and fee-for-service databases further identified [redacted], the **TARGET RESIDENCE**, as an address associated with both **B.D.** and **K.D.** Law enforcement database checks revealed a firearms carry permit ([redacted]) issued to **B.D.**, [redacted] on November 23, 2021 with an expiration date of November 23, 2026, and sale/transfer records associated with two firearms (NFI).

28. Pursuant to a subpoena issued to Phantom Fireworks Phantom Showrooms, LLC, the FBI obtained records showing that, on April 15, 2023, **B.D.** purchased two packages of Phantom Assorted Candles (6 piece), item number C-007, and a Crackling Phantom Cannon Ball Mortar Kit (6 piece), item number G-255A, from the Phantom Fireworks store located at 4680 Old William Penn Hwy, Monroeville, PA 15146. The Phantom Fireworks store requires purchasers to show valid identification documents when purchasing these items. The purchase records show that **B.D.** produced his driver's license, showing his date of birth and his address of [redacted], the **TARGET RESIDENCE**.

29. FBI surveillance conducted on April 26 and 27, 2023, observed **B.D.** and **K.D.** entering and exiting the **TARGET RESIDENCE**, driving in the black [redacted] with license plate PA/[redacted], and also driving **THE MOTORCYCLE** with license plate PA/[redacted]. FBI surveillance observed **B.D.** park the motorcycle in a driveway behind [redacted] and cover it with a black motorcycle cover.

30. Your affiant has viewed videos of the ignition and detonation of crackling phantom cannon ball fireworks. The detonation of these devices appears to be consistent with what witnesses heard and observed on April 18, 2023, when the firework was tossed into the group of UPP officers.

31. On or about May 6, 2023, Investigators including you Affiant were notified of **B.D.**'s domestic flight travel itinerary. **B.D.** was scheduled to travel aboard Spirit Airlines flight #[redacted], which departs Oakland, CA (OAK) and arrives into Newark, NJ (EWR), and continuing on aboard Spirit Airlines flight #[redacted], departing EWR and arriving in PIT. During airport security screening at the Transportation Security Administration (TSA) checkpoint, **B.D.** alarmed the Explosive Trace Detection (ETD) machine after a swab sample was taken from his belongings.

The alarm was cleared by Transportation Security Specialists for Explosives (TSS-E) and **B.D.** was allowed to travel, however, **B.D.** did not take the flight. On or about May 9, 2023, Investigators including your Affiant were provided the ETD alarm report. The ETD report stated that **B.D.** alarmed for a compound called "RDX," which is known to Investigators as a high explosive.

32. On or about May 10, 2023, investigators including your Affiant were notified of another domestic flight travel itinerary scheduled for [redacted] **B.D**. He was to travel aboard Southwest Airlines flight #[redacted], departing OAK and arriving Denver, Colorado (DEN), and continuing on aboard Southwest Airlines flight #[redacted], departing DEN and arriving PIT. During airport security screening at the TSA checkpoint, **B.D.** once again alarmed the ETD machine after a swab sample was taken from his belongings. Your Affiant was verbally informed that **B.D.** again alarmed the ETD machine for RDX after a swab sample was taken from the interior seams on his bag. The alarm was cleared by TSS-E and **B.D.** was allowed to travel.

33. On or about May 12, 2023, investigators, including your Affiant, participated in a warrantless search of the trash outside of the **TARGET RESIDENCE** set on a public sidewalk. Investigators recovered various items of indicia belonging to **B.D.** and **K.D.** addressed to [redacted] including, but not limited to: Chase bank statements, Verizon wireless bills, Department of Motor Vehicle correspondence, dental statements, Amazon packaging slips, and Starbucks order printouts. Investigators also recovered a printed copy of an article published to www.crimethinc.com titled "THE CITY IN THE FOREST: Reinventing Resistance for an Age of Climate Crisis and Police Militarization." According to the publication, CrimethInc. describes itself as "a rebel alliance – a decentralized network pledged to anonymous collective action – a breakout from the prisons of our age." Review of the article revealed that "THE CITY IN THE

FOREST" is in reference to the city Atlanta, Georgia, and the "Defend the Atlanta Forest." As a matter of background, the "Defend the Atlanta Forest" movement has been active since approximately April 2021 and involves protesters unlawfully occupying a wooded area of land where the city plans to build a police training facility. Lastly, investigators recovered a printed zine that appears to be a typed letter addressed to "[redacted]" from **B.D.** discussing anarchist ideology. Review of the zine revealed the writing is likely a response to a zine previously given to the author from [redacted].

