

UNITED STATES DISTRICT COURT

for the

District of Columbia

IN THE MATTER OF THE SEARCH OF A SAMSUNG GALAXY S10 CELLULAR TELEPHONE WITH IMEI 356021101533525 CURRENTLY LOCATED AT THE FEDERAL BUREAU OF INVESTIGATION WASHINGTON FIELD OFFICE, 601 4TH STREET, N.W., WASHINGTON, DC, 20535

Case No. 21-SW-303

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

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

See Attachment A

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

See Attachment B

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

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

The search is related to a violation of:

Table with 2 columns: Code Section, Offense Description. Rows include 18 U.S.C. § 1752(a)(1) - Knowingly Entering or Remaining in any Restricted Building or Grounds Without Lawful Authority; 40 U.S.C. § 5104(e) (2)(D) - Violent Entry and Disorderly Conduct on Capitol Grounds; 18 U.S.C. § 1752(a)(2) - Knowingly Entering or Remaining in any Restricted Building or Grounds Without Lawful Authority; 18 U.S.C. § 111(a) - Forcibly Assaulting, Resisting, or Impeding Certain Officers or Employees.

The application is based on these facts:

See Affidavit in Support of Application for Search Warrant.

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

Handwritten signature of Emily Eckert

Applicant's signature

Emily Eckert, Special Agent
Printed name and title

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

Date: 9/16/2021

Judge's signature

City and state: Washington, D.C.

Zia M. Faruqui
United States Magistrate Judge

UNITED STATES DISTRICT COURT

for the
District of Columbia

IN THE MATTER OF THE SEARCH OF A SAMSUNG)
GALAXY S10 CELLULAR TELEPHONE WITH IMEI)
356021101533525 CURRENTLY LOCATED AT THE) Case No. 21-SW-303
FEDERAL BUREAU OF INVESTIGATION)
WASHINGTON FIELD OFFICE, 601 4TH STREET,)
N.W., WASHINGTON, DC, 20535)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

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

See Attachment A (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 (incorporated by reference).

YOU ARE COMMANDED to execute this warrant on or before September 29, 2021 *(not to exceed 14 days)*
 in the daytime 6:00 a.m. to 10:00 p.m. at any time in the day or night because good cause has been established.

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

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Zia M. Faruqi _____
(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: 9/16/2021

Judge's signature

City and state: Washington, D.C.

Zia M. Faruqi
United States Magistrate Judge

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

Return

Case No.: 21-SW-303	Date and time warrant executed:	Copy of warrant and inventory left with:
------------------------	---------------------------------	--

Inventory made in the presence of :

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

Certification

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

Date: _____

Executing officer's signature

Printed name and title

ATTACHMENT A

Property to be searched

The property to be searched is a Samsung Galaxy S10 cellular telephone with IMEI 356021101533525, hereinafter the “Device.” The Device is currently located at the Federal Bureau of Investigation Washington Field Office, 601 4th Street, N.W., Washington, DC, 20535.

ATTACHMENT B

Property to be seized

1. The items, information, and data to be seized are fruits, evidence, information relating to, contraband, or instrumentalities, in whatever form and however stored, relating to violations of 18 U.S.C. §§ 111(a)(1) and (b); 18 U.S.C. § 231(a)(3); 18 U.S.C. §§ 1512(c)(2); 18 U.S.C. § 1752(a)(1) and (b)(1)(A); 18 U.S.C. § 1752(a)(2) and (b)(1)(A); 18 U.S.C. § 1752(a)(3); 18 U.S.C. § 1752(a)(4) and (b)(1)(A); 40 U.S.C. § 5104(e)(2)(D); 40 U.S.C. § 5104(e)(2)(E); and 40 U.S.C. § 5104(e)(2)(F), as described in the search warrant affidavit, including, but not limited to:

- a. Evidence concerning planning to unlawfully enter the U.S. Capitol, including any maps or diagrams of the building or its internal offices;
- b. Evidence concerning awareness of the official proceeding that was to take place at Congress on January 6, 2021, i.e., the certification of the Electoral College vote;
- c. Evidence concerning efforts to disrupt the official proceeding that was to take place at Congress on January 6, 2021, i.e., the certification of the Electoral College vote;
- d. Evidence relating to a conspiracy to illegally enter and/or occupy the U.S. Capitol Building on or about January 6, 2021;
- e. Evidence concerning a breach and/or unlawful entry of the United States Capitol, including any property of the U.S. Capitol, and any conspiracy or plan to do so;
- f. Evidence concerning the riot and/or civil disorder at the United States Capitol on January 6, 2021;

