

UNITED STATES DISTRICT COURT

for the
District of Columbia

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
BLACK IPAD (SERIAL DMPDH0UUNTJ2) AND BLACK SAMSUNG
SMARTPHONE (IMEI 350237721681926)

Case No. 24-SW-129

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

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

See Attachment A (incorporated by reference)

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

See Attachment B (incorporated by reference)

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

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

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. §§ 111(a)(1) -assaulting, resisting, or impeding certain officers; 18 U.S.C. § 231 -civil disorder; 18 U.S.C. § 1752(a)(1) -entering or remaining in restricted buildings 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 or disruptive conduct on the Capitol grounds).	

The application is based on these facts:

See Affidavit in Support of Application for Search Warrant.

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



Applicant's signature

Ryan Hunt, Special Agent
Printed name and title

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

Date: 4/22/2024

Judge's signature

City and state: Washington, D.C.

Robin M. Meriweather
(United States Magistrate Judge)

UNITED STATES DISTRICT COURT

for the
District of Columbia

In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address))
BLACK IPAD (SERIAL DMPDH0UUNTJ2) AND BLACK SAMSUNG)
SMARTPHONE (IMEI 350237721681926))
)
)

Case No. 24-SW-129

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

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

See Attachment A (incorporated by reference).

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

See Attachment B (incorporated by reference).

YOU ARE COMMANDED to execute this warrant on or before May 05, 2024 (not to exceed 14 days)
 in the daytime 6:00 a.m. to 10:00 p.m. at any time in the day or night because good cause has been established.

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

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Moxila A. Upadhyaya
(United States Magistrate Judge)

Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

for _____ days (not to exceed 30) until, the facts justifying, the later specific date of _____.

Date and time issued: 4/22/2024

Judge's signature

City and state: Washington, D.C.

Robin M. Meriweather
United States Magistrate Judge

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

Return

Case No.:

24-SW-129

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

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

Certification

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

Date: _____

Executing officer's signature

Printed name and title

ATTACHMENT A

Object to be Searched

The following devices seized pursuant to the search warrant for 5865 W. Post Rd., Las Vegas, Nevada on January 8, 2024: a black iPad (serial DMPDH0UUNTJ2) and a black Samsung smartphone (IMEI 350237721681926) (the “GONZALEZ DEVICES”). The GONZALEZ DEVICES are currently being stored at the FBI Washington Field Office located at 601 4th Street NW, Washington, DC 20535. This search warrant authorizes the search and forensic examination of the GONZALEZ DEVICES seized pursuant to Attachment B for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Property to be seized

1. The items to be seized are fruits, evidence, information, contraband, or instrumentalities, in whatever form and however stored, relating to violations of 18 U.S.C. §§ 111(a)(1) (assaulting, resisting, or impeding certain officers); 231 (civil disorder), 1752(a)(1) (entering or remaining in restricted buildings or grounds); 1752(a)(2) (disorderly and disruptive conduct in a restricted building or grounds) and 40 U.S.C. § 5104(e)(2)(D) (disorderly or disruptive conduct on the Capitol grounds) (the “TARGET OFFENSES”) that have been committed by MARIO GONZALEZ (“the Subject”) and other identified and unidentified persons, as described in the search warrant affidavit; including, but not limited to:

- a. Evidence of any conspiracy, planning, or preparation to commit the TARGET OFFENSES;
- b. Evidence concerning efforts after the fact to conceal evidence of those offenses, or to flee prosecution for the same;
- c. Evidence concerning materials, devices, or tools that were used to unlawfully commit the TARGET OFFENSES;
- d. Evidence of communication devices used in relation to the TARGET OFFENSES;
- e. 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
- f. 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.
- g. Evidence concerning planning to unlawfully enter the U.S. Capitol, including any maps or diagrams of the building or its internal offices;
- h. Evidence concerning unlawful entry into the U.S. Capitol, including any property of the U.S. Capitol;

