

FILED

5/25/2023

THOMAS G. BRUTON
CLERK, U.S. DISTRICT COURT

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

In the Matter of the Search of:

Case Number: 23M554

One Samsung Galaxy S20+ 5G cellular telephone bearing International Mobile Equipment Identity ("IMEI") number 3545511102792641, and assigned telephone number 773-910-2491, and Image-1 further described in Attachment A

APPLICATION AND AFFIDAVIT FOR A SEARCH WARRANT

I, John J. Coleman, a Special Agent of the Federal Bureau of Investigation, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property or premises:

See Attachment A

located in the Northern District of Illinois, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is evidence and instrumentalities.

The search is related to a violation of:

Code Section

Title 18, United States Code, Sections 1752(a)(1) and (2); and Title 40 U.S.C. Sections 5104(e)(2)(C)(i), (D), and (G)

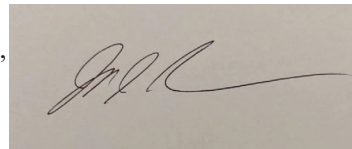
Offense Description

Unlawful entry on restricted building and grounds; and violent entry, disorderly conduct, and other offenses on U.S. Capitol grounds

The application is based on these facts:

See Attached Affidavit,

Continued on the attached sheet.



Applicant's Signature

JOHN J. COLEMAN, Special Agent
Federal Bureau of Investigation

Printed name and title

Pursuant to Fed. R. Crim. P. 4.1, this Application is presented by reliable electronic means. The above-named agent provided a sworn statement attesting to the truth of the statements in the Application and Affidavit by telephone.

Date: May 25, 2023 11:45am



Judge's signature

City and State: Chicago, Illinois

JEFFREY COLE, U.S. Magistrate Judge

Printed name and title

offenses on U.S. Capitol grounds, in violation of 40 U.S.C. §§ 5104(e)(2)(C)(i), (D), and (G) (the “Subject Offenses”).

4. The statements in this affidavit are based on my personal knowledge, and on information I have received from other law enforcement personnel and from persons with knowledge regarding relevant facts. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included every fact known to me concerning this investigation. I have set forth facts that I believe are sufficient to establish probable cause to believe that evidence and instrumentalities of the Subject Offenses are located on the Subject Phone and Image-1.

I. FACTS SUPPORTING PROBABLE CAUSE TO SEARCH

Background – The U.S. Capitol on January 6, 2021¹

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

6. The Capitol 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 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 is the West Front, which includes the inaugural stage scaffolding, a variety of open concrete spaces, a fountain

¹ The facts presented in this section are based on video from the U.S. Capitol Police, accounts from U.S. Capitol Police, and photos and videos taken by news organizations and individuals at the Capitol that day.

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 this area was barricaded and off limits to the public on January 6, 2021.

7. The Capitol is secured twenty-four hours a day by USCP. Restrictions around the Capitol include permanent and temporary security barriers and posts manned by USCP. Only authorized people with appropriate identification are allowed access inside the Capitol.

8. On January 6, 2021, a joint session of the United States Congress was scheduled to convene at the Capitol to certify the vote count of the Electoral College of the 2020 Presidential Election, which took place on Tuesday, November 3, 2020 ("Certification"). The exterior plaza of the U.S. Capitol was closed to members of the public.

9. A crowd began to assemble near the Capitol around 12:30 p.m. Eastern Standard Time ("EST"). At about 12:50 p.m., known and unknown individuals broke through the police lines, toppled the outside barricades protecting the Capitol, and pushed past USCP and supporting law enforcement officers there to protect the Capitol.

10. The joint session began at approximately 1:00 p.m. in the House Chamber.

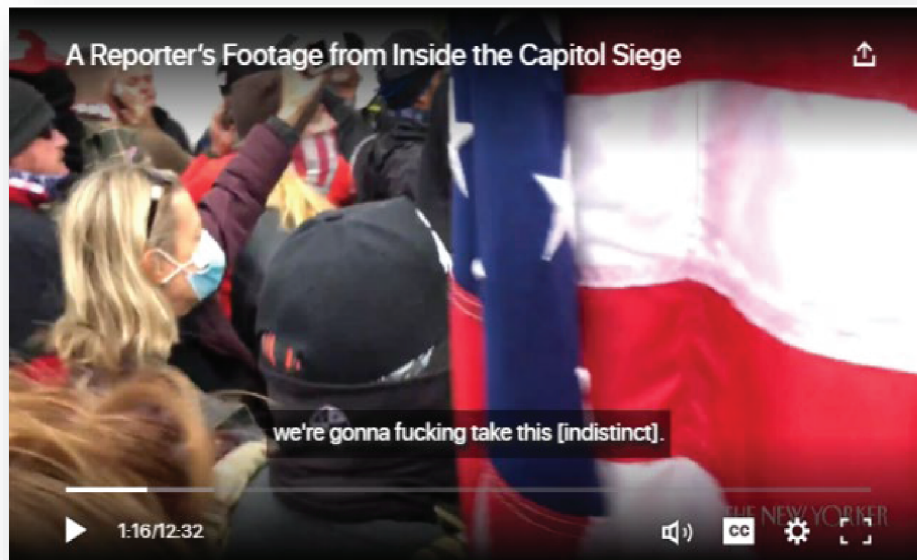
11. At approximately 1:30 p.m., the House and Senate adjourned to separate chambers to resolve a particular objection. Vice President Mike Pence was present and presiding, first in the joint session, and then in the Senate chamber. Around this time, USCP also ordered Congressional staff to evacuate the 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.

12. As the proceedings continued in both the House and the Senate, USCP attempted to keep the crowd away from the Capitol and the proceedings underway inside. 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.

13. At approximately 2:00 p.m., some people in the crowd forced their way through, up, and over additional 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 USCP officers or other authorized security officials. At such time, the Certification proceedings were still underway and the exterior doors and windows of the Capitol were locked or otherwise secured. Members of law enforcement attempted to maintain order and keep the crowd from entering the Capitol.

14. At about 2:10 p.m., individuals in the crowd forced entry into the 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.



15. Shortly thereafter, at approximately 2:20 p.m., members of the House and Senate, including the President of the Senate—Vice President Pence—were instructed to and did evacuate the chambers. 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 rioters 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.

16. At approximately 2:30 p.m., known and unknown subjects broke windows and pushed past USCP and supporting law enforcement officers forcing their way into the 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 federal police officers were injured and several were admitted to the hospital. The subjects also confronted and terrorized members of Congress, Congressional staff, and the media. The subjects carried weapons including tire irons, sledgehammers, bear spray, and tasers. They also took police equipment from

overrun police including shields and police batons. At least one of the subjects carried a handgun with an extended magazine. These actions by the unknown individuals resulted in the disruption and ultimate delay of the Certification.

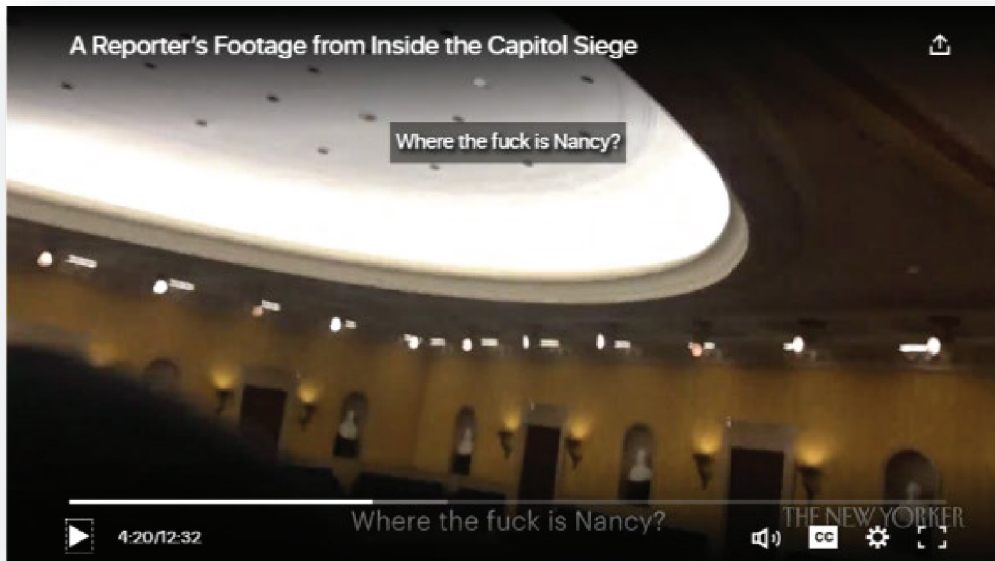
17. At approximately 2:30 p.m., as subjects reached the rear door of the House Chamber, USCP ordered the evacuation of lawmakers, Vice President Pence, and Senator Charles Grassley—president pro tempore of the Senate—for their safety.