34. On or about May 12, 2023, your Affiant reviewed report of laboratory findings from the County of Allegheny, Office of the Medical Examiner, Division of Forensic Laboratories. The report examined two remains of incendiary devices and the remains of road flare collected by PBP Arson Division on the night of April, 18, 2023. The incendiary devices referenced in this report are the same "smoke bombs" Investigators witnessed **B.D.** ignite and utilize earlier that day. A white solid substance was examined microscopically and/or instrumentally using Fourier Transform Infrared Spectrometry that was consistent with potassium carbonate. Consultation with FBI Special Agent Bomb Technician revealed that potassium carbonate is an oxidizer that will burn when mixed with a fuel source.

CONCLUSION

35. Based upon your Affiant's training and experience, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities, more particularly described in Attachments B1 and B2, of the **TARGET OFFENSE** are presently located in the **TARGET RESIDENCE** and on **THE MOTORCYCLE.**

36. It is further respectfully requested that this Court issue an Order sealing, until further order of Court, all papers submitted in support of this application, including the application,

affidavit, and the search warrant, and the requisite inventory notice. Sealing is necessary because the items and information to be seized are relevant to an ongoing investigation and premature disclosure of the contents of this affidavit and related documents may have a negative impact of this continuing investigation and may jeopardize its effectiveness.

The above information is true and correct to the best of my knowledge, information, and belief.

s/ Grant Lee Polson
GRANT LEE POLSON
Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me,
by telephone pursuant to Fed. R. Crim. P. 4.1(b)(2)(A),
this 18th day of May, 2023.

Cynthia R. Eddy

HONORABLE CYNTHIA R. EDDY
United States Magistrate Judge
Western District of Pennsylvania

ATTACHMENT A1

Location to be Searched

The locations to be searched are as follow:

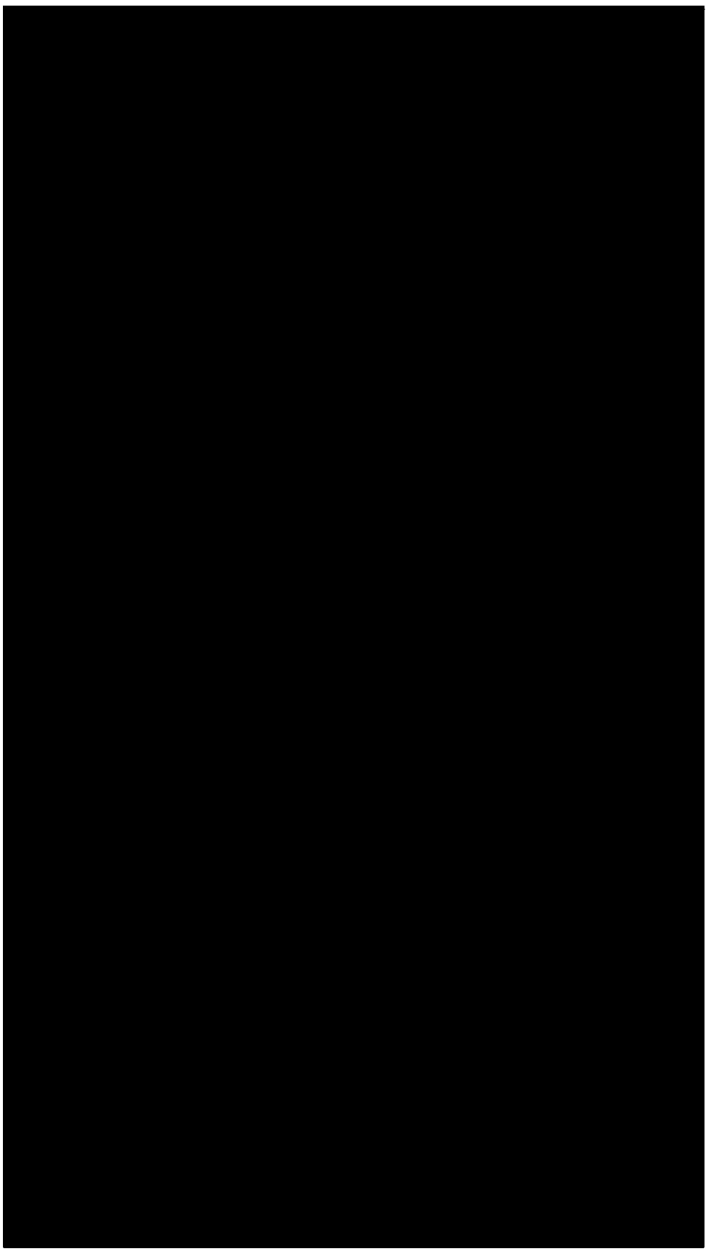
1. **TARGET RESIDENCE -** [redacted].