- i. Evidence concerning the official proceeding that was to take place at Congress on January 6, 2021, i.e., the certification process of the 2020 Presidential Election;
 - j. Evidence concerning efforts to obstruct, impede, or 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;
 - k. Evidence concerning the breach and unlawful entry of the United States Capitol on January 6, 2021;
 - l. Evidence concerning the riot and/or civil disorder at the United States Capitol on January 6, 2021;
 - m. 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;
 - n. Evidence concerning damage to, or theft of, property at the United States Capitol on January 6, 2021;
 - o. Evidence concerning awareness that the U.S. Capitol was closed to the public on January 6, 2021;
 - p. Evidence of the defendant's presence at the U.S. Capitol on or around January 6, 2021;
 - q. Evidence concerning the results of, challenges to, or questions about the legitimacy of the 2020 Presidential Election;
 - r. Evidence regarding travel to Washington, D.C. in or around January 2021, motive and intent for travel to Washington, D.C. in or around January 2021, the planning of travel to and activity in Washington, D.C. on or about January 6, 2021, research about the U.S. Capitol, and mode of travel, travel expenses, and travel logistics on or about January 6, 2021.
 - s. Evidence regarding the riot at the U.S. Capitol on January 6, 2021;
 - t. Clothing and other items that reflect evidence of defendant's presence at the U.S. Capitol on January 6, 2021.
2. Records and information that constitute evidence of identity, including but not

limited to:

- a. clothing worn by the subject, to include a red, white, and blue beanie hat with a red pompom on top, the word "TRUMP" written in white lettering on a blue background, and the number "45" on the lower navy band around the bottom of the hat; a black hooded sweatshirt with a stylistic American-style flag in white with a

stripe replaced with the word “TRUMP” written vertically down the sweatshirt; olive green pants with thick black bands around the knees, dark shoes, and (on occasion) a dark gray facemask with black lining;

- b. clothing and other articles that reflect evidence of having participated in the unlawful activity at the U.S. Capitol, including evidence of pepper spray or other non-lethal crowd control remnants;
 - c. Other paraphernalia used by or associated with the Subject;
3. Address and/or telephone books and papers reflecting names, addresses and/or telephone numbers, which constitute evidence of conspirators and potential witnesses of violations of the TARGET OFFENSES.
4. Records and information—including but not limited to documents, communications, 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 November, 2020 through January, 2021;**
 - c. Any records and/or evidence revealing the Subject’s (and others’) motive and intent for traveling to the U.S. Capitol on or about January 6, 2021; and
 - d. Any records and/or evidence revealing the Subject’s (and others’) activities in and around Washington, D.C., specifically the U.S. Capitol, on or about January 6, 2021.
5. Photographs, in particular photographs of the subject, co-conspirators, or events in Washington D.C. on January 6, 2021, which constitute evidence of the TARGET OFFENSES.
6. Evidence of relationships between members of a conspiracy, including evidence of identification and evidence of motivation to engage in TARGET OFFENSES.

7. Cellular telephones, SIM cards, computers, laptops, I-Pads, DVDs, hard drives, and electronic store devices, and receipts reflecting their ownership and use by MARIO GONZALEZ, which contain records of the commission of the TARGET OFFENSES.

8. Indicia of ownership, including, receipts, invoices, bills, canceled envelopes, and keys, which provides evidence of identity as to individuals committing the TARGET OFFENSES; and

9. For any digital device 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(s)":

- a. evidence of who used, owned, or controlled the Device(s) 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(s), 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(s) 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(s);
- e. evidence of the times the Device(s) was used;

- f. passwords, encryption keys, and other access devices that may be necessary to access the Device(s);
- g. documentation and manuals that may be necessary to access the Device(s) or to conduct a forensic examination of the Device(s);
- h. records of or information about Internet Protocol addresses used by the Device(s);
- i. records of or information about the Device(s)'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.