18. At around 2:45 p.m., subjects broke into the office of House Speaker Nancy Pelosi. At about the same time, one subject was shot and killed while attempting to break into the House chamber through the broken windows.

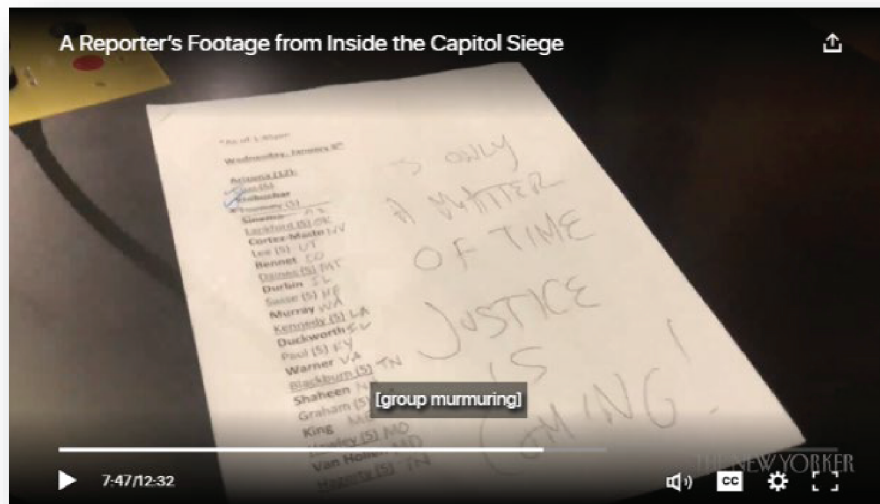
19. At around 2:47 p.m., subjects broke into the United States Senate Chamber. Publicly available video shows an individual asking, “Where are they?” as they opened the door to the Senate Chamber. Based upon the context, law enforcement believes that the word “they” is about members of Congress.



20. 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.



21. A subject left a note on the podium on the floor of the Senate Chamber. This note, captured by the filming reporter, stated “It’s Only A Matter of Time Justice is Coming.”



22. During the time when the subjects were inside the Capitol, multiple subjects were observed inside the 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 many individuals were expected to be taken into custody.



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

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

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

26. Based on these events, all proceedings of 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 Capitol, including the danger posed by individuals who had entered the Capitol without any security screening or weapons check, Congressional proceedings could not resume until after every unauthorized occupant had left the Capitol, and the building had been confirmed secured. The proceedings resumed at approximately 8:00 p.m. after the building had been secured. Vice President Pence remained in the United States Capitol from the time he was evacuated from the Senate Chamber until the session resumed.

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

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

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

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

31. 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 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.

32. Many subjects seen on news footage around the Capitol are using a cell phone in some capacity. It appears some subjects were recording the events occurring in and around the Capitol and others appear to be taking photos, to include photos and video of themselves after breaking into the Capitol, including photos or videos of themselves damaging or stealing property. As reported in the news media, others inside and immediately outside the Capitol live-streamed their activities, including those described above as well as statements about these activities.

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





Facts Specific to This Application

A. Images and Other Evidence of KAROL CHWIESIUK at the U.S. Capitol on January 6, 2021

34. Since January 6, 2021, the FBI has been investigating and identifying those who were inside of the Capitol without authority and disrupted the proceedings. During that investigation, and pursuant to a federal search warrant, the FBI learned that a mobile device associated with the Google account kchwiesiuk24@gmail.com (the “CHWIESIUK Google Account”) was present near or inside of the geographic boundaries of the U.S. Capitol between approximately 2:37 p.m. and 3:24 p.m. EST on January 6, 2021. The CHWIESIUK Google Account is associated with the name kchwiesiuk and a recovery telephone number of +1-773-910-2491 (which is the number of the Subject Phone). Legal process to the service provider of the Subject Phone identified the name of the individual to whom that telephone number is registered KAROL J. CHWIESIUK, with the address 5425 North Oconto Avenue, Chicago, IL 60656 (the “Premises”). Legal process further identified that the device associated with the Subject Phone’s number and the CHWIESIUK Google Account has an IMEI of 3545511102792641 and is a Samsung Galaxy S20+ 5G.

35. A search of publicly available resources identified CHWIESIUK as potentially an employee of the Chicago Police Department (“CPD”).² The FBI confirmed with CPD that the defendant is currently employed as a Police Officer with the CPD—badge # 7156. CPD employment records show that the defendant listed the Subject Phone number as his home phone number.

² See <https://rateourcops.org/officer/9288>; <https://staging.openoversight.com/officer/31327>; <https://data.cityofchicago.org/api/views/t572-8ikd/rows.pdf?accessType=DOWNLOAD>

36. Through a federal search warrant, your affiant obtained and reviewed geolocation and communication records associated with the CHWIESIUK Google Account. Notably, on Tuesday, January 5, 2021, at approximately 10:46 p.m., the defendant received an email from an account that identified itself as Ali Alexander, Stop The Steal <Ali@stopthesteal.us>. The subject line of the email is: **Tomorrow is going to be a historic day in Washington DC**. The text of the email is as follows:

Patriots,

Tomorrow is going to be a historic day in Washington DC. There are going to be millions of likeminded patriots attending the Stop The Steal events that we have scheduled.

Please pay close attention to the following event details:

Venue Address #1

*The Ellipse w/ **Your President Donald J Trump***

Constitution Ave NW between 15th St NW & 17th St NW

Washington, DC 20230

Doors open at 7:00 AM EST. The event will begin at 9:00 AM EST.

Parking

There is no designated parking are for this event. Arriving on foot or via ride share is strongly encouraged. There are many local lots in downtown D.C. Please see below for road closure information.

Guest Arrival Information

*Gates open at **7:00 AM EST**. The event will begin at **9:00 AM EST**.*

First Come First Serve

***** Expect heavy traffic delays and plan to arrive early *****

Please enter Constitution Ave NW by foot from the National Mall (south of Constitution Ave NW).

Venue Address #2

US Capitol

Capitol Hill North East by Constitution Avenue Northeast

Washington, DC 20230

Begins at 1:00 PM

Our presence outside of the US Capitol building will let Members of Congress know that we stand with Rep. Mo Brooks and his colleagues in the House of Representatives who will bravely object to the certification of the Electoral College. This will be one of the most historic events of our lifetime.

*I look forward to making history with you,
Ali Alexander – Founder of Stop The Steal*

37. The CHWIESIUK Google Account's geolocation data show that the defendant left Chicago, Illinois, on January 4, 2021, and arrived in Washington, D.C., on January 5, 2021. The defendant departed Washington, D.C., on January 7, 2021, and returned to Chicago on January 8, 2021.

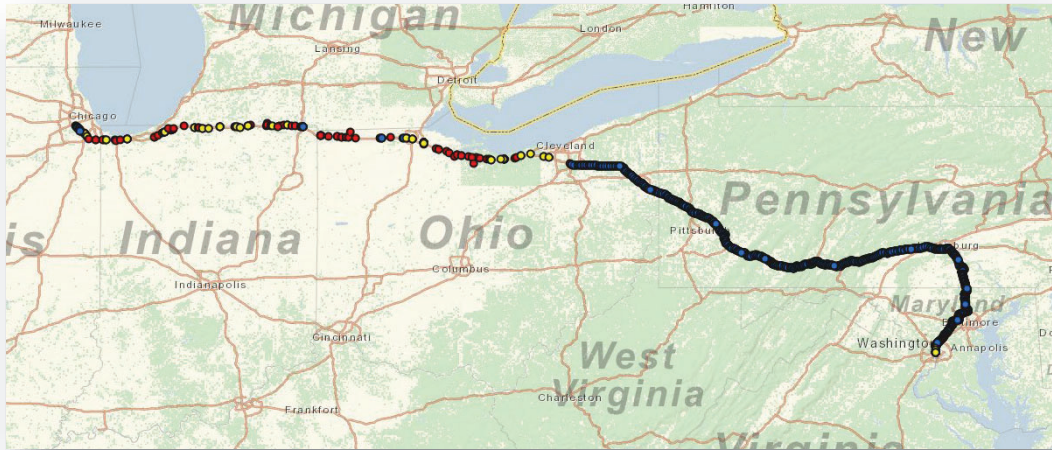


IMAGE 1: A screenshot of the defendant's geolocation data showing him traveling from Chicago, IL, to Washington, D.C.

