IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

| | |
|---|---|
| IN THE MATTER OF THE SEARCH OF<br><br>ONE Galaxy Z Flip 3 5G CELL PHONE, MODEL: SM-F711U, SERIAL: R5CR80Q3G1B, IEMI: 350345700268274 , CURRENTLY LOCATED AT THE FEDERAL BUREAU OF INVESTIGATION (FBI), 15 CONSTITUTION DRIVE, BEDFORD, NEW HAMPSHIRE | Case No. 22-mj-13-01-AJ |

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

I, Mark A. Hastbacka, 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—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been since October of 1997. I am currently assigned to the Joint Terrorism Task Force ("JTTF") of the FBI's Boston Division/ Bedford, New Hampshire (NH) office. Before I became a Special Agent, I was a Police Officer in Nashua, New Hampshire for ten years. Over my career, I have investigated and assisted investigations of robberies, burglaries, larcenies, assaults, and terrorism, related offenses. During my career, my investigations have included the use of various surveillance techniques and the execution of various search, seizure, and arrest warrants

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

## IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is a Galaxy Z Flip 3 5G cell phone, Model: SM-F711U, Serial: R5CR80Q3G1B, IEMI: 350345700268274, hereinafter the "Device." The Device is currently located at the Federal Bureau of Investigation (FBI), 15 Constitution Drive, Bedford, New Hampshire.

5. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

## PROBABLE CAUSE

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

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

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

side, and two large skylights into the Visitor's Center surrounded by a concrete parkway. All of this area was barricaded and off limits to the public on January 6, 2021.

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

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

10. On January 6, 2021, a joint session of the United States Congress convened at the U.S. Capitol. During the joint session, elected members of the United States House of Representatives and the United States Senate were meeting in separate chambers of the U.S. Capitol to certify the vote count of the Electoral College of the 2020 Presidential Election, which took place on November 3, 2020 ("Certification"). The joint session began at approximately 1:00 p.m. Eastern Standard Time (EST). Shortly thereafter, by approximately 1:30 p.m., the House and Senate adjourned to separate chambers to resolve a particular objection. Vice President Mike Pence was present and presiding, first in the joint session, and then in the Senate chamber.

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

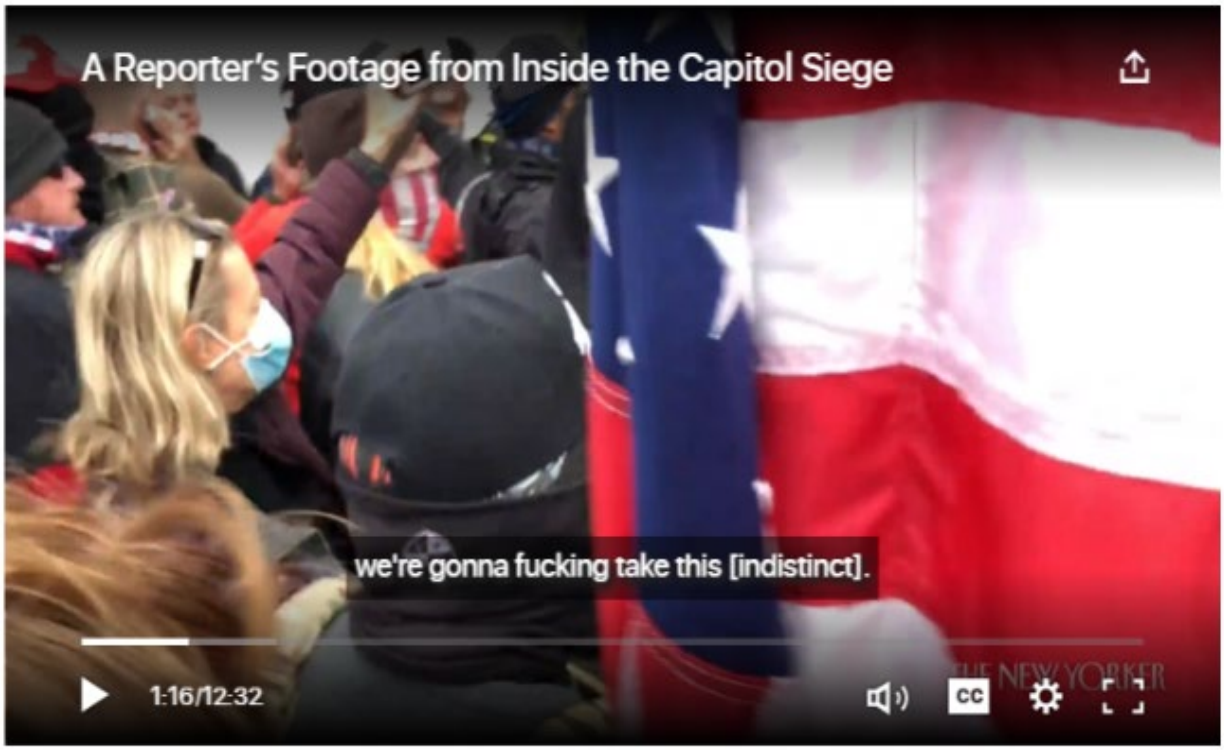
12. At around 1:00 p.m. EST, known and unknown individuals broke through the police lines, toppled the outside barricades protecting the U.S. Capitol, and pushed past USCP and supporting law enforcement officers there to protect the U.S. Capitol.

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

14. Media reporting showed a group of individuals outside of the Capitol chanting, "Hang Mike Pence." I know from this investigation that some individuals believed that Vice President Pence possessed the ability to prevent the certification of the presidential election and that his failure to do so made him a traitor.