- g. Evidence concerning the assault(s) of federal officer(s)/agent(s) and efforts to impede such federal officer(s)/agent(s) in the performance of their duties the United States Capitol on January 6, 2021;
- h. Evidence concerning damage to, or theft of, property at the United States Capitol, including its grounds, on January 6, 2021;
- i. Evidence concerning efforts after the fact to conceal evidence of those offenses, or to flee prosecution for the same;
- j. Evidence concerning materials, devices, or tools that were used to assault law enforcement officers and/or unlawfully enter the U.S. Capitol, including, but not limited to, weapons such as mace, pepper spray, OC spray, or smoke grenades;
- k. Evidence of communication devices, including closed circuit radios or walkie-talkies, that could have been used by co-conspirators to communicate during the unlawful entry into the U.S. Capitol;
- l. Evidence of the state of mind of PETER SCHWARTZ and/or other co-conspirators, *e.g.*, intent, absence of mistake, or evidence indicating preparation or planning, or knowledge and experience, related to the criminal activity under investigation; and
- m. Evidence concerning the identity of persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation; or (ii) communicated with the unlawful actors about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts;

2. Evidence of SCHWARTZ's possible affiliation with groups that participated in attempts to obstruct the Congressional proceeding, i.e., the certification of the Electoral College vote, on January 6, 2021;

3. Evidence—including but not limited to documents, communications, emails, text messages, online postings, photographs, videos, calendars, itineraries, and receipts—of:

- a. SCHWARTZ'S presence at the January 6, 2021 riot, or previous events related to the Presidential Election in November 2020;
- b. SCHWARTZ'S travel to and from Washington, D.C., on or about January 6, 2021;
- c. SCHWARTZ's motive and intent for traveling to Washington, D.C. on or about January 6, 2021;
- d. SCHWARTZ's activities in and around Washington, D.C., specifically the U.S. Capitol, on or about January 6, 2021;

4. Evidence of any weapons used in the commission of the riots at the U.S. Capitol on January 6, 2021, including firearm(s); lachrymatory agents, such as mace; baton(s); club(s); chair(s); and other objects;

5. Evidence of criminal charges and/or court supervision pending against SCHWARTZ in other jurisdictions including the State of Kentucky and the State of New York;

6. For the Device, described in Attachment A:

- a. 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, email, email contacts, chat, instant messaging logs, photographs, and correspondence;

- b. evidence of software, or the lack thereof, that would allow others to control the Device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the attachment to the Device of other storage devices or similar containers for electronic evidence;
- d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Device;
- e. evidence of the times the Device was used;
- f. passwords, encryption keys, and other access devices that may be necessary to access the Device;
- g. documentation and manuals that may be necessary to access the Devices or to conduct a forensic examination of the Device;
- h. records of or information about Internet Protocol addresses used by the Device; and
- i. records of or information about the Devices' 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.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF A
SAMSUNG GALAXY S10 CELLULAR
TELEPHONE WITH IMEI 356021101533525
CURRENTLY LOCATED AT THE FEDERAL
BUREAU OF INVESTIGATION
WASHINGTON FIELD OFFICE, 601 4TH
STREET, N.W., WASHINGTON, DC, 20535

SW No. 21-SW-303

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

I, Emily Eckert, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—a digital device—which is currently in law enforcement possession (the “Device”), as described in Attachment A, and the extraction from that property of electronically stored information as described in Attachment B.

2. I am a Special Agent assigned to the Federal Bureau of Investigation. I have been in this position since March 2016. In my duties as a Special Agent, I am currently tasked with investigating criminal activity in and around the Capitol on January 6, 2021. Currently, I am assigned to the Washington Field Office, where I am also responsible for conducting and assisting in investigations involving child pornography, the sexual exploitation of children, and human trafficking. I have gained experience through training with the FBI and in my everyday work related to conducting these types of investigations. During my career as an FBI agent, I have (a) participated in the execution of search warrants and arrest warrants for various crimes; (b) reviewed and analyzed numerous recorded conversations and other documentation of criminal

activity; (c) debriefed cooperating confidential human sources; (d) monitored wiretapped conversations; and (e) conducted physical surveillance of individuals engaged in various crimes. As a federal agent, I am authorized to investigate violations of laws of the United States, and as a law enforcement officer I am authorized to execute warrants issued under the authority of the United States.

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

4. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that violations of 18 U.S.C. §§ 111(a)(1) and (b); 18 U.S.C. § 231(a)(3); 18 U.S.C. §§ 1512(c)(2); 18 U.S.C. § 1752(a)(1) and (b)(1)(A); 18 U.S.C. § 1752(a)(2) and (b)(1)(A); 18 U.S.C. § 1752(a)(3); 18 U.S.C. § 1752(a)(4) and (b)(1)(A); 40 U.S.C. § 5104(e)(2)(D); 40 U.S.C. § 5104(e)(2)(E); and 40 U.S.C. § 5104(e)(2)(F) have been committed by PETER SCHWARTZ and identified and unidentified individuals (hereinafter “SUBJECTS”). There is also probable cause to search the Device, further described below and in Attachment A, for the things described in Attachment B.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

5. The property to be searched is a Samsung Galaxy S10 cellular telephone with IMEI 356021101533525, hereinafter the “Device.”