38. Once the defendant arrived in Washington, D.C., the defendant’s geolocation data show that he spent a significant amount of time in and around a location that your affiant has identified as The Mayflower Hotel (based on open source internet searches). According to records from the hotel, The Mayflower Hotel had a reservation under the name of an individual who has been identified as the defendant’s sister, AGNIESZKA CHWIESIUK, from January 5th through 7th, 2021.

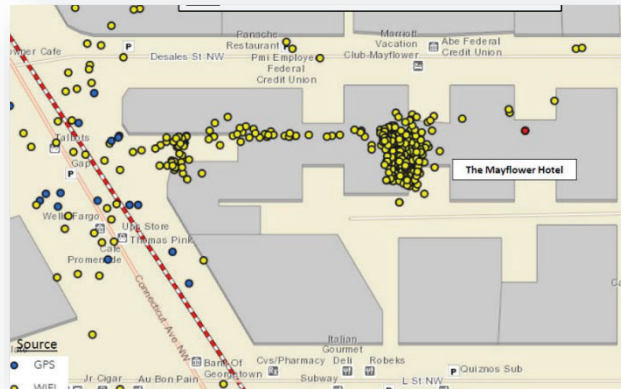


IMAGE 2: A screenshot of the defendant’s geolocation data on a map of Washington, D.C., with a cluster of location data points at The Mayflower Hotel during a period that covers January 5-7, 2021.

39. A further review of the defendant’s geolocation data during the period of January 5, 2021, shows that the defendant traveled from The Mayflower Hotel to the Capitol and back, as depicted below.

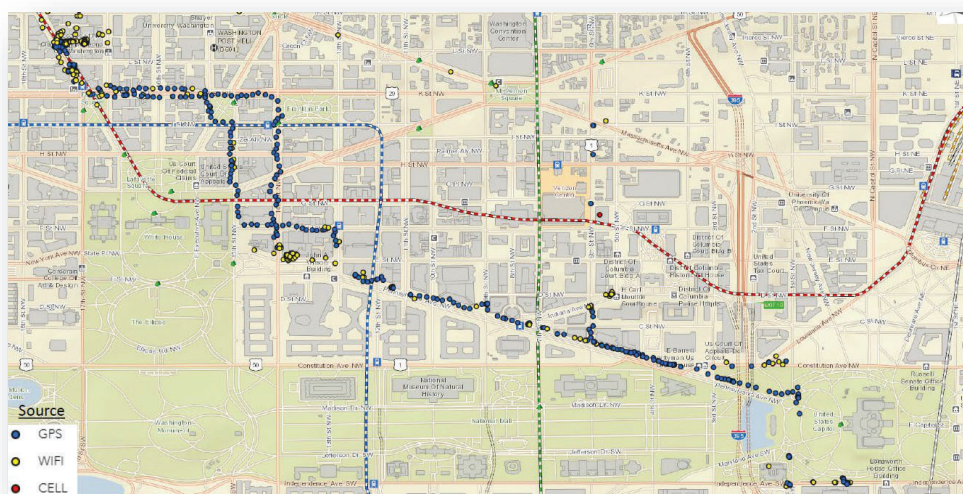
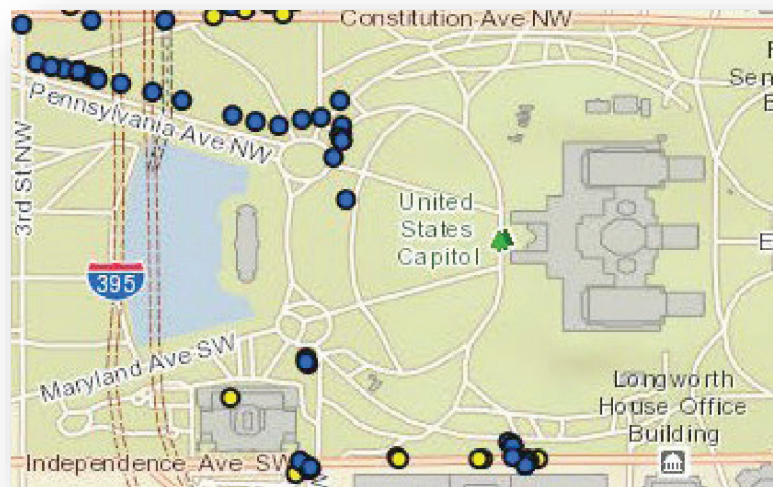
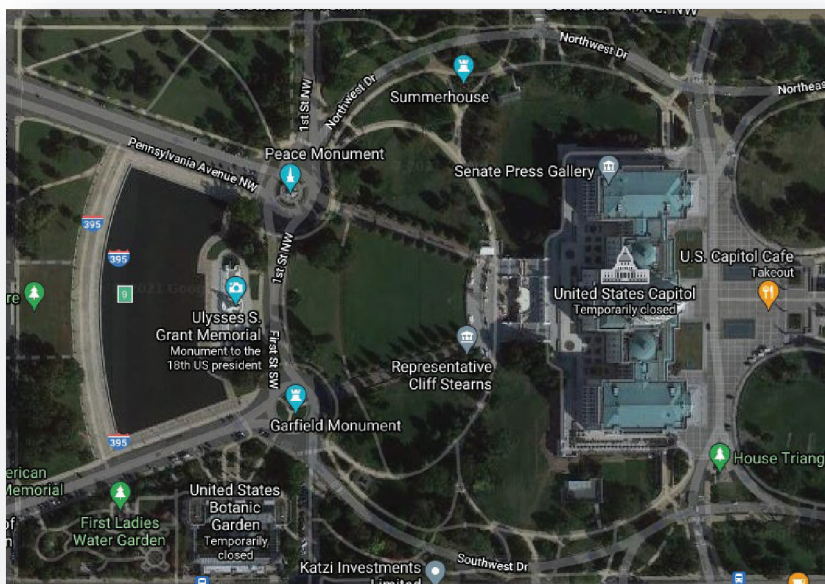


IMAGE 3: A screenshot of the defendant’s geolocation data on a map of Washington, D.C., during a period that covers January 5, 2021.

40. As can be seen in Image 3 above, the defendant traveled to the vicinity of the Capitol the night before the attack on the Capitol. According to the geolocation data, the defendant arrived in the vicinity of a location known as the Peace Monument at approximately 9:06 p.m. As stated above, the defendant would not have been able to get any closer to the Capitol at that time because of the USCP security barricades that were already in place. Accordingly, the geolocation data, depicted in greater detail below, show the defendant traveling south along the barricade line and past the Garfield Monument to Independence Ave SW. According to the geolocation data, the defendant then traveled east to an area in the vicinity of the Longworth House Office Building, arriving there at approximately 9:27 p.m. The defendant then appears to have backtracked and returned to The Mayflower Hotel.





IMAGES 4, 5: (top) A screenshot of the defendant's geolocation data in the vicinity of the Capitol, during the period of January 5, 2021, from approximately 9:00 p.m. to approximately 9:45 p.m.; (bottom) a screenshot of a satellite-view map of approximately the same area.

41. During the investigation, the FBI reviewed the toll records associated with the Subject Phone number. During the time period from January 5, 2021, at approximately 9:11 p.m. to approximately 9:39 p.m., while the defendant was in the vicinity of the Capitol, the defendant sent approximately 44 picture messages to three individuals whose identities are known to the FBI.

42. On January 6, 2021, the defendant's geolocation data from the federal search warrant to Google discussed above show that he was in the vicinity or inside of the Capitol between

the approximate times of 2:37 p.m. and 3:24 p.m.