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

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




17. Shortly thereafter, at approximately 2:20 p.m. members of the United States House of Representatives and United States Senate, including the President of the Senate, Vice President Mike Pence, were instructed to—and did—evacuate the chambers. That is, at or about this time, USCP ordered all nearby staff, Senators, and reporters into the Senate chamber and locked it down. USCP ordered a similar lockdown in the House chamber. As the subjects attempted to break into the House chamber, by breaking the windows on the chamber door, law enforcement were forced to draw their weapons to protect the victims sheltering inside.

18. At approximately 2:30 p.m. EST, known and unknown subjects broke windows and pushed past USCP and supporting law enforcement officers forcing their way into the U.S. Capitol on both the west side and the east side of the building. Once inside, the subjects broke windows and doors, destroyed property, stole property, and assaulted federal police officers. Many of the federal police officers were injured, several were admitted to the hospital, and at least one federal

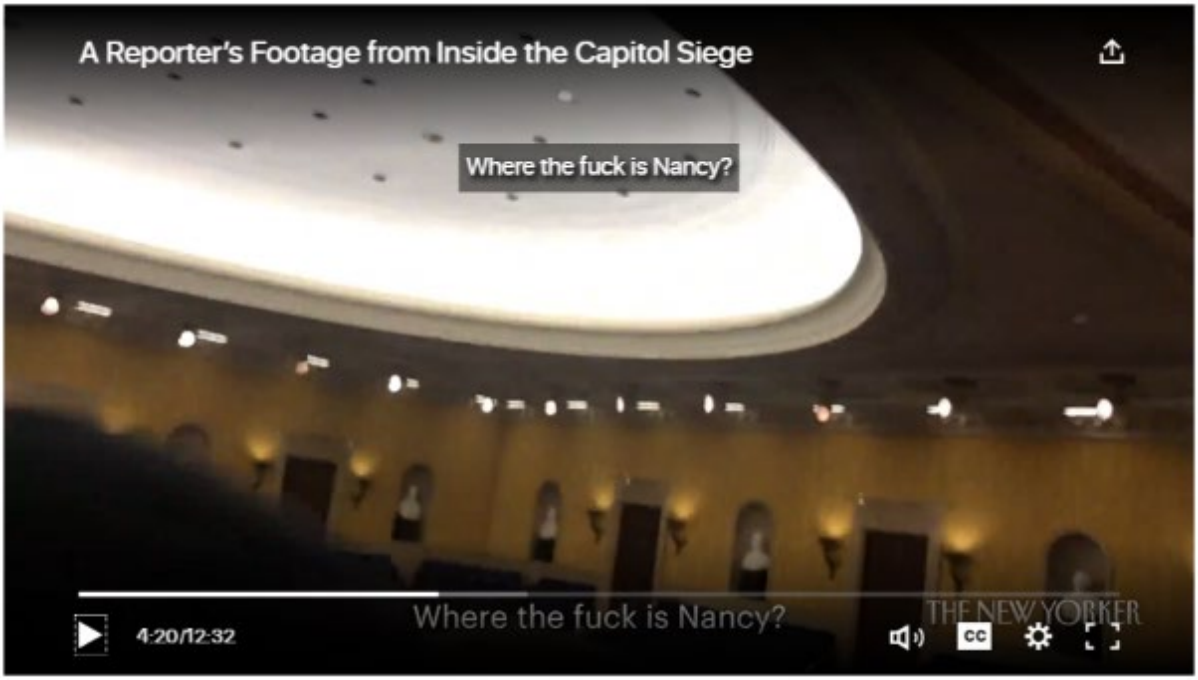
police officer died as a result of the injuries he sustained. The subjects also confronted and terrorized members of Congress, Congressional staff, and the media. The subjects carried weapons including tire irons, sledgehammers, bear spray, and Tasers. They also took police equipment from overrun police including shields and police batons. At least one of the subjects carried a handgun with an extended magazine. These actions by the unknown individuals resulted in the disruption and ultimate delay of the vote Certification.

19. Also, at approximately 2:30 p.m. EST, USCP ordered the evacuation of lawmakers, Vice President Mike Pence, and president pro tempore of the Senate, Charles Grassley, for their safety.