6. The Device is currently located at the Federal Bureau of Investigation Washington Field Office, 601 4th Street, N.W., Washington, DC, 20535.

PROBABLE CAUSE

The 2020 United States Presidential Election and the Official Proceeding on January 6, 2021

7. The 2020 United States Presidential Election occurred on November 3, 2020.

8. The United States Electoral College is a group required by the Constitution to form every four years for the sole purpose of electing the president and vice president, with each state appointing its own electors in a number equal to the size of that state's Congressional delegation.

9. On December 14, 2020, the presidential electors of the U.S. Electoral College met in the state capital of each state and in the District of Columbia and formalized the result of the 2020 U.S. Presidential Election: Joseph R. Biden, Jr. and Kamala D. Harris were declared to have won sufficient votes to be elected the next president and vice president of the United States.

10. On January 6, 2021, a Joint Session of the United States House of Representatives and the United States Senate ("the Joint Session") convened in the United States Capitol building ("the Capitol") to certify the vote of the Electoral College of the 2020 U.S. Presidential Election ("the Electoral College vote").

The Attack at the U.S. Capitol on January 6, 2021

11. The Capitol is secured 24 hours a day by United States Capitol Police. The Capitol Police maintain permanent and temporary barriers to restrict access to the Capitol exterior, and only authorized individuals with appropriate identification are allowed inside the Capitol building.

12. On January 6, 2021, at approximately 1:00 p.m., the Joint Session convened in the Capitol building to certify the Electoral College vote. Vice President Michael R. Pence, in his constitutional duty as President of the Senate, presided over the Joint Session.

13. A large crowd began to gather outside the Capitol perimeter as the Joint Session got underway. Crowd members eventually forced their way through, up, and over Capitol Police

barricades and advanced to the building's exterior façade. Capitol Police officers attempted to maintain order and stop the crowd from entering the Capitol building, to which the doors and windows were locked or otherwise secured. Nonetheless, shortly after 2:00 p.m., crowd members forced entry into the Capitol building by breaking windows, ramming open doors, and assaulting Capitol Police officers. Other crowd members encouraged and otherwise assisted the forced entry. The crowd was not lawfully authorized to enter or remain inside the Capitol, and no crowd member submitted to security screenings or weapons checks by Capitol Police or other security officials.

14. Shortly thereafter, at approximately 2:20 p.m., members of the House and Senate (including Vice President Pence)—who had withdrawn to separate chambers to resolve an objection—were evacuated from their respective chambers. The Joint Session and the entire official proceeding of the Congress was halted while Capitol Police and other law enforcement officers worked to restore order and clear the Capitol of the unlawful occupants.

15. Later that night, law enforcement regained control of the Capitol. At approximately 8:00 p.m., the Joint Session reconvened, presided over by Vice President Pence, who had remained hidden within the Capitol building throughout these events.

16. In the course of these events, approximately many members of the Capitol Police and the Metropolitan Police Department were assaulted. Additionally, many media members were assaulted and had cameras and other news-gathering equipment destroyed, and the Capitol suffered millions of dollars in damage—including broken windows and doors, graffiti, and residue of various pepper sprays, tear gas, and fire extinguishers deployed both by crowd members who stormed the Capitol and by Capitol Police officers trying to restore order.

17. As a result of these events, the U.S. Capitol Police, the FBI, and assisting law enforcement agencies are investigating the riot, the actors, and related offenses – including

possible violations of 18 U.S.C. §§ 111 (Assaulting a Federal Agent), 231 (Civil Disorders), 371 (Conspiracy), 372 (Conspiracy to Assault Federal Officers), 930 (Possession of Firearms and Dangerous Weapons in Federal Facilities), 1030 (Unauthorized Access of a Protected Computer), 1114 (Protection of a Federal Agent), 1361 (Destruction of Government Property), 1505 and 1512 (Obstruction of Congress), 1752(a) (Unlawful Entry on Restricted Buildings or Grounds), 2101 (Rioting), 2383 (Rebellion or Insurrection), and 2384 (Seditious Conspiracy), and 40 U.S.C. § 5104 (Injury to Property, Violent Entry, and Disorderly Conduct on Capitol Grounds) – that occurred at the United States Capitol Building, located at 1 First Street, NW, Washington, D.C., 20510, on January 6, 2021.