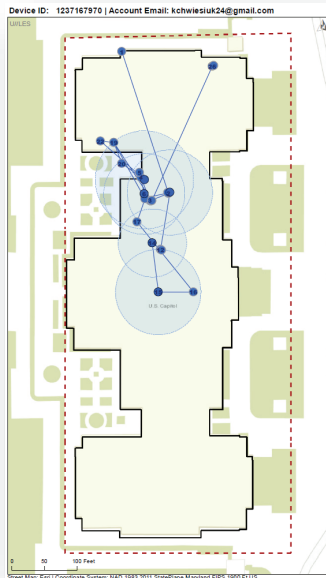
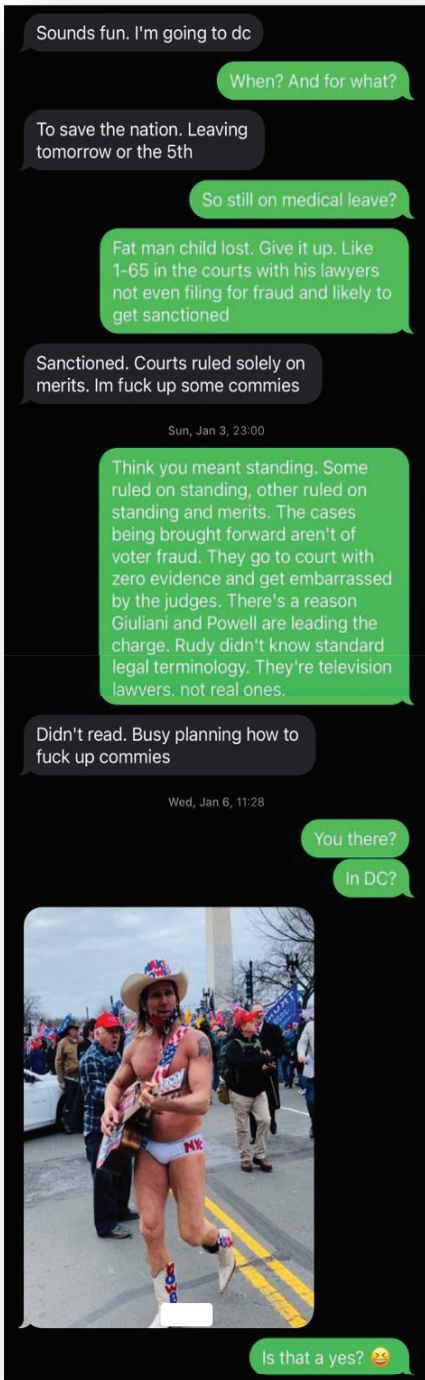


IMAGE 6: A screenshot of the defendant's geolocation data between approximately 2:37 PM and 3:24 PM showing him in the vicinity or inside of the Capitol.

43. The toll records further indicate that while the Subject Phone was inside of the Capitol, approximately 73 SMS/MMS messages were sent to or received from multiple contacts. During that time frame, approximately 36 messages containing an image were sent from the Subject Phone number. Seven messages were exchanged with one number in particular.

44. The FBI identified and spoke with the subscriber (whose identity is known to the FBI) associated with that particular number ("Individual A"). When interviewed by the FBI, Individual A indicated that he/she has known the defendant for more than 10 years and has maintained regular communication with the defendant. Individual A further stated that he/she received text messages and pictures from the defendant on and around January 6, 2021. Individual A voluntarily provided copies of these messages to the FBI.

45. The FBI's review of the text messages exchanged between Individual A (referred to as "Subscriber" in the text message exchanges below) and the defendant shows the following:



Sunday, January 3, 2021, at unknown Time

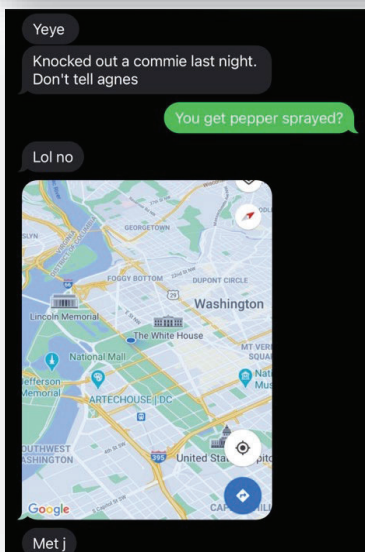
CHWIESIUK: Sounds fun. I'm going to dc
SUBSCRIBER: When? And for what?
CHWIESIUK: To save the nation. Leaving tomorrow or the 5th
SUBSCRIBER: So still on medical leave? Fat man child lost. Give it up. Like 1-65 in the courts with his lawyers not even filing for fraud and likely to get sanctioned.
CHWIESIUK: Sanctioned. Courts ruled solely on merits. Im fuck up some commies

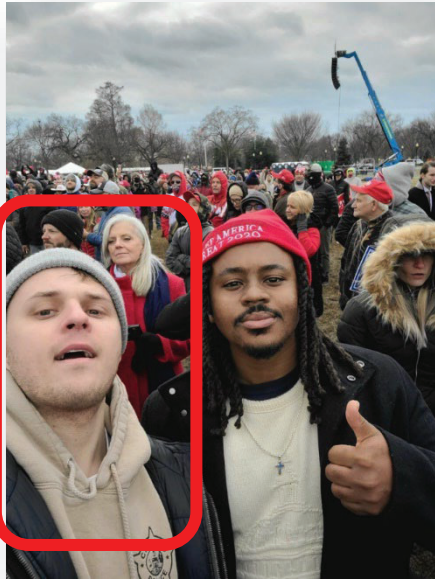
Sunday, January 3, 2021, at 11:00 p.m.

SUBSCRIBER: Think you meant standing. Some ruled on standing, other ruled on standing and merits. The cases being brought forward aren't of voter fraud. The go to court with zero evidence and get embarrassed by the judges. There's a reason Giuliani and Powell are leading the charge. Rudy didn't know standard legal terminology. They're television lawyers, not real ones.
CHWIESIUK: Didn't read. Busy planning how to fuck up commies

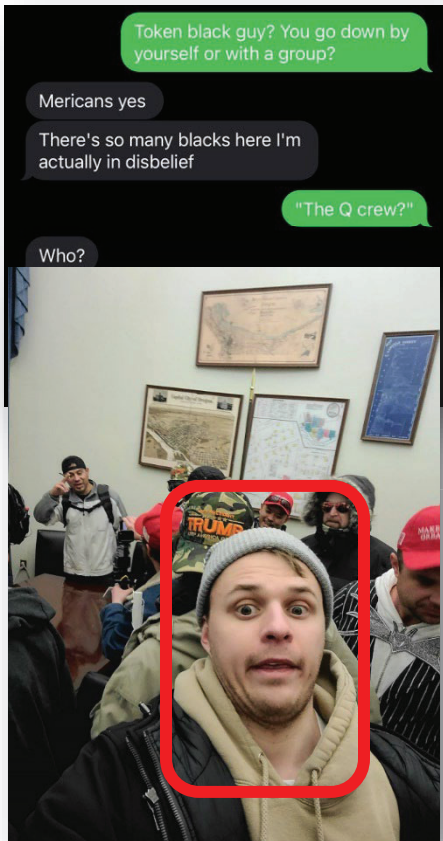
Wednesday, January 6, 2021 @ 11:28 a.m.

SUBSCRIBER: You there? In DC?
CHWIESIUK: [picture of street performer in the vicinity of the Washington Monument]
SUBSCRIBER: Is that a yes?
CHWIESIUK: Yeye. Knocked out a commie last night. Don't tell [redacted]
SUBSCRIBER: You get pepper sprayed?
CHWIESIUK: Lol no
CHWIESIUK: [image of a blue location circle on a map of Washington, D.C., in front of The White House]
CHWIESIUK: Met j
CHWIESIUK: [IMAGE 7 (below)]





IMAGES 7, 8, 9: (left to right, top to bottom) Photograph sent from the defendant to the subscriber showing the defendant (circled in red) wearing a beige hooded sweatshirt with a CHICAGO POLICE emblem, a black zip-up jacket, and a grey beanie; a close-up of the CHICAGO POLICE emblem from IMAGE 7; and an open source image of what appears to be the CHICAGO POLICE emblem on the defendant's hooded sweatshirt.



SUBSCRIBER: Token black guy? You go down by yourself or with a group?

CHWIESIUK: Mericans yes. There's so many blacks here I'm actually in disbelief

SUBSCRIBER: "The Q crew?"

CHWIESIUK: Who?

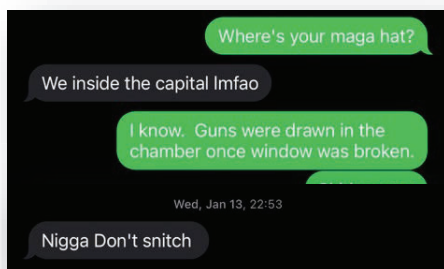
SUBSCRIBER: People down there lol

Wednesday, January 6, 2021, at 2:58 p.m.