The residence is a three-story brick building with a double landing staircase leading from the sidewalk to a white front door.

a. As described in this warrant, the **TARGET RESIDENCE** includes all rooms, attics, basements, and other parts therein, the surrounding grounds, and any garages, storage rooms, trash containers, and outbuildings within the curtilage of and directly associated with **TARGET RESIDENCE**.

b. As described in this warrant, the **TARGET RESIDENCE** includes any vehicles parked directly on the property or in the street in front of or nearby or adjacent to the property, provided further that said vehicles can be specifically connected to the occupants or permanent residents of the **TARGET RESIDENCE** prior to any search of said vehicle or vehicles.

c. As described in this warrant, the **TARGET RESIDENCE** includes any residents or long-term guests of the **TARGET RESIDENCE**, who are found at the property, and who might possess items sought in the search warrant. Prior to searching any residents or long-terms guests of the **TARGET RESIDENCE**, law enforcement will attempt to identify the individual and ascertain that person's connection to the **TARGET RESIDENCE**.



ATTACHMENT B1

Items to be Searched for and Seized

1. Evidence, contraband, fruits, or instrumentalities of violations of Title 18 United States Code Section 231(a)(3), including the following:

    a. Information, correspondence, records, documents, zines, indicia, writings, journals, manuals, and other materials or items, in hard copy or electronic form, constituting evidence pertaining to the **TARGET OFFENSE**

    b. Cellular phones, computers, and other devices or storage mediums that contain, or in which can be stored, evidence of **TARGET OFFENSE**

    c. Records or documents evidencing occupancy or ownership of **TARGET RESIDENCE** or **THE MOTORCYCLE**

    d. Black shoes with white stripes and brown soles

    e. Grey motorcycle helmet

    f. Keys to **THE MOTORCYCLE**

    g. Black over the shoulder bag/backpack/satchel bag

    h. Dark green cloth shoes

    i. Dark blue/black jacket zip up jacket with hood appearing to be Carhartt brand

    j. Grey winter hats with square patch appearing to be Carhartt brand

    k. Black leather women's boots

    l. White puffer jacket, knee length, with vertical and horizontal zippers

    m. Grey gloves with black palm/finger grip

    n. Black leggings, women's tight cloth pants

    o. Dark black men's jeans

p. Red/maroon hoodie

q. Black rim glasses

r. Blue surgical mask

s. Black face mask

t. Women's glasses, light color large lens

u. Explosives and their precursors, components, chemicals, and initiation systems.

v. Tools and supplies used or capable of being used for the acquisition, manufacture, testing, modification, or use of explosives, initiation systems and their components;

w. Items used or intended to be used for storing explosives, initiation systems and their components.

x. Training, instructional, and reference materials or other information, whether printed or in digital format, relating to explosives;

y. Records, documents, programs, applications, or materials relating to items listed above;

z. Address and/or telephone books, telephones, pagers, answering machines, customer lists, and any papers reflecting names, addresses, telephone numbers, pager numbers, fax numbers and/or identification numbers of sources of supply of explosives, military munitions or ordnance, or any tools, containers, or supplies relating to such items;

aa. Documents and records, including electronic mail and electronic messages, reflecting the ownership, occupancy, possession, or control of the **TARGET RESIDENCE**, including lease/rental agreements, rent receipts, registration

documents, bank records, utility bills, telephone bills, other addressed envelopes, and correspondence;

bb. Any digital device used to facilitate the above-listed violations and forensic copies thereof.

cc. With respect to any digital device used to facilitate the above-listed violations or containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device 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, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, 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;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device'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.

2. During the execution of the search of the **TARGET RESIDENCE** described in Attachment A1, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed to be law enforcement to be a user of a device found at the premises, to the fingerprint scanner of the device; (2) hold a device found at the premises in front of the face of those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

3. 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 writings, drawings or paintings); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

4. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.
5. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

ATTACHMENT A2

Vehicle to be Searched - THE MOTORCYCLE

The vehicle to be searched is as follows:

1. A [redacted] Motorcycle, Pennsylvania License Plate [redacted], VIN [redacted]

ATTACHMENT B2

Items to be Searched for and Seized

1. Evidence, contraband, fruits, or instrumentalities of violations of Title 18 United States Code Section 231(a)(3), including the following:

    a. Records or documents evidencing occupancy or ownership of **TARGET RESIDENCE** or **THE MOTORCYCLE**

    b. Grey motorcycle helmet with clear visor

    c. Keys to **THE MOTORCYCLE**

    d. Black over the shoulder bag/backpack/satchel bag

    e. Black rim glasses

    f. Blue surgical mask

    g. Black face mask