Facts Specific to This Application

Identification of Peter Schwartz

18. On January 11, 2021, the FBI National Threats Operations Center received a tip from an individual (hereinafter W-1) who is personally acquainted with PETER SCHWARTZ. W-1 reported that “Pete Schwartz” was involved in the Capitol Riots. W-1 saw a picture of Schwartz on the Capitol building steps that appeared to have been taken on January 6, 2021. W-1 provided a Facebook URL for Schwartz’s Facebook page.

19. On January 24, 2021, your affiant contacted W-1 about Schwartz. W-1 stated that he is friends with Schwartz and last saw Schwartz in-person about six months ago. He noted that Schwartz still owes him money. W-1 indicated that when he spoke with Schwartz about the riots on January 6, 2021, Schwartz told him, “We were there.” W-1 also identified Schwartz in a “Be On the Lookout” (“BOLO”) photograph disseminated by the FBI. The BOLO photograph is a

screenshot taken from a video of Schwartz using mace against law enforcement officers on January 6, 2021, outside the Capitol, as shown here:¹



20. That same day, FBI agents in Kentucky interviewed a Lieutenant from the Owensboro, KY, police force who had served legal process on Schwartz in April 2020. When he

¹ Your affiant is using the generic term “mace” to describe the substance that SCHWARTZ sprayed out of various canisters at officers on January 6, 2021. You affiant believes the substance was some form of lachrymatory agent, such as mace or pepper spray, based on officer reports that numerous individuals within the crowd were spraying mace-like substances at them on January 6, 2021. Some of the canisters wielded by SCHWARTZ appear identical to MPD issued MK-9 pepper spray, which is regularly carried and was carried by MPD officers on January 6, 2021. Additionally, the officers’ reaction to the spray was consistent with the substance being a chemical irritant.

served process on Schwartz, he had a face-to-face conversation with him. The lieutenant identified Schwartz in the BOLO as well.²

21. Your affiant also reviewed the public Facebook profile for Schwartz, as identified by W-1. A post from January 7, 2021, that appeared to be made by Schwartz, states: “All the violence from the left was terrorism. What happened yesterday was the opening of a war. I was there and whether people will acknowledge it or not we are now at war. It would be wise to be ready!”

22. In the comments written under the January 7, 2021, post, Schwartz writes: “I’ll tell you this . . . I’m shocked reading the reports of what happened yesterday. Very different than what I saw up close and personal. (We’re still spitting up gas and mace today.)”

Schwartz’s actions against police officers on January 6, 2021

23. MPD body-worn camera video shows Schwartz at the Capitol on January 6, 2021, participating in multiple assaults on officers. In the first assault, beginning at around 2:30 p.m., Schwartz is captured on the body-worn camera video of Officer Christopher Boyle. In the video, a large group of USCP and MPD officers are gathered to protect the doors of the Lower West Terrace and tunnel that leads into the Capitol Building. A large group of rioters is gathered near the officers on the west terrace, which is on the exterior of the building. In the video, Schwartz is seen wearing a distinctive yellow-and-blue checked jacket. He is carrying a large canister

² The FBI has received numerous tips in response to the BOLO, most of which identified Schwartz. However, the FBI has also received two tips identifying individuals other than Schwartz. One of those identified an individual in Utah based on similar ideology and beards. Another identified an individual in Oklahoma whom the tipster last saw in 2011. However, there is no other evidence to connect either individual to the events at the Capitol on January 6, 2021.

containing mace. He then repeatedly walks, points the canister, and sprays the mace directly at the group of officers, as depicted here:



24. In the second officer assault, which takes place at approximately 2:35, Schwartz is captured on the BWC of Officer Larry Hale Jr. In that video, Schwartz can be seen extending his arm out toward a group of officers while holding a can of mace. He then sprays a stream of mace directly at the group of officers. That same assault is also captured on a video from “Action 8 News” that was posted to YouTube on January 7, 2021. Your affiant viewed the publicly-available video on YouTube several days later. The video briefly shows Schwartz and then pans across the crowd outside the Capitol building on January 6, 2021. The video shows an arm--with the same distinctive yellow-and-blue checked pattern worn by Schwartz--reach out and directly spray an

officer in the face with mace, as shown here:



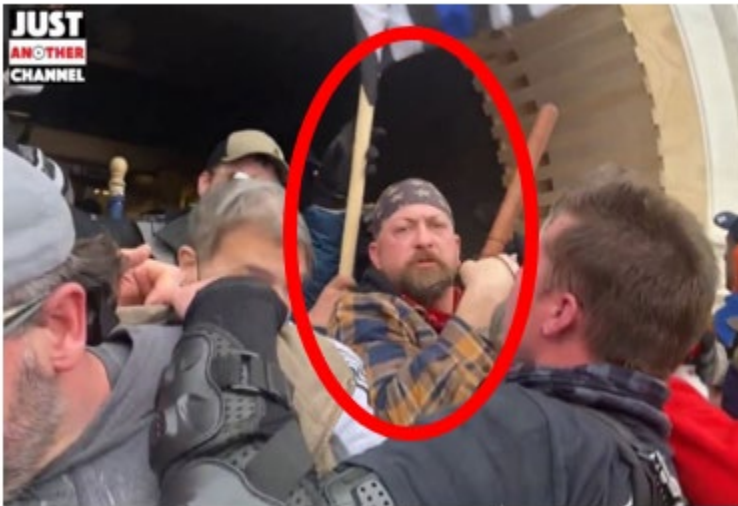
The officer quickly turns away after being sprayed.

25. Schwartz is next captured on surveillance video that was filmed inside of the Lower West Terrace Arch beginning at approximately 3:07 p.m. The video camera is located inside of the arch, facing toward the terrace. The video captures Schwartz entering the archway around 3:07 and remaining inside for approximately six minutes. While inside the archway, Schwartz can be seen handing a can of mace to another rioter. That rioter then hands the can of mace to a third rioter, who is at the front of the crowd near the police line. The third rioter tries to use the mace can but it does not work. He then hands the canister back to Schwartz, who “fixes” it. Schwartz then hands it back to the third rioter who then points the canister at the officers and appears to activate it. The third rioter then moves off camera.

26. Schwartz remains inside the arch for several more minutes. At one point he pushes the crowd forward as the crowd attempts--through brute force--to break through the line of officers at the entrance.

27. Another open-source video, filmed by photojournalist Jon Farina, captures Schwartz using the force of his body to “heave-ho” as the crowd attempts to breach the police line inside the arch. Twenty seconds later, Officer Daniel Hodges can be seen being crushed in the archway door as defendant Patrick McCaughey pushes a riot shield against Officers Hodges, rendering him unable to move. Schwartz is a member of the “heave-ho” mob that is trying to push through the police line at the same time that Officer Hodges is assaulted.

28. Finally, Schwartz is also seen in the video carrying a wooden baton in the midst of the large crowd of rioters near the tunnel arch, as shown here:



29. That baton is also seen on his waistband in the BWC video as well.

Schwartz's Arrest and Seizure of Evidence

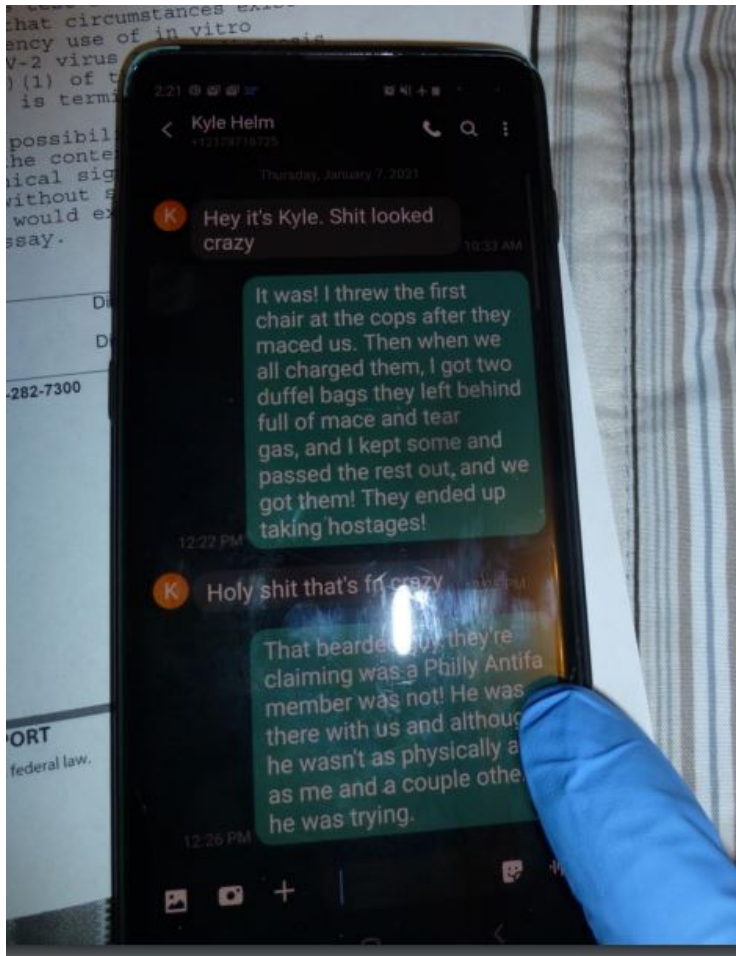
30. On February 4, 2021 Schwartz was arrested in Uniontown, Pennsylvania pursuant to an arrest warrant issued by the Honorable Judge Zia M. Faruqui in the United States District Court for the District of Columbia.