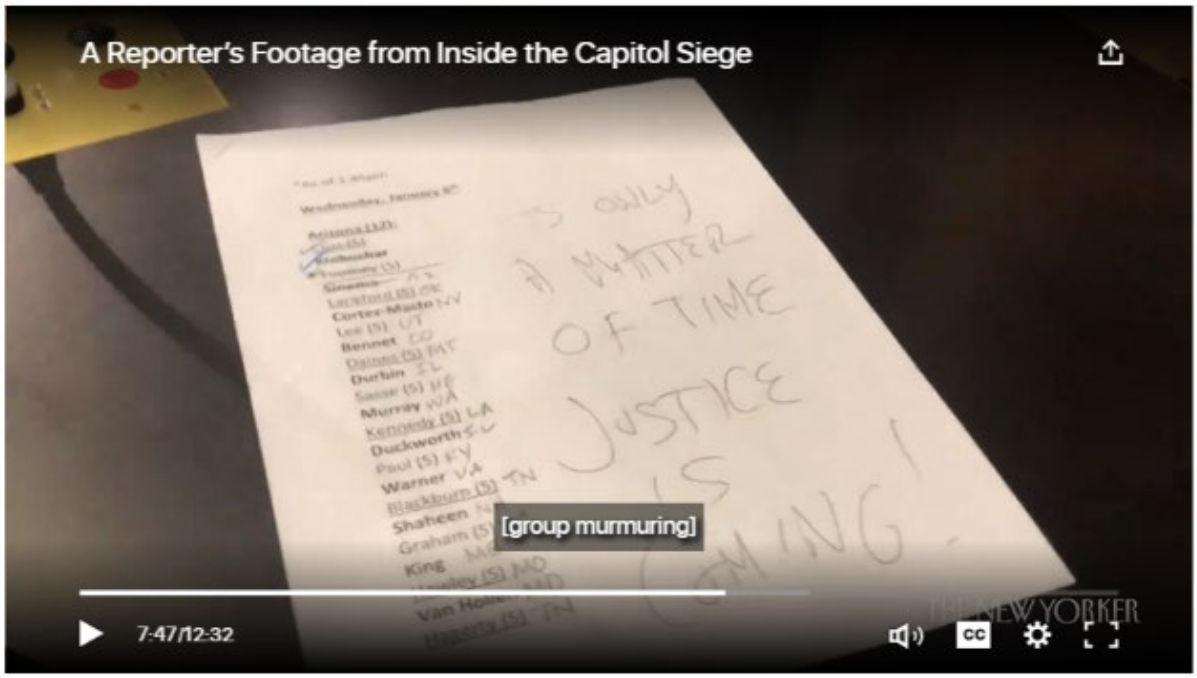
20. At around 2:45 p.m. EST, subjects broke into the office of House Speaker Nancy Pelosi.

21. At around 2:47 p.m., subjects broke into the United States Senate Chamber. Publicly available video shows an individual asking, "Where are they?" as they opened up the door to the Senate Chamber. Based upon the context, law enforcement believes that the word "they" is in reference to members of Congress.


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




23. An unknown subject left a note on the podium on the floor of the Senate Chamber. This note, captured by the filming reporter, stated "A Matter of Time Justice is Coming."



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

25. At around 2:48 p.m. EST, DC Mayor Muriel Bowser announced a citywide curfew beginning at 6:00 p.m.

26. At around 2:45 p.m. EST, one subject was shot and killed while attempting to break into the House chamber through the broken windows.

27. At about 3:25 p.m. EST, law enforcement officers cleared the Senate floor.

28. Between 3:25 and around 6:30 p.m. EST, law enforcement was able to clear the U.S. Capitol of all of the subjects.

29. Based on these events, all proceedings of the United States Congress, including the joint session, were effectively suspended until shortly after 8:00 p.m. the same day. In light of the dangerous circumstances caused by the unlawful entry to the U.S. Capitol, including the danger posed by individuals who had entered the U.S. Capitol without any security screening or weapons check, Congressional proceedings could not resume until after every unauthorized occupant had

left the U.S. Capitol, and the building had been confirmed secured. The proceedings resumed at approximately 8:00 pm after the building had been secured. Vice President Pence remained in the United States Capitol from the time he was evacuated from the Senate Chamber until the session resumed.

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

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

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

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

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

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

U.S. Capitol live-streamed their activities, including those described above as well as statements about these activities.

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


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

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

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

***Facts Specific to This Application***

**Tipster Information**

37. On or around January 7, 2021, the FBI received a text tip about Kirstyn Niemela that stated the tipster was unsure if Niemela was "directly part of the riots, but she's currently there and has posted numerous live videos on her FB [Facebook] page." The tipster also indicated Niemela posted, "grab your popcorn… it's coming…." Some of the language in the tip appeared to be cut off and was not available in the TIPS database.

38. A search of Niemela's name in the TIPS database revealed on June 13, 2021, the FBI received a tip from Witness-1 (W-1). W-1 reported that they and Niemela were friends months ago, but they distanced themself because of her rhetoric. They indicated they talked to her two weeks earlier and Niemela indicated she was "going to take back the country." Niemela told W–1 she was in Washington, DC on January 6, 2021 and she showed them a video of her breaking a window in the Capitol building. She also mentioned to them that she was a member of the Proud Boys. W-1 also claimed Niemela stated that "there is something big coming… [that] the whole nation will watch it happen." W-1 mentioned that Niemela "carries a[n] illegal handgun with her at all times." W-1 also listed Niemela's phone number as a telephone number ending in 7169.

39. On Facebook postings made by another individual, also obtained through TTK database, a woman believed to be Niemela can be seen in photos outside the U.S. Capitol on January 6, 2021 wearing an American flag as a cape, sunglasses, and a black sweatshirt that reads "We the People ARE PISSED OFF." In both Facebook photos this woman can be seen with another woman in an identical sweatshirt. In one posted photograph, the women are seen with two men:

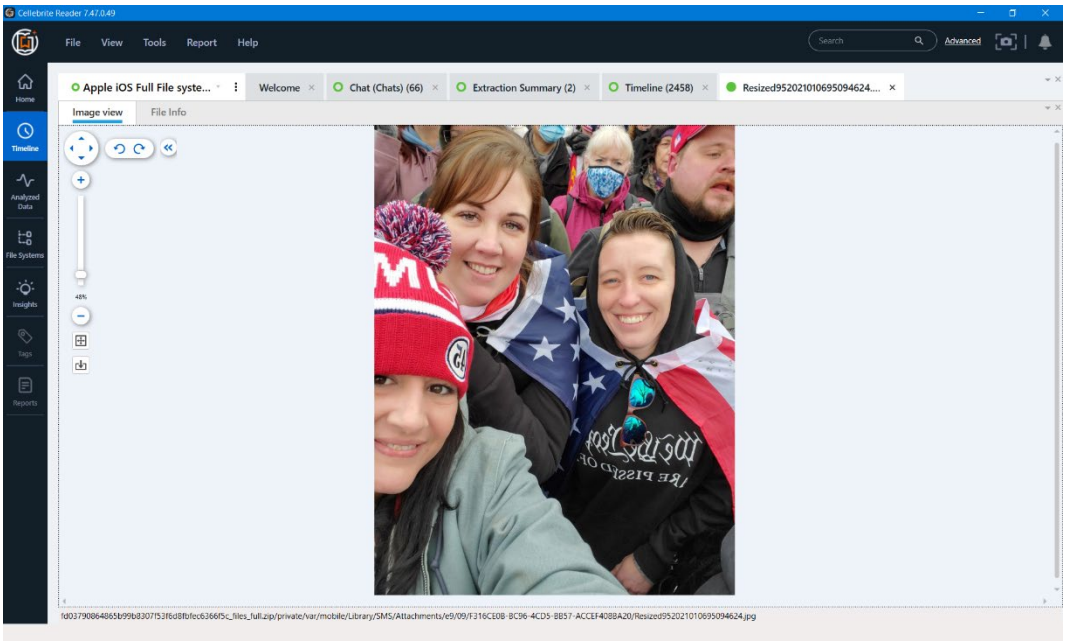
**Figure 1:**


Through open-source research, the FBI identified the man wearing the red cap and body armor as Michael Eckerman. Eckerman has since been indicted in the District of Columbia for his part in the riots occurring on January 6, 2021.

40. W-1 was interviewed by agents with the FBI on November 4, 2021 and acknowledged they had a falling out with Niemela because of a personal matter and that they had distanced themselves from Niemela because they were a felon and didn't want trouble. W-1 stated they had known Niemela for approximately five years and had lived with her and her mother two years ago for approximately four months. W-1 stated Niemela told them that she and