10. During the execution of the search of the GONZALEZ DEVICES described in Attachment A, law enforcement personnel are also specifically authorized to obtain from MARIO GONZALEZ (but not any other individuals present at the PREMISES at the time of execution of the warrant) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint, facial characteristics, or iris display) necessary to unlock any Device(s) requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person(s)' physical biometric characteristics will unlock the Device(s), to include pressing fingers or thumbs against and/or putting a face before the sensor, or any other security feature requiring biometric recognition of:

- (a) GONZALEZ DEVICES obtained during the execution of a search warrant [(24-mj-00023-EJY), authorized by Magistrate Judge Elayna J. Youchah of the District of Nevada] at the property known as 5865 W. Post Road, Las Vegas, NV,

- (b) where the Device(s) are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,

for the purpose of attempting to unlock the Device(s)'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(s) 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(s). 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(s) for the password to any Device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any Device(s), 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.

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.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “digital devices” includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); security devices; and any other type of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF:
BLACK IPAD (SERIAL
DMPDH0UUNTJ2) AND BLACK
SAMSUNG SMARTPHONE (IMEI
350237721681926)

SW No. 24-SW-129

Filed Under Seal

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

I, Ryan Hunt, being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the digital devices namely: a black iPad (serial DMPDH0UUNTJ2) and a black Samsung smartphone (IMEI 350237721681926) obtained during the execution of a search warrant (24-mj-00023-EJY), authorized by Magistrate Judge Elayna J. Youchah of the District of Nevada at the property known as 5865 W. Post Road, Las Vegas, NV, for the things described in Attachment B.

2. Unless otherwise noted, wherever in this affidavit I assert that a statement was made, that statement is described in substance and is not intended to be a verbatim recitation of such statement.

3. Unless otherwise stated, the conclusions and beliefs I express in this affidavit are based on my training, experience, and knowledge of the investigation, and reasonable inferences I've drawn from my training, experience, and knowledge of the investigation.

AFFIANT BACKGROUND

4. I, Ryan Hunt, hereinafter referred to as your affiant, am a Special Agent with the Federal Bureau of Investigation assigned to the Washington Field Office. As a Special Agent, I am authorized by law or by a Government agency to engage in or supervise the prevention, detection, investigation, or prosecution of a violation of Federal criminal laws. I have been a Special Agent since December 2022, in which time I have investigated several violations involving domestic terrorism. I have a Bachelor of the Arts Degree in Law & Society from the University of California at Santa Barbara and I am a graduate of the FBI Academy in Quantico, Virginia where I received extensive training in federal law. As such, I am an “investigative or law enforcement officer” of the United States within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Section 2516 of Title 18, United States Code. As part of my duties, I am tasked with investigating criminal activity in and around the Capitol grounds on January 6, 2021. I am currently involved in the investigation of Mario Gonzalez.

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

6. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that violations of 18 U.S.C. §§ 111(a)(1) (assaulting, resisting, or impeding certain officers); 231 (civil disorder), 1752(a)(1) (entering or remaining in restricted buildings or grounds); 1752(a)(2) (disorderly and disruptive conduct in a restricted building or grounds) and 40 U.S.C. § 5104(e)(2)(D) (disorderly or disruptive conduct on

the Capitol grounds) (the “TARGET OFFENSES”) that have been committed by MARIO GONZALEZ (“the Subject”) and other identified and unidentified persons, including others who may have been aided and abetted by, or conspiring with, the Subject, as well as others observed by the Subject. There is probable cause to search the GONZALEZ DEVICES, further described in Attachment A, for the things described in Attachment B.

PROBABLE CAUSE

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

7. U.S. Capitol Police (USCP), the FBI, and assisting law enforcement agencies are investigating a riot and related offenses that occurred on January 6, 2021, at the United States Capitol Building, located at 1 First Street, NW, Washington, D.C., 20510.