31. On the same day, FBI agents searched 36 Cleveland Avenue, Uniontown Pennsylvania, which is where Schwartz was living, pursuant to a search and seizure warrant issued by the Honorable Patricia L. Dodge in the Western District of Pennsylvania.

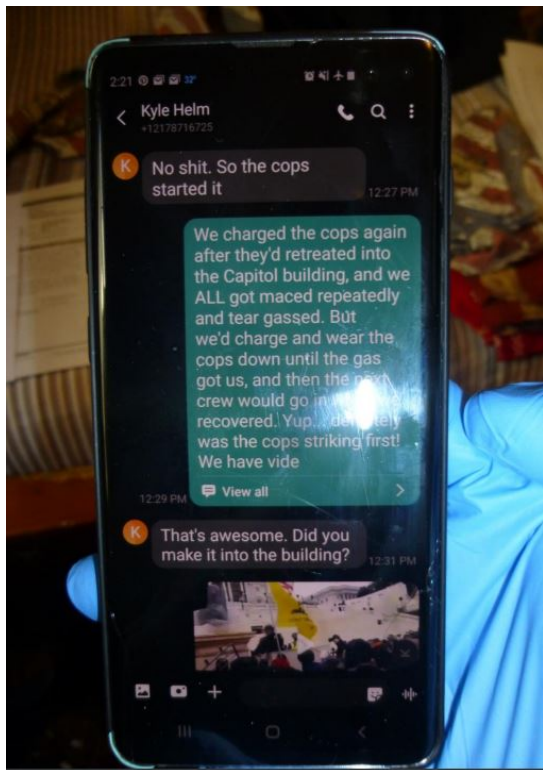
32. FBI agents seized from the residence clothing consistent with that worn by Schwartz on January 6, 2021, including a yellow and blue flannel checked jacket, brown boots, and an American flag bandana. FBI agents also seized a Samsung Galaxy S10 cellular telephone bearing IMEI 356021101533525 from the residence.

33. During the execution of the search warrant, pursuant to the language in the warrant authorizing use of biometrics to unlock digital devices on premises, FBI agents used Schwartz's fingerprint to unlock the Samsung Galaxy S10 cellular telephone.

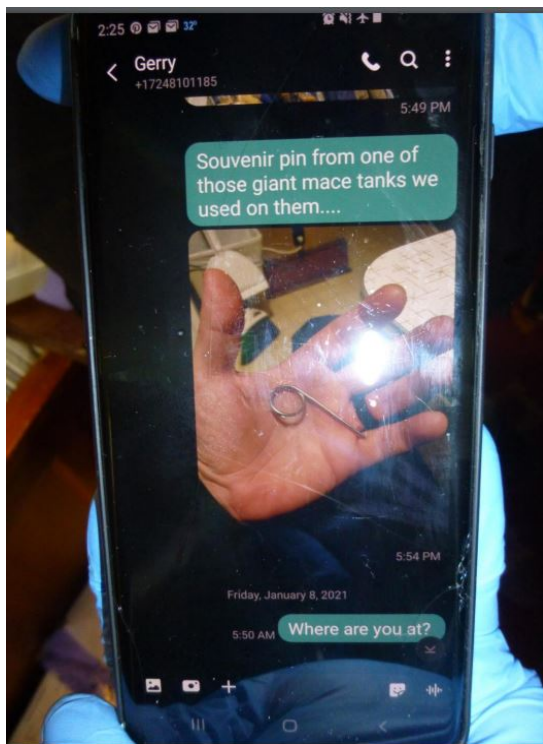
34. Agents captured photographs of several text messages dated January 6, 2021 and January 7, 2021 on the cellular phone including the following text message in which Schwartz admits to “thr[o]w[ing] the first chair at the cops after they maced us” and then stealing “two duffel bags they left behind full of mace and tear gas” and then “g[e]t[tting] them!”