her girlfriend had participated in the U.S. Capitol riot of January 6, 2021 and showed them a video on her cell phone claiming it to be from the riots. W-1 also stated they could only make out feet and legs in the video Niemela showed them. W-1 advised that the girlfriend Niemela was referencing in the conversation was "Stefanie," who lived in Dracut, MA, and whom W-1 had met a couple of times. W-1 was shown a series of 14 still photographs taken from within the United States Capitol and identified Niemela and "Stefanie" in the two Facebook photographs posted by others - Figure 1 above and Figure 2, below :

**Figure 2:**




From the still photographs below, from the security cameras within the United States Capitol, W-1 positively identified both Niemela and "Stefanie" inside the United States Capitol:

**Figure 3:**

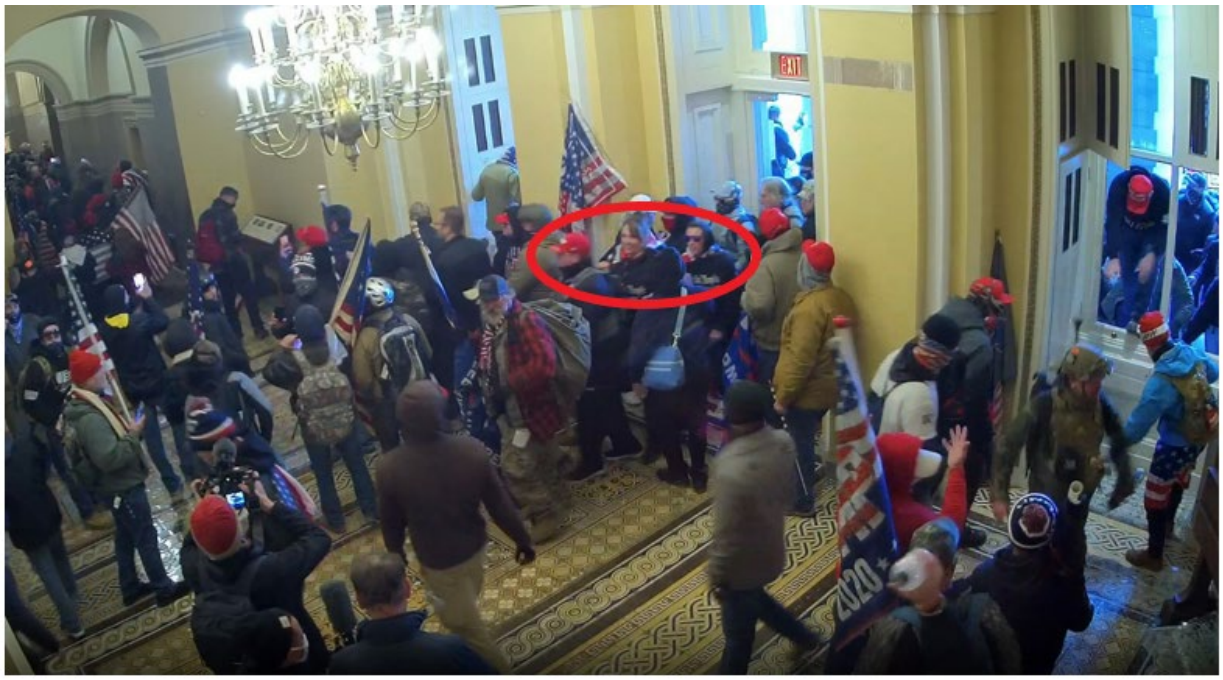
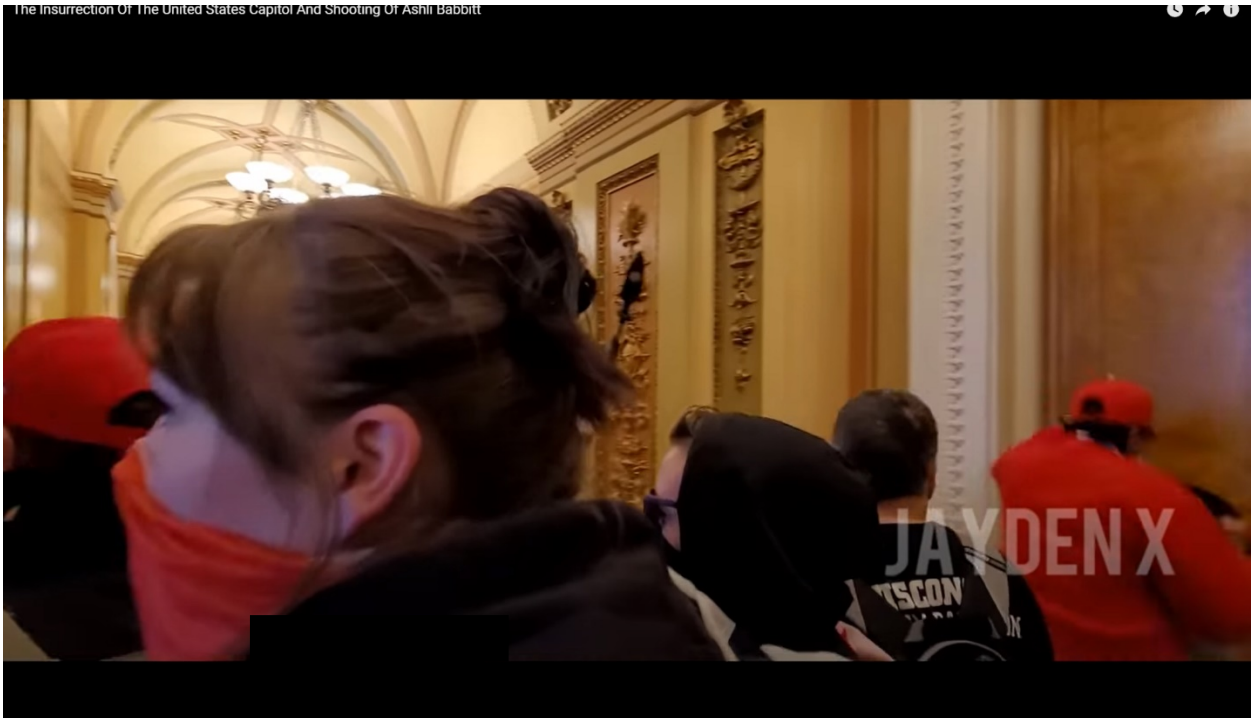