SUBSCRIBER: Wonder if I'll see you on tv

CHWIESIUK: [IMAGE 9 (below)]

IMAGE 10 (left): Photograph sent from the defendant to the subscriber showing the defendant (circled in red) wearing a beige hooded sweatshirt, a black zip-up jacket, and a grey beanie.



SUBSCRIBER: Where's your maga hat?
CHWIESIUK: We inside the capital [sic] Imfao
SUBSCRIBER: I know. Guns were drawn in the chamber once window was broken. Shithousery.
CHWIESIUK: Yeah I was there

Wednesday, January 13, 2021, at 10:53 p.m.

CHWIESIUK: Nigga Don't snitch

46. During his interview with the FBI, Individual A stated in sum and substance that the individual wearing the beige hoodie in IMAGE 7 and IMAGE 10 is the defendant—KAROL CHWIESIUK.

47. Regarding IMAGE 10 (above), the FBI believes that the defendant took the selfie when he was inside a room of the Capitol, specifically room S140. Your affiant knows Room S140 to be an office of Senator Jeff Merkley (D-OR). Sen. Merkley tweeted a video of the destruction to his office on January 6, 2021.³ At approximately 2:36 of that video, the following screenshot appears:

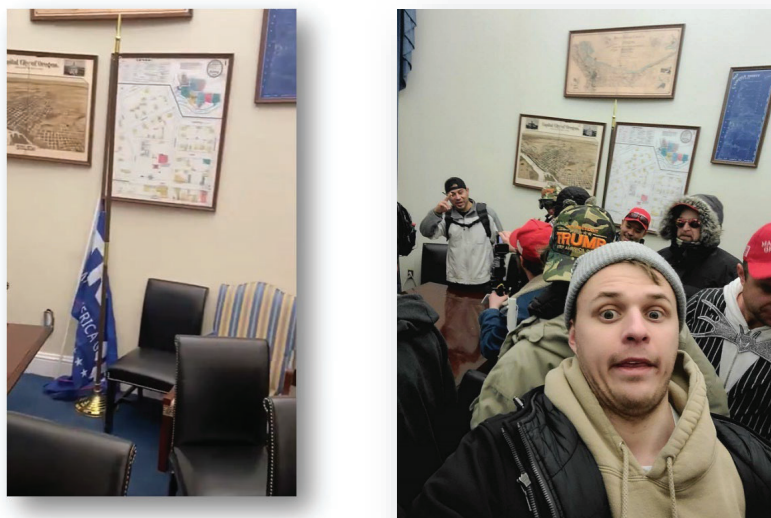


IMAGE 11: (left) A screenshot from approximately 2:36 of a video filmed by Sen. Merkley of the destruction caused to his office (S140) as compared to IMAGE 10 (right), the selfie photograph of the defendant. The flagpole and wall hangings appear to be identical.

³ <https://twitter.com/SenJeffMerkley/status/1347039504528498688>

48. Further, The New Yorker photographer Balazs Gardi took a photo inside of Sen. Merkley's office during the riot that was published as part of Luke Mogelson's article *Among the Insurrectionists*.⁴ Although the defendant cannot be seen in Gardi's photo, the defendant's selfie appears to have been taken at approximately the same time.



IMAGE 12: (left) A photograph taken by Balazs Gardi published in The New Yorker magazine in a location identified as Sen. Merkley's office (S140) as compared to IMAGE 10 (right), the selfie photograph of the defendant. The flagpole and wall hangings appear to be identical, and many of the individuals in the photos appear to be in the same or similar locations.

49. The FBI reviewed additional open-source videos, including a livestreamed video recorded and simulcast by the separately charged defendant Anthime Joseph Gionet (AKA Tim, AKA Baked Alaska).⁵ An individual that appears to be the defendant is seen at approximately 7:27 just inside the Senate Wing doors in the DLive broadcast.

⁴ <https://www.newyorker.com/magazine/2021/01/25/among-the-insurrectionists>

⁵ *United States v. Gionet*, No. 21-MJ-14 (District Court for District of Columbia).

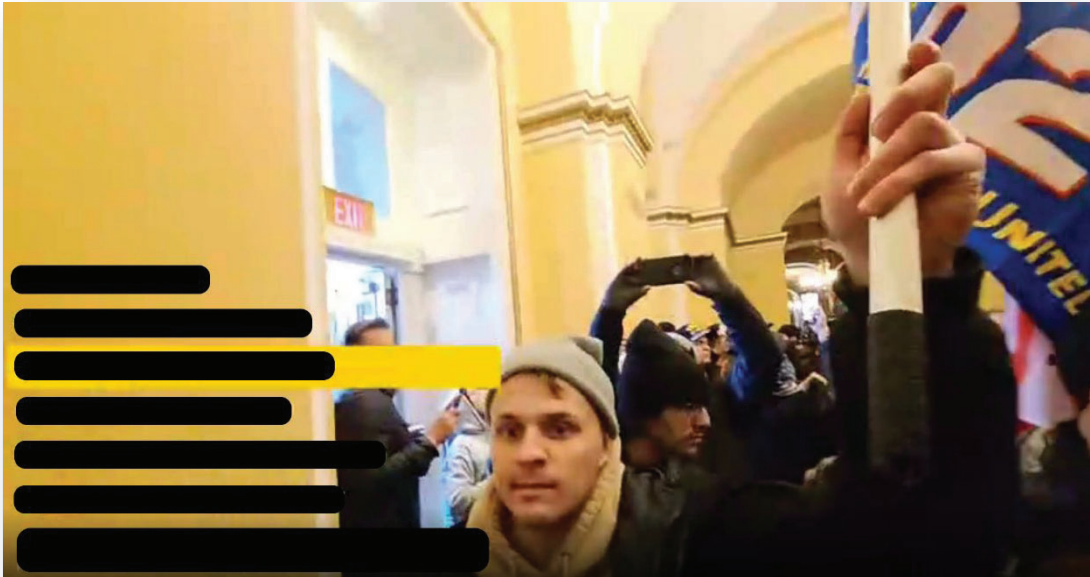


IMAGE 13: A screenshot from separately charged defendant Gionet's livestream (at approx. 7:27) showing the defendant wearing a beige hoodie and grey beanie holding a Trump flag just inside the Senate Wing doors.

50. By reviewing CCTV from the Capitol, your affiant was able to identify and isolate a screenshot that shows approximately the same moment as IMAGE 13 from a different angle.

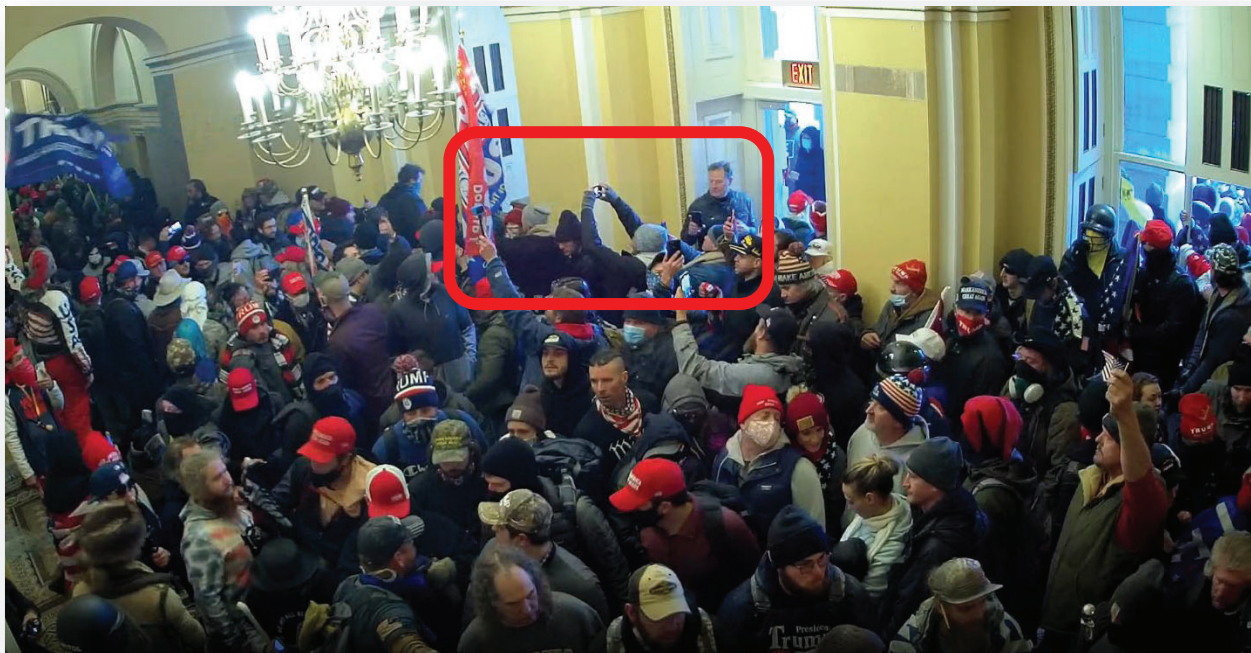


IMAGE 14: A screenshot from the Capitol's CCTV showing a different angle of the defendant (circled in red), his flag, and those around him at approximately the same time as IMAGE 13.