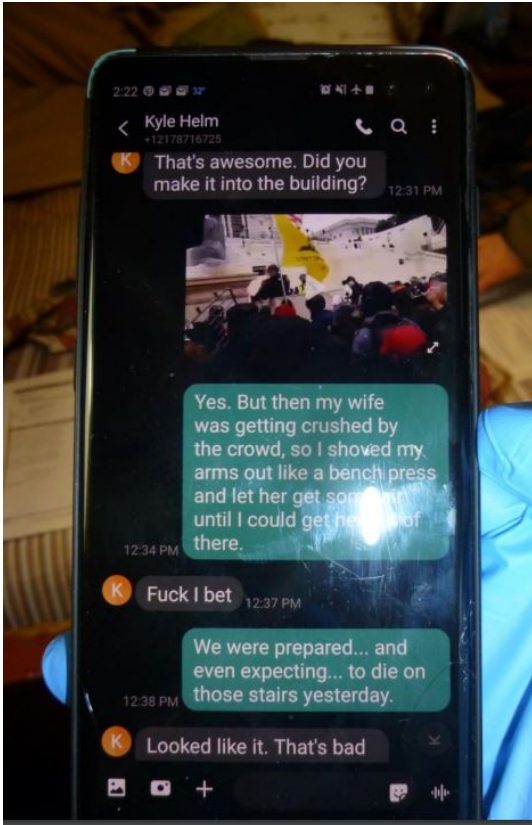
35. He also brags in another text message that he “charged the cops again after they’d retreated into the Capitol building, and we ALL got maced repeatedly,”:



36. He also sent a photograph by text message of, in his words, “a souvenir pin from one of those giant mace tanks we used on [the officers]:”



37. He further claimed that he was “expecting . . . to die on those stairs yesterday”:



38. Due to an oversight, after the FBI agents captured screenshots of text messages from Schwartz’s phone, the phone data was not forensically extracted and the phone was not searched further despite a signed search warrant authorizing such a search, and no data has been extracted to-date. Therefore, while the FBI might already have all necessary authority to examine the Device, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Device will comply with the Fourth Amendment and other applicable laws.

39. The phone has been maintained pursuant to FBI evidence policy since February 4, 2021 and is currently located at the FBI Washington Field Office, 601 4th St. N.W., Washington, DC, 20535.

40. Screenshots of the “About phone” section taken when it was unlocked with biometrics indicate the associated telephone number of the Samsung Galaxy S10 cellular telephone

bearing IMEI 356021101533525 is 270-903-4010. AT&T records provided on February 2, 2021 responsive to a federal search warrant indicate the subscriber of telephone number 270-903-4010 from June 17, 2020 to February 2, 2021 was “Pete Schwartz.”

41. On February 4, 2021, while in FBI custody and after being informed of his *Miranda* rights, Schwartz agreed to speak to FBI agents. During the interview, Schwartz stated he drove to Washington, DC on January 6, 2021 to attend the Stop the Steal rally. Schwartz stated he brought his cellular telephone with him to the Capitol and carried the phone in his pocket. Schwartz stated he may have worn a checkered jacket. Schwartz stated he made it to the top of the Capitol stairs. Schwartz stated he did not get into any altercations or violent encounters during his time at the Capitol and he did not have any interactions with police. Schwartz stated his cellular telephone was an Android and he opened it with his thumbprint, as explained in paragraph 33 above.

TECHNICAL TERMS

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

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

1) A “computer” means an electronic, magnetic, optical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e)(1). Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited

to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.

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

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

b. “Wireless telephone” (or mobile telephone, or cellular telephone), a type of digital device, is a handheld wireless device used for voice and data communication at least in part through radio signals and also often through “wi-fi” networks. When communicating via radio signals, these telephones send signals through networks of transmitters/receivers, enabling communication with other wireless telephones, traditional “land line” telephones, computers, and other digital devices. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling

voice communications, wireless telephones offer a broad range of applications and capabilities. These include, variously: storing names and phone numbers in electronic “address books”; sending, receiving, and storing text messages, e-mail, and other forms of messaging; taking, sending, receiving, and storing still photographs and video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; utilizing global positioning system (“GPS”) locating and tracking technology, and accessing and downloading information from the Internet.

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

d. A “GPS” navigation device, including certain wireless phones and tablets, uses the Global Positioning System (generally abbreviated “GPS”) to display its current location, and often retains records of its historical locations. Some GPS navigation devices can give a user driving or walking directions to another location, and may contain records of the addresses or locations involved in such historical navigation. The GPS consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives

signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

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

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

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

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

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

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

k. A “router” often serves as a wireless Internet access point for a single or multiple devices, and directs traffic between computers connected to a network (whether by wire or wirelessly). A router connected to the Internet collects traffic bound for the Internet from its client machines and sends out requests on their behalf. The router also distributes to the relevant

client inbound traffic arriving from the Internet. A router usually retains logs for any devices using that router for Internet connectivity. Routers, in turn, are typically connected to a modem.

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

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

n. “Peer to Peer file sharing” (P2P) is a method of communication available to Internet users through the use of special software, which may be downloaded from the Internet. In general, P2P software allows a user to share files on a computer with other computer users running compatible P2P software. A user may obtain files by opening the P2P software on the user’s computer and searching for files that are currently being shared on the network. A P2P file transfer is assisted by reference to the IP addresses of computers on the network: an IP address identifies the location of each P2P computer and makes it possible for data to be transferred

between computers. One aspect of P2P file sharing is that multiple files may be downloaded at the same time. Another aspect of P2P file sharing is that, when downloading a file, portions of that file may come from multiple other users on the network to facilitate faster downloading.