**Figure 4:**

**Figure 5:**


**Figure 6:**

**Figure 7:**


The Insurrection Of The United States Capitol And Shooting Of Ashli Babbitt
JAYDEN X

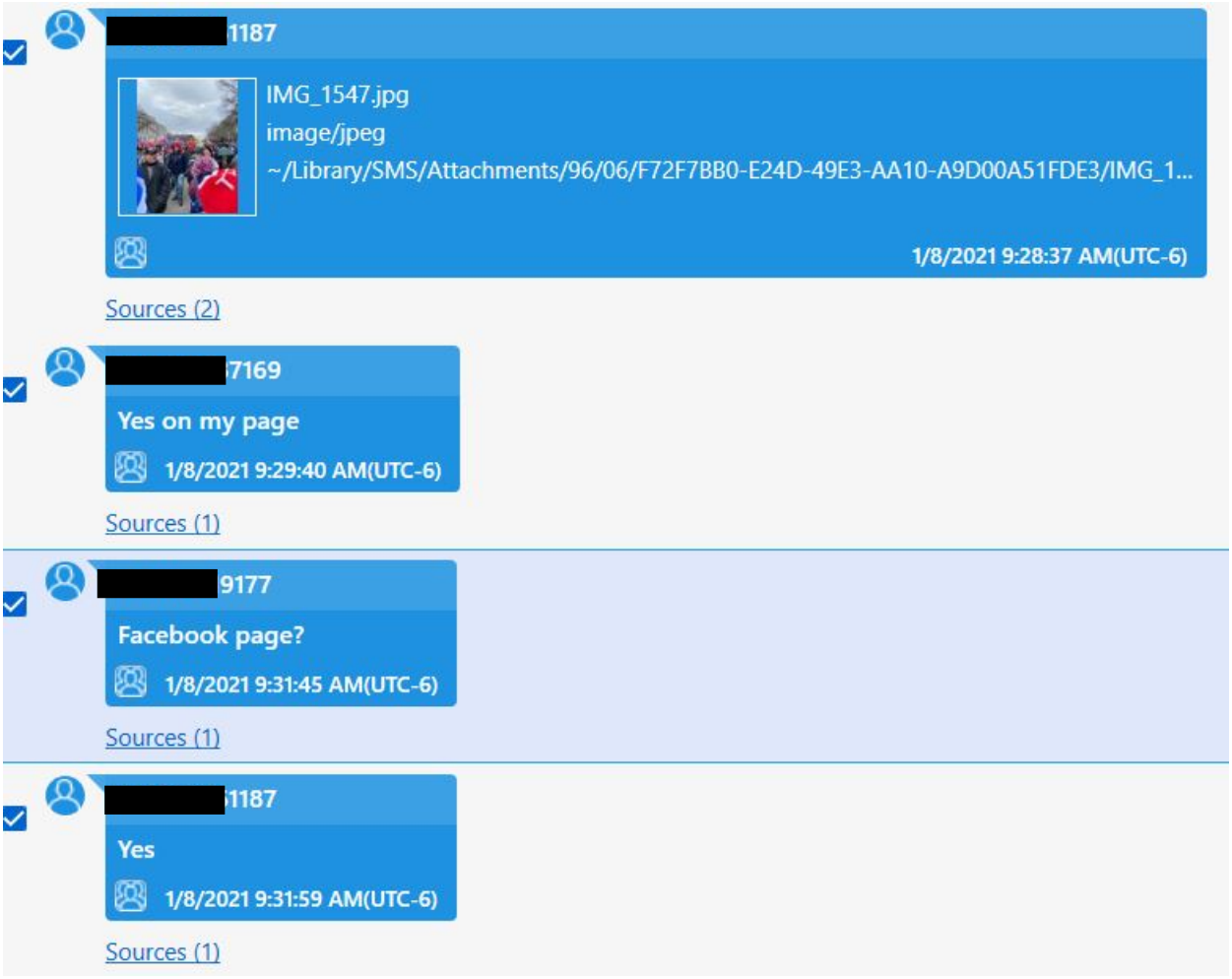

The Insurrection Of The United States Capitol And Shooting Of Ashli Babbitt
JAYDEN X

**Figure 9:**


41. "Stefanie" has been positively identified at Stefanie Nicole Chiguer from an interview of W-1 who stated during their interview that Kirstyn Niemela had been dating "Stefanie" who resided in Dracut, MA. I found a police incident report that showed on or about September 4, 2021, the Dracut, MA Police Department responded to the residence of Stefanie Nicole Chiguer, in Dracut, MA for a domestic dispute between Chiguer and Niemela. I obtained a State of Massachusetts driver's license photo for Stefanie Chiguer and positively identified Chiguer as the female party with Niemela in paragraph #37 above.

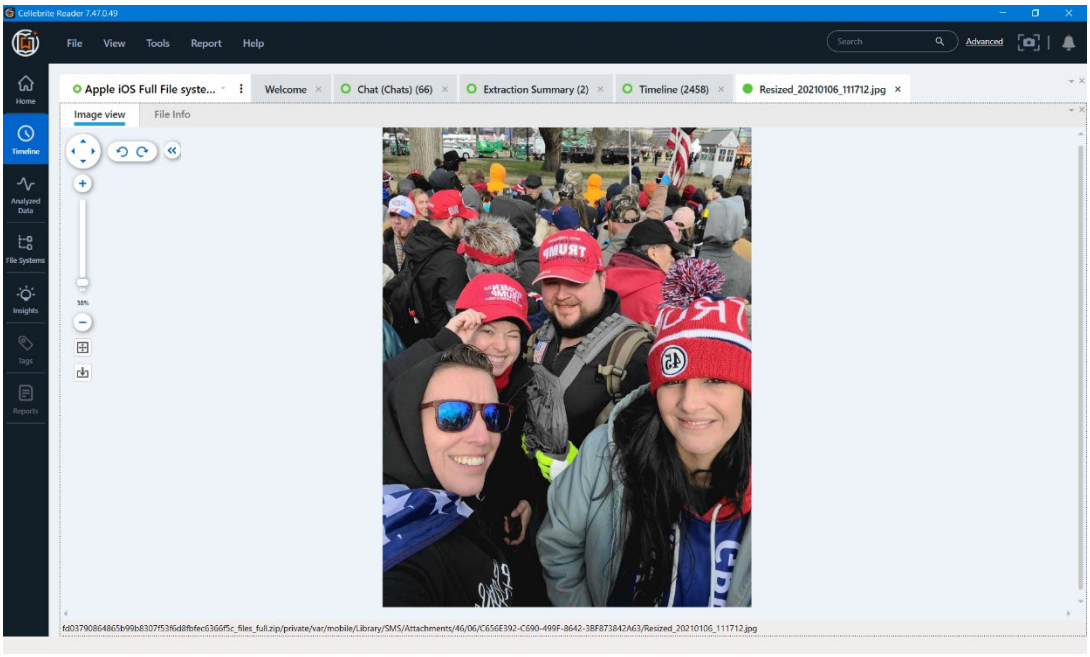
42. Michael Eckerman's telephone was seized on September 17, 2021 by the FBI pursuant to a search warrant issued by a federal judge in the District of Kansas. Upon searching the telephone for pertinent evidence within the scope of the search warrant, a text chain was found which included the telephone number ending in 7169, identified by W-1 as belonging to Niemela.

Niemela texted that the photographs being used by another group member were from her (Niemela's) Facebook page:



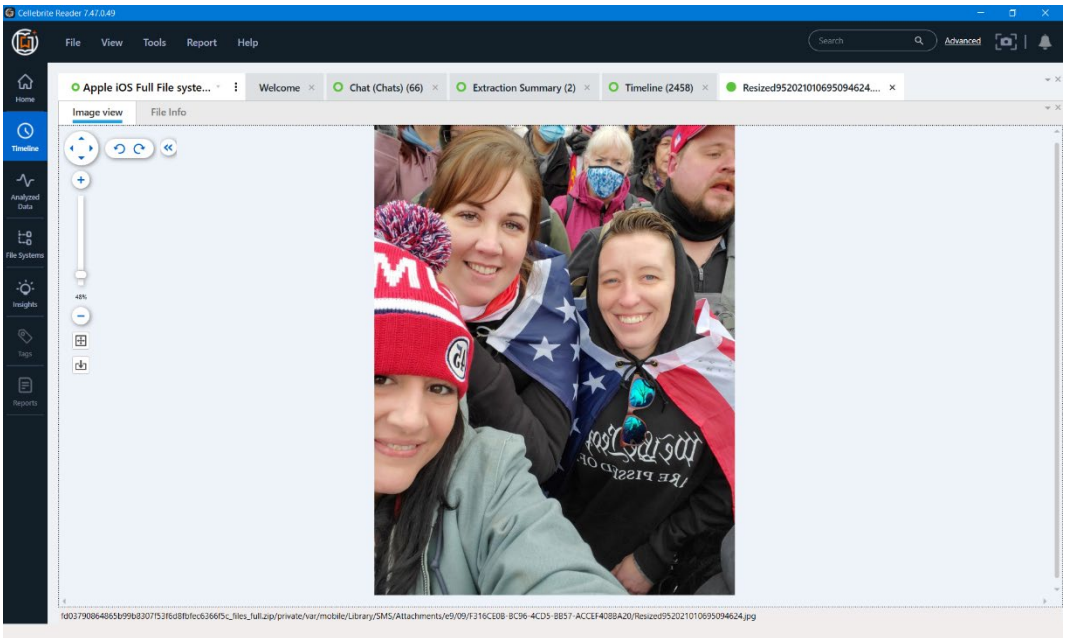

The following photographs were also located in a text chain. It shows Niemela in the left foreground wearing sunglasses and Eckerman in the red hat in the middle:

**Figure 10:**




Also located was a photograph with Chiguer to the right of Niemela, without a hat:

**Figure 2:**



43. A second tip was found on the 'Kirstyn_Niemela_Name_Search' database results document from Witness -2 (W-2) who reported seeing posts and pictures on Facebook posted by Niemela. W-2 stated they were a relative of Niemela, and stated Niemela posted several pictures of herself on her Facebook page in the crowd of people with the Capitol building and other landmarks in the background. Niemela referred to a line she and many others stood in to make it in. W-2 said that since returning home, Niemela was almost always in a Facebook chatroom.

44. W-2 was interviewed by agents of the FBI, on or about November 5, 2021. W-2 stated they saw Niemela's posting on Facebook before Niemela's accounts were taken down. W-2 stated Niemela was posting on Facebook the day of the United States Capitol riot on January 6, 2021 under her real name, from the United States Capitol. W-2 did not see any posting made from inside the United States Capitol but did provide a CNN video they found on the internet which captured Niemela walking around inside the United States Capitol Rotunda on the afternoon of January 6, 2021 W-2 was shown a series of 14 still photographs taken from within the United States Capitol. W-2 positively identified Niemela in several photographs including the two photographs posted on Facebook as seen in **Figures 1 and 2** above in paragraphs #36 and #37.

45. From the still photographs taken from the security cameras within the United States Capitol, W-2 positively identified Niemela in six of the twelve photographs inside the United States Capitol, including **Figures 3 and 5** above in paragraph #37.

46. I know, from my training and experience, that people often take pictures and post to social media platforms, like Facebook, from their cellphones. This occurred as well on January 6, 2021 at the Capitol Buildings as discussed more fully in paragraphs #32-33 above.

47. A telephone number ending in 7169 has been linked to Niemela through tip reporting, CLEAR, Accurint, and open source data. According to records obtained through a

search warrant which was served on Verizon, on January 6, 2021, in and around the time of the incident, the cellphone associated with the telephone number ending in 7169 was identified as having utilized a cell site consistent with providing service to a geographic area that included the interior of the United States Capitol building.

48. According to records obtained through a search warrant which was served on Verizon, on January 6, 2021, in and around the time of the incident, the telephone number ending in 1187 was identified as having utilized a cell site consistent with providing service to a geographic area that included the interior of the United States Capitol building. Research of telephone number ending in 1187 through Accurint, CLEAR, and open source searches revealed the likely user of the phone was Dracut, Massachusetts-based Stefanie Nicole CHIGUER.

49. According to records obtained through a search warrant which was served on Google, mobile device(s) associated with variations of Niemela's name as email addresses were present at the U.S. Capitol on January 6, 2021. Google estimates device location using sources including GPS data and information about nearby Wi-Fi access points and Bluetooth beacons. This location data varies in its accuracy, depending on the source(s) of the data. As a result, Google assigns a "maps display radius" for each location data point. Thus, where Google estimates that its location data is accurate to within 10 meters, Google assigns a "maps display radius" of 10 meters to the location data point. Finally, Google reports that its "maps display radius" reflects the actual location of the covered device approximately 68% of the time

50. On January 14, 2022, Niemela and Chiguer were charged with violations of 18 U.S.C. § 1752(a)(1) - Entering and Remaining in a Restricted Building or Grounds; 18 U.S.C. § 1752(a)(2) - Disorderly and Disruptive Conduct in a Restricted Building or Grounds; 40 U.S.C. §

5104(e)(2)(D) - Disorderly Conduct in a Capitol Building; and 40 U.S.C. § 5104(e)(2)(G) - Parading, Demonstrating, or Picketing in a Capitol Building, in the United States District Court for the of District of Columbia. An accompanying arrest warrant issued.

51. On January 18, 2022, Niemela was arrested on the outstanding charges. The Device was seized from her person during the arrest, incident to that arrest.

52. The Device is currently in storage at the Federal Bureau of Investigation (FBI), 15 Constitution Drive, Bedford, New Hampshire. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the FBI.

## TECHNICAL TERMS

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

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. 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 capabilities. These capabilities include storing

names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital

data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "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. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media

include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

g. Pager: A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.

h. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer 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.