51. Additional CCTV video shows the defendant at various locations throughout the Capitol, including taking a selfie in the vicinity of the Senate Wing doors, walking through a location known as the Capitol Crypt, and leaving through a window near the Senate Wing doors.

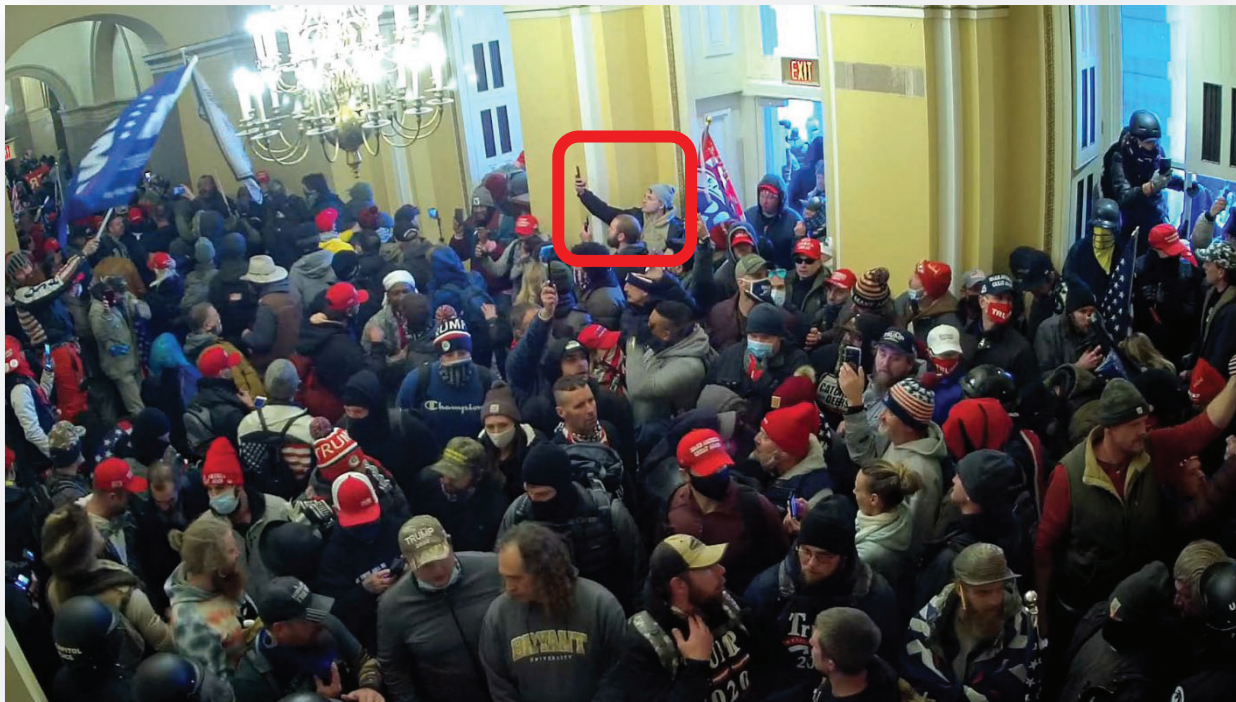


IMAGE 15: A screenshot from the Capitol's CCTV showing the defendant (circled in red), taking a selfie in front of the Senate Wing doors.



IMAGE 16: A screenshot from the Capitol's CCTV showing the defendant (circled in red), inside the Capitol Crypt wearing a beige hoodie, a grey beanie, and holding the same flag as previously shown.

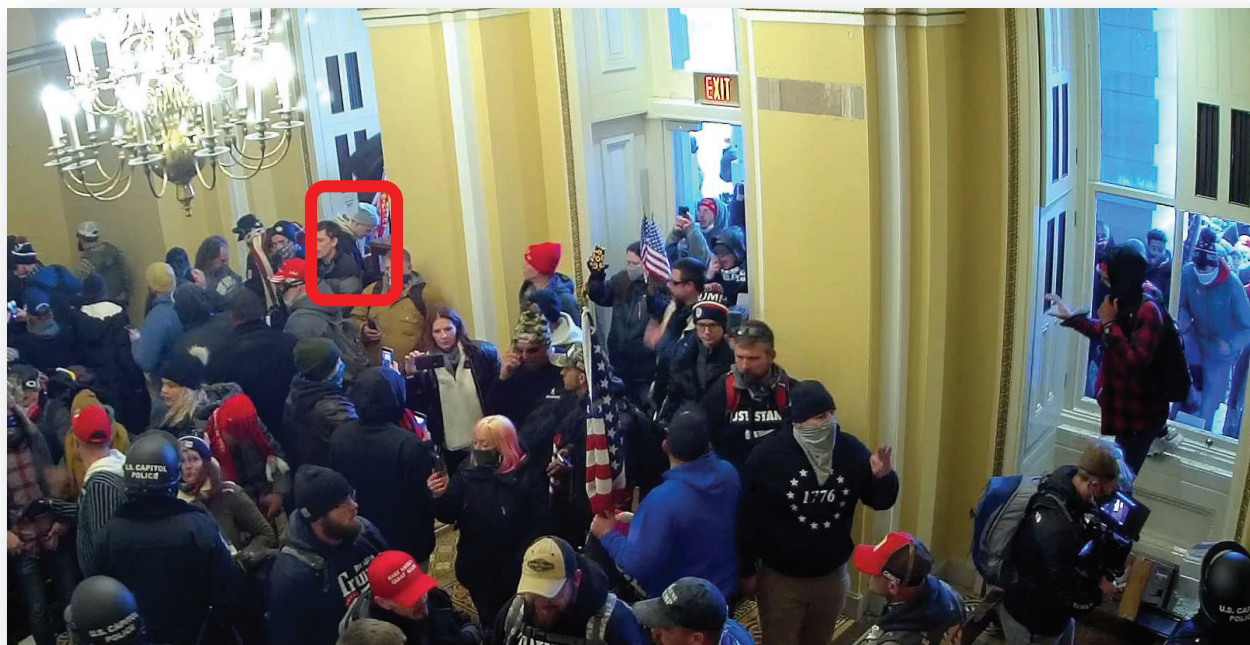


IMAGE 17: A screenshot from the Capitol's CCTV showing the defendant (circled in red), leaving the Capitol through a window in the vicinity of the Senate Wing doors wearing a beige hoodie, a grey beanie, and holding the same flag as previously shown.

52. In summary, on January 3, 2021, the defendant indicated that he was going to travel to Washington, D.C., “to save the nation,” and that he was going to leave on January 4 or 5, 2021. In response, Individual A told the defendant to “give it up,” and that the “man child lost.”⁶ In response, the defendant minimized the courts’ decisions against then-President Trump by stating that the courts ruled solely on merits (the defendant likely meant to say standing). After a lengthy response by Individual A, the defendant responded that he had not read either Individual A’s text or the court decisions—precisely which one is unclear—because he was “[b]usy planning how to

⁶ Taken in context of the current events of that period, specifically then-President Trump’s various unsuccessful legal challenges to the results of the 2020 presidential election, your affiant believes this exchange between the defendant and the subscriber shows that the defendant supports the belief that then-President Trump won the election and is willing to take action to help Trump achieve the victory in an election that Trump did not win.

fuck up commies.”