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

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

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

p. "Encryption" is the process of encoding messages or information in such a way that eavesdroppers or hackers cannot read it but authorized parties can. In an encryption

scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any unintended party that can see the ciphertext should not be able to determine anything about the original message. An authorized party, however, is able to decode the ciphertext using a decryption algorithm that usually requires a secret decryption key, to which adversaries do not have access.

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

43. Based on my training, experience, and research, I know that the Device, a Samsung Galaxy S10 cellular telephone has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, video recorder, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device, and sometimes by implication who did not, as well as evidence relating to the commission of the offenses under investigation.

COMPUTERS, ELECTRONIC/MAGNETIC STORAGE, AND FORENSIC ANALYSIS

44. As described above and in Attachment B, this application seeks permission to search for evidence, fruits, contraband, instrumentalities, and information that might be found within the Device, in whatever form they are found. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that there is probable cause

to believe that the records and information described in Attachment B will be stored in the Device for at least the following reasons:

a. Individuals who engage in criminal activity, including violations of 18 U.S.C. §§ 111(a)(1) and (b), 2; 18 U.S.C. § 231(a)(3), 2; 18 U.S.C. §§ 1512(c)(2), 2; 18 U.S.C. § 1752(a)(1) and (b)(1)(A); 18 U.S.C. § 1752(a)(2) and (b)(1)(A); 18 U.S.C. § 1752(a)(3); 18 U.S.C. § 1752(a)(4) and (b)(1)(A); 40 U.S.C. § 5104(e)(2)(D); 40 U.S.C. § 5104(e)(2)(E); and 40 U.S.C. § 5104(e)(2)(F), particularly those individuals who committed these offenses at the Capitol on January 6, 2021, used digital devices, like the Device, to communicate with co-conspirators and others about the riots and to document and record their illegal activity, which includes logs of online chats with co-conspirators; email correspondence; text or other “Short Message Service” (“SMS”) messages; contact information of co-conspirators, including telephone numbers, email addresses, identifiers for instant messaging and social medial accounts; stolen financial and personal identification data, including bank account numbers, credit card numbers, and names, addresses, telephone numbers, and social security numbers of other individuals.

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

c. Digital device files, or remnants of such files, can be recovered months or even many years after they have been downloaded onto the medium or device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person “deletes” a file on a digital device such as

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

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

d. Although some of the records called for by this warrant might be found in the form of user-generated documents or records (such as word processing, picture, movie, or

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

e. Forensic evidence on a digital device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information,

configuration files, user profiles, e-mail, e-mail address books, chats, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time, and potentially who did not.

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

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

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

METHODS TO BE USED TO SEARCH DIGITAL DEVICES

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

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

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

k. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device

was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a digital device is not segregable from the digital device itself. Analysis of the digital device as a whole to demonstrate the absence of particular data or software requires specialized tools and a controlled laboratory environment, and can require substantial time.

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

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

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

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

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

o. The digital devices, and/or any digital images thereof created by law enforcement, sometimes with the aid of a technical expert, in an appropriate setting, in aid of the examination and review, will be examined and reviewed in order to extract and seize the information, records, or evidence described in Attachment B.

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

storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

q. In searching the digital devices, the forensic examiners may examine as much of the contents of the digital devices as deemed necessary to make a determination as to whether the contents fall within the items to be seized as set forth in Attachment B. In addition, the forensic examiners may search for and attempt to recover “deleted,” “hidden,” or encrypted data to determine whether the contents fall within the items to be seized as described in Attachment B. Any search techniques or protocols used in searching the contents of the Device(s) will be specifically chosen to identify the specific items to be seized under this warrant.

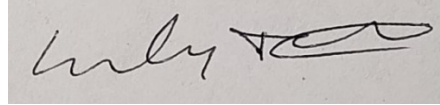
AUTHORIZATION TO SEARCH AT ANY TIME OF THE DAY OR NIGHT

48. Because forensic examiners will be conducting their search of the digital devices in a law enforcement setting over a potentially prolonged period of time, I respectfully submit that good cause has been shown, and therefore request authority, to conduct the search at any time of the day or night.

CONCLUSION

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

Respectfully submitted,

A rectangular area containing a handwritten signature in black ink. The signature appears to be "Emily Eckert" written in a cursive style.

Emily Eckert
Special Agent
FBI

Subscribed and sworn pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3) on September 16, 2021.

UNITED STATES MAGISTRATE JUDGE