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

54. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, 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.

55. 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 subject premises 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.

**ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

56. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

57. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device 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).

b. Forensic evidence on a 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.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic 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 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 a storage medium.

58. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but

not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

59. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

## CONCLUSION

60. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully Submitted,

/s/ Mark A. Hastbacka
Mark A. Hastbacka
Special Agent
Federal Bureau of Investigation

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone, this 21st day of January 2022.

HONORABLE ANDREA K. JOHNSTONE
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

The property to be searched is a Galaxy Z Flip 3 5G cell phone, Model: SM-F711U, Serial: R5CR80Q3G1B, IEMI: 350345700268274, hereinafter the "Device." The Device is currently located at the Federal Bureau of Investigation (FBI), 15 Constitution Drive, Bedford, New Hampshire. This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

**ATTACHMENT B**

*Property to be seized*

1. All records on the Device described in Attachment A that relate to violations of 18 U.S.C. § 1752(a)(1) - Entering and Remaining in a Restricted Building or Grounds; 18 U.S.C. § 1752(a)(2) - Disorderly and Disruptive Conduct in a Restricted Building or Grounds; 40 U.S.C. § 5104(e)(2)(D) - Disorderly Conduct in a Capitol Building; and 40 U.S.C. § 5104(e)(2)(G) - Parading, Demonstrating, or Picketing in a Capitol Building (the "Target Offenses") that have been committed by Kirstyn Niemela ("the Subject") and other identified and unidentified persons, 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 unlawful entry into the U.S. Capitol, including any property of the U.S. Capitol;

c. Evidence concerning awareness of the official proceeding that was to take place at Congress on January 6, 2021, i.e., the certification process of the 2020 Presidential Election;

d. Evidence concerning efforts to disrupt the official proceeding that was to take place at Congress on January 6, 2021, i.e., the certification process of the 2020 Presidential Election;

e. Evidence relating to a conspiracy to illegally enter and/or occupy the U.S. Capitol Building on or about January 6, 2021;

f. Evidence concerning the breach and unlawful entry of the United States Capitol, and any conspiracy or plan to do so, on January 6, 2021;

g. Evidence concerning the riot and/or civil disorder at the United States Capitol on January 6, 2021;

h. Evidence concerning the assaults of federal officers/agents and efforts to impede such federal officers/agents in the performance of their duties the United States Capitol on January 6, 2021;

i. Evidence concerning damage to, or theft of, property at the United States Capitol on January 6, 2021;

j. Evidence of any conspiracy, planning, or preparation to commit those offenses;

k. Evidence concerning efforts after the fact to conceal evidence of those offenses, or to flee prosecution for the same;

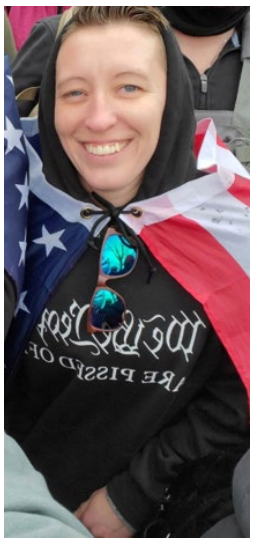
l. Evidence of communication devices, including closed circuit radios or walkie-talkies, that could have been used by co-conspirators to communicate during the unlawful entry into the U.S. Capitol;

m. Evidence of the state of mind of the subject 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

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

a. Depictions of clothing worn by the subject, to include an American flag as a cape, sunglasses, and a black sweatshirt that reads "We the People ARE PISSED OFF" as shown below:

;

c. Depictions of other paraphernalia used by or associated with the Subject, to include signs, flags and other items connected to the Stop the Steal rally or protest of the 2020 presidential election.

3. Records and information that constitute evidence of the Subject's possible affiliation with Q-Anon or other group represented at the Capitol January 6, 2021 riot;

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

   a. Any records and/or evidence revealing the Subject's presence at the January 6, 2021 riot;

   b. Any physical records, such as receipts for travel, which may serve to prove evidence of travel of to or from Washington D.C. from December of 2020 through January of 2021;

   c. The Subject's (and others's) motive and intent for traveling to the U.S. Capitol on or about January 6, 2021;

   d. The Subject's (and others's) activities in and around Washington, D.C., specifically the U.S. Capitol, on or about January 6, 2021;

5. For any digital device, including but not limited to a cellular telephone, which is capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities as described in the search warrant affidavit and above, hereinafter the "Device":

   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 Device(s) or to conduct a forensic examination of the Device;

h. records of or information about Internet Protocol addresses used by the Device;

i. 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.

6. Law enforcement personnel are specifically authorized to obtain from Kirstyn Niemela the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint, facial characteristics, or iris display) necessary to unlock any Device requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned persons' physical biometric characteristics will unlock the Device, to include pressing fingers or thumbs against and/or putting a face before the sensor, or any other security feature requiring biometric recognition of the Device for the purpose of attempting to unlock the Device's security features in order to search the contents as authorized by this warrant.

While attempting to unlock the device by use of the compelled display of biometric characteristics pursuant to this warrant, law enforcement is not authorized to demand that the aforementioned person state or otherwise provide the password or identify the specific biometric characteristics (including the unique finger(s) or other physical features), that may be used to unlock or access the Device. Nor does the warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person(s) to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person(s) is permitted. To avoid confusion on that point, if agents in executing the warrant ask any of the aforementioned person for the password to any Device, or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any Device, the agents will not state or otherwise imply that the warrant requires the person to provide such information and will make clear that providing any such information is voluntary and that the person is free to refuse the request.
As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

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