53. The defendant followed through on his stated intent to travel to Washington, D.C., by traveling from Chicago, Illinois, to Washington, D.C. Based on geolocation data, the defendant left Chicago on January 4, 2021, at approximately 8:30 p.m. and arrived in Washington, D.C., on January 5, 2021, at approximately 7:50 a.m.

54. On the evening of January 5, 2021, the defendant walked to the Capitol and surveyed the barricades that were already set out and in place. While in the vicinity of the Capitol, the defendant sent 44 images to three individuals. The next day, the defendant went to the White House at approximately the same time that then-President Trump was giving a speech, and texted Individual A that he “met j,” a likely reference to then-President Donald J. Trump.

55. On January 6, 2021, the defendant then walked approximately the same route as the evening before, but this time he walked past the barricades that he had seen the previous evening. Together with a large group—many of whom were climbing through broken windows as seen in IMAGE 14 and many of whom were screaming and chanting—the defendant entered the Capitol.

56. Once inside, the defendant proceeded to S140, Senator Merkley’s office where at least two individuals are seen smoking what appear to be cigars at approximately the same time that the defendant is in S140. While inside S140, the defendant stopped to take a picture and brag to Individual A that he was “inside the capital [sic] lmfao.”

57. After leaving S140, the defendant walked through the Capitol Crypt, then returned to the Senate Wing door, and appears to have left through a broken-out window.

B. The Complaint and the Information

58. On June 10, 2021, based on a complaint that I submitted in support of an arrest warrant for the defendant (the “Complaint”), the Honorable Robin Meriweather, United States

Magistrate Judge for the District of Columbia, found probable cause that the defendant violated the Subject Offenses and issued a warrant for his arrest. On February 14, 2023, the United States Attorney for the District of Columbia filed a superseding information charging the defendant and his sister, Agnieszca Chwiesiuk, with the Subject Offenses,⁷ in *United States v. Karul Chwiesiuk and Agnieszca Chwiesiuk*, case no. 21-CR-536, District of Columbia. The case remains pending, and trial is scheduled to begin on August 7, 2023.

C. Seizure and Search of the Subject Phone

59. On June 10, 2021, based on an application that I submitted in support of a search warrant, the Honorable Gabriel Fuentes, United States Magistrate Judge for the Northern District of Illinois, found probable cause to believe that evidence of the Subject Offenses would be found in the defendant's Premises and in the Subject Phone, case numbers 21-m-361 and 21-m-362.

60. On June 11, 2021, agents arrested the defendant on the outstanding warrant. Agents searched the Premises following the arrest. During the search, the defendant stated that the Subject Phone was inside of a vehicle. The defendant opened the vehicle and consented to the retrieval of the Subject Phone from the vehicle.

61. Pursuant to the warrant issued on June 10, 2021, the FBI made a forensic image of the Subject Phone—that is, Image-1. I went on to identify and document the subset of the information on Image-1 that the FBI had authority to seize under the warrant. I then prepared a “scoped” version of the extraction report for Image-1. The “scoped” version was intended to identify materials in Image-1 that were responsive to the warrant issued on June 10, 2021.

⁷ Agnieszca Chwiesiuk is charged with 18 U.S.C. §§ 1752(a)(1) and (2), and violent entry, disorderly conduct, and other offenses on U.S. Capitol grounds, in violation of 40 U.S.C. §§ 5104(e)(2)(D), and (G). She is not charged with 40 U.S.C. § 5104(e)(2)(C)(i).

62. In reviewing Image-1, I found numerous items relating to the defendant and Agnieszca Chwiesiuk's participation in the January 6, 2021 riot, including video the defendant took of himself inside the Capitol and images of his sister, Agnieszca Chwiesiuk, inside the Capitol. I also found text messages where the defendant admitted to entering the Capitol.

63. In May of 2023, I reviewed the materials from the "scoped" version of the extraction report for Image-1. During that review, I realized that certain conversations that were responsive to the June 10, 2021 warrant were inadvertently omitted from the "scoped" version. For example, I recall seeing the exchange between the defendant and Individual A identified above when reviewing Image-1, but that conversation is not in the "scoped" version.

64. I therefore submit that there is probable cause to believe that the Subject Phone and Image-1 contain additional materials that are responsive to the June 10, 2021 warrant, that is, evidence or instrumentalities related to the Subject Offenses and that information described in Attachments B1 and B2 remains stored in the Subject Phone and Image-1.

65. Device-1 and storage devices containing Image-1 are currently in the lawful possession of the FBI Chicago Field Office.

II. TECHNICAL TERMS

66. 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, certain wireless telephones, 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. “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.

d. “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.

III. COMPUTERS, ELECTRONIC/MAGNETIC STORAGE, AND FORENSIC ANALYSIS

67. As described above and in Attachments B1-B2, this application seeks permission to search for evidence, instrumentalities, and information that might be found within the Subject Phone and Image-1, 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 Attachments B1-B2 will be stored in the Subject Device and Image-1. Indeed, my initial review of the Subject Review and Image-1 revealed records pertaining to the defendant’s participation in the riot at the U.S. Capitol on January 6, 2021. In addition:

a. Individuals who engage in criminal activity, including the crimes associated with the January 6, 2021, riots, access websites to facilitate illegal activity and to communicate with co-conspirators online; to store on digital devices, like the Subject Phone, documents and records relating to their illegal activity, which can include 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; and records of illegal transactions using stolen financial and personal identification data, to, among other things, (1) keep track of co-conspirator's contact information; (2) keep a record of illegal transactions for future reference; (3) keep an accounting of illegal proceeds for purposes of, among other things, splitting those proceeds with co-conspirators; and (4) store stolen data for future exploitation.

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.

68. As further described in Attachments B1-B2, 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 Subject Phone was used, the purpose of its use, who used them (or did not), and when. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit there is probable cause to believe that this forensic electronic evidence and information will be in Image-1 because:

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

b. Forensic evidence on a digital device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, chats, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time, and potentially who did not.

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

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

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

IV. METHODS TO BE USED TO SEARCH DIGITAL DEVICES

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

- a. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of

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

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

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

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

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

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

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

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

70. In searching for information, records, or evidence, further described in Attachments B1-B2, law enforcement personnel executing this search warrant will employ the following procedures:

a. The Subject Phone and Image-1, 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 Attachments B1-B2.

b. 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.

c. 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 Attachments B1-B2. 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 Attachments B1-B2. Any search techniques or protocols used in searching the contents of the Device will be specifically chosen to identify the specific items to be seized under this warrant.

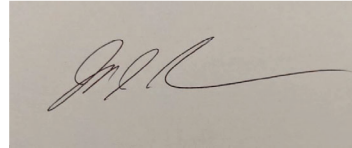
V. AUTHORIZATION TO SEARCH AT ANY TIME OF THE DAY OR NIGHT

71. Because the Subject Phone and Image-1 are in the custody of the FBI, and given that forensic examiners will be conducting their search of that data 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.

VI. CONCLUSION


72. Based on the above information, I submit that this affidavit supports probable cause for a warrant to search the property described in Attachments A1-A2 and to seize the items described in Attachments B1-B2, respectively.

FURTHER AFFIANT SAYETH NOT.



John J. Coleman
Special Agent
Federal Bureau of Investigation

Sworn to and affirmed by telephone 25th day of May, 2023



Honorable JEFFREY COLE
United States Magistrate Judge

ATTACHMENT A1

Property to be searched

The property to be searched is a Samsung Galaxy S20+ 5G cellular telephone bearing International Mobile Equipment Identity (“IMEI”) number 3545511102792641 and assigned telephone number 773-910-2491 (the “Subject Phone”).

The Subject Phone is currently located at the Federal Bureau of Investigation’s Chicago Field Office, 2111 Roosevelt Road, Chicago, Illinois.

ATTACHMENT A2

Property to be searched

The property to be searched is a forensic image of the Samsung Galaxy S20+ 5G cellular telephone bearing International Mobile Equipment Identity (“IMEI”) number 3545511102792641 and assigned telephone number 773-910-2491, assigned lab number 23-CGRCFL-0330 (“Image-1”).

A storage device containing Image-1 is currently located at the Federal Bureau of Investigation’s RCFL, 610 S. Canal St., Chicago, Illinois.

ATTACHMENT B1

LIST OF ITEMS TO BE SEIZED

All records in the Subject Phone described in Attachment A1 that relate to violations of 18 U.S.C. §§ 1752(a)(1) and (2), and violent entry, disorderly conduct, and other offenses on U.S. Capitol grounds, in violation of 40 U.S.C. §§ 5104(e)(2)(C)(i), (D), and (G) (the “Subject Offenses”) that involve KAROL CHWIESIUK, AGNIESZCA CHWIESIUK, and other unidentified persons, including:

- 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 the Subject Offenses;

- k. Evidence concerning efforts after the fact to conceal evidence of the Subject Offenses, or to flee prosecution for the same;
 - l. Evidence concerning materials, devices, or tools that were used to unlawfully enter or attempt to enter the U.S. Capitol by deceit or by force, including weapons and elements used to breach or attempt to breach the building or to counter efforts by law-enforcement, such as pepper spray or smoke grenades;
 - m. Evidence of communication devices, including cellphones, closed circuit radios, or walkie-talkies, that could have been used by the Karol and Agnieszca Chwiesiuk's and/or co-conspirators to communicate during the unlawful entry into the U.S. Capitol;
 - 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.
 - o. Any records and/or evidence revealing the Karol and Agnieszca Chwiesiuk's presence at the January 6, 2021 riot;
 - p. Any 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;
 - q. Karol and Agnieszca Chwiesiuk's (and others') motive and intent for traveling to the U.S. Capitol on or about January 6, 2021; and
 - r. Karol and Agnieszca Chwiesiuk's (and others') activities in and around Washington, D.C., specifically the U.S. Capitol, on or about January 5 and 6, 2021.
2. Evidence of who used, owned, or controlled the Subject Phone 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.

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.

3. 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.

ATTACHMENT B2

LIST OF ITEMS TO BE SEIZED

All records in Image-1 described in Attachment A2 that relate to violations of 18 U.S.C. §§ 1752(a)(1) and (2), and violent entry, disorderly conduct, and other offenses on U.S. Capitol grounds, in violation of 40 U.S.C. §§ 5104(e)(2)(C)(i), (D), and (G) (the “Subject Offenses”) that involve KAROL CHWIESIUK, AGNIESZCA CHWIESIUK, and other unidentified persons, including:

- 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 the Subject Offenses;

- k. Evidence concerning efforts after the fact to conceal evidence of the Subject Offenses, or to flee prosecution for the same;
 - l. Evidence concerning materials, devices, or tools that were used to unlawfully enter or attempt to enter the U.S. Capitol by deceit or by force, including weapons and elements used to breach or attempt to breach the building or to counter efforts by law-enforcement, such as pepper spray or smoke grenades;
 - m. Evidence of communication devices, including cellphones, closed circuit radios, or walkie-talkies, that could have been used by the Karol and Agnieszca Chwiesiuk's and/or co-conspirators to communicate during the unlawful entry into the U.S. Capitol;
 - 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.
 - o. Any records and/or evidence revealing the Karol and Agnieszca Chwiesiuk's presence at the January 6, 2021 riot;
 - p. Any 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;
 - q. Karol and Agnieszca Chwiesiuk's (and others') motive and intent for traveling to the U.S. Capitol on or about January 6, 2021; and
 - r. Karol and Agnieszca Chwiesiuk's (and others') activities in and around Washington, D.C., specifically the U.S. Capitol, on or about January 5 and 6, 2021.
4. Evidence of who used, owned, or controlled the Subject Phone 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.

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.

5. 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.

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

In the Matter of the Search of:

Case No. 23M554

One Samsung Galaxy S20+ 5G cellular telephone bearing International Mobile Equipment Identity ("IMEI") number 3545511102792641, and assigned telephone number 773-910-2491, and Image-1 further described in Attachment A

SEARCH AND SEIZURE WARRANT

To: John J. Coleman and any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Northern District of Illinois:

See Attachment A

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:

See Attachment B

YOU ARE HEREBY COMMANDED to execute this warrant on or before June 8, 2023, at any time of the day or night because probable 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 the issuing United States Magistrate Judge.

Date and time issued: May 25, 2023 11:45am

City and State: Chicago, Illinois


Judge's signature

JEFFREY COLE, U.S. Magistrate Judge
Printed name and title

Return

Case No:

Date and Time Warrant Executed:

Copy of Warrant and Inventory Left With:

Inventory made in the presence of:

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

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 A1

Property to be searched

The property to be searched is a Samsung Galaxy S20+ 5G cellular telephone bearing International Mobile Equipment Identity (“IMEI”) number 3545511102792641 and assigned telephone number 773-910-2491 (the “Subject Phone”).

The Subject Phone is currently located at the Federal Bureau of Investigation’s Chicago Field Office, 2111 Roosevelt Road, Chicago, Illinois.

ATTACHMENT A2

Property to be searched

The property to be searched is a forensic image of the Samsung Galaxy S20+ 5G cellular telephone bearing International Mobile Equipment Identity (“IMEI”) number 3545511102792641 and assigned telephone number 773-910-2491, assigned lab number 23-CGRCFL-0330 (“Image-1”).

A storage device containing Image-1 is currently located at the Federal Bureau of Investigation’s RCFL, 610 S. Canal St., Chicago, Illinois.

ATTACHMENT B1

LIST OF ITEMS TO BE SEIZED

All records in the Subject Phone described in Attachment A1 that relate to violations of 18 U.S.C. §§ 1752(a)(1) and (2), and violent entry, disorderly conduct, and other offenses on U.S. Capitol grounds, in violation of 40 U.S.C. §§ 5104(e)(2)(C)(i), (D), and (G) (the “Subject Offenses”) that involve KAROL CHWIESIUK, AGNIESZCA CHWIESIUK, and other unidentified persons, including:

- 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 the Subject Offenses;

- k. Evidence concerning efforts after the fact to conceal evidence of the Subject Offenses, or to flee prosecution for the same;
 - l. Evidence concerning materials, devices, or tools that were used to unlawfully enter or attempt to enter the U.S. Capitol by deceit or by force, including weapons and elements used to breach or attempt to breach the building or to counter efforts by law-enforcement, such as pepper spray or smoke grenades;
 - m. Evidence of communication devices, including cellphones, closed circuit radios, or walkie-talkies, that could have been used by the Karol and Agnieszca Chwiesiuk's and/or co-conspirators to communicate during the unlawful entry into the U.S. Capitol;
 - 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.
 - o. Any records and/or evidence revealing the Karol and Agnieszca Chwiesiuk's presence at the January 6, 2021 riot;
 - p. Any 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;
 - q. Karol and Agnieszca Chwiesiuk's (and others') motive and intent for traveling to the U.S. Capitol on or about January 6, 2021; and
 - r. Karol and Agnieszca Chwiesiuk's (and others') activities in and around Washington, D.C., specifically the U.S. Capitol, on or about January 5 and 6, 2021.
2. Evidence of who used, owned, or controlled the Subject Phone 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.

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.

3. 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.

ATTACHMENT B2

LIST OF ITEMS TO BE SEIZED

All records in Image-1 described in Attachment A2 that relate to violations of 18 U.S.C. §§ 1752(a)(1) and (2), and violent entry, disorderly conduct, and other offenses on U.S. Capitol grounds, in violation of 40 U.S.C. §§ 5104(e)(2)(C)(i), (D), and (G) (the “Subject Offenses”) that involve KAROL CHWIESIUK, AGNIESZCA CHWIESIUK, and other unidentified persons, including:

- 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 the Subject Offenses;

- k. Evidence concerning efforts after the fact to conceal evidence of the Subject Offenses, or to flee prosecution for the same;
 - l. Evidence concerning materials, devices, or tools that were used to unlawfully enter or attempt to enter the U.S. Capitol by deceit or by force, including weapons and elements used to breach or attempt to breach the building or to counter efforts by law-enforcement, such as pepper spray or smoke grenades;
 - m. Evidence of communication devices, including cellphones, closed circuit radios, or walkie-talkies, that could have been used by the Karol and Agnieszca Chwiesiuk's and/or co-conspirators to communicate during the unlawful entry into the U.S. Capitol;
 - 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.
 - o. Any records and/or evidence revealing the Karol and Agnieszca Chwiesiuk's presence at the January 6, 2021 riot;
 - p. Any 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;
 - q. Karol and Agnieszca Chwiesiuk's (and others') motive and intent for traveling to the U.S. Capitol on or about January 6, 2021; and
 - r. Karol and Agnieszca Chwiesiuk's (and others') activities in and around Washington, D.C., specifically the U.S. Capitol, on or about January 5 and 6, 2021.
4. Evidence of who used, owned, or controlled the Subject Phone 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.

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.

5. 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.