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 the west side of the Capitol building is the West Front, which includes the inaugural stage scaffolding, a variety of open concrete spaces, two staircases, and multiple terraces. On the east side of the Capitol is the East Front, which includes 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 closed to members of the public on January 6, 2021.

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 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 Time¹ in the House of Representatives. 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. The grounds around the Capitol were posted and cordoned off, and the entire area as well as the Capitol building itself were restricted as that term is used in Title 18, United States Code, Section 1752 due to the fact that the Vice President and the immediate family of the Vice President, among others, would be visiting and did visit the Capitol complex that day.

12. At around 1:00 p.m., 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. As a result of these and other similar actions by the crowd, the situation at the Capitol became a civil disorder as that term is used in Title 18, United States Code, Section 231. The civil disorder obstructed the ability of the U.S. Secret Service to perform the federally protected function of protecting Vice President Pence.

13. As they advanced unlawfully onto Capitol grounds and towards the U.S. Capitol building over the next several hours, individuals in the crowd destroyed barricades and metal fencing and assaulted law enforcement officers with fists, poles, thrown objects, and chemical irritant sprays, among other things. Individuals in the crowd carried weapons including tire irons, sledgehammers, bear spray, and tasers, some of which were also used to assault members of law enforcement. A number of individuals in the crowd wore tactical vests, helmets, and respirators.

¹ All times stated in this affidavit are in Eastern Standard Time or Eastern Daylight Time unless otherwise noted.

14. 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. 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.

15. Beginning 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.

16. Once inside, certain of the unlawful entrants destroyed property, stole property, and assaulted federal police officers.

17. Between approximately 2:10 p.m., and 2:30 p.m., Vice President Pence evacuated the Senate Chamber, and the Senate and House of Representatives went into recess. Unlawful entrants into the U.S. Capitol building attempted to break into the House chamber by breaking the windows on the chamber door. Law enforcement officers inside the House of Representatives drew their weapons to protect members of the House of Representatives who were stuck inside. Both the Senate and the House of Representatives Chamber were eventually evacuated.

18. At around 2:47 p.m., subjects broke into the Senate Chamber not long after it had been evacuated.

19. At around 2:48 p.m., DC Mayor Muriel Bowser announced a citywide curfew beginning at 6:00 p.m. Mayor Bowser's order imposing a curfew in the District of Columbia impacted interstate commerce. For example, grocery store Safeway closed all 12 of its stores in the District of Columbia as of 4 p.m. that day, and Safeway's stores were supposed to close at 11 p.m.

20. At about 3:25 p.m., law enforcement officers cleared the Senate floor. Between 3:25 and around 6:30 p.m., law enforcement was able to clear the U.S. Capitol of all of the subjects.

21. 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, the joint session 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 throughout the events, including during the time he was evacuated from the Senate Chamber until the joint session concluded at approximately 3:44 a.m. on January 7, 2021.

22. 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.

23. 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.

24. 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.

Facts Specific to This Application

25. According to records obtained through legal process, I know that MARIO GONZALEZ traveled via plane from Las Vegas, Nevada to Philadelphia, Pennsylvania on January 5, 2021. I also know, based on analysis of open-source videos from January 6, 2021, that GONZALEZ was present in Washington D.C. and moved throughout the city with three other individuals: specifically, open source video and photos show GONZALEZ walking along Pennsylvania Avenue in Washington, D.C. in direction of the Capitol Building (below, in Photo 1), on Capitol grounds near the Peace Monument (below, in Photo 2), and outside the Capitol Building (below, in Photo 3).



Photo 1: Screen grab from open-source video: Youtube- Benjamin John: Heading up to Capitol Hill pt6.mp4 showing Mario Gonzalez (highlighted inside yellow oval) with three companions (highlighted inside blue ovals).



Photo 2: Screen grab from open-source video: Rumble | Gfive - vck5zn-trump-washington-dc-protest-jan-6th-2021-13.mp4 showing Mario Gonzalez (highlighted inside yellow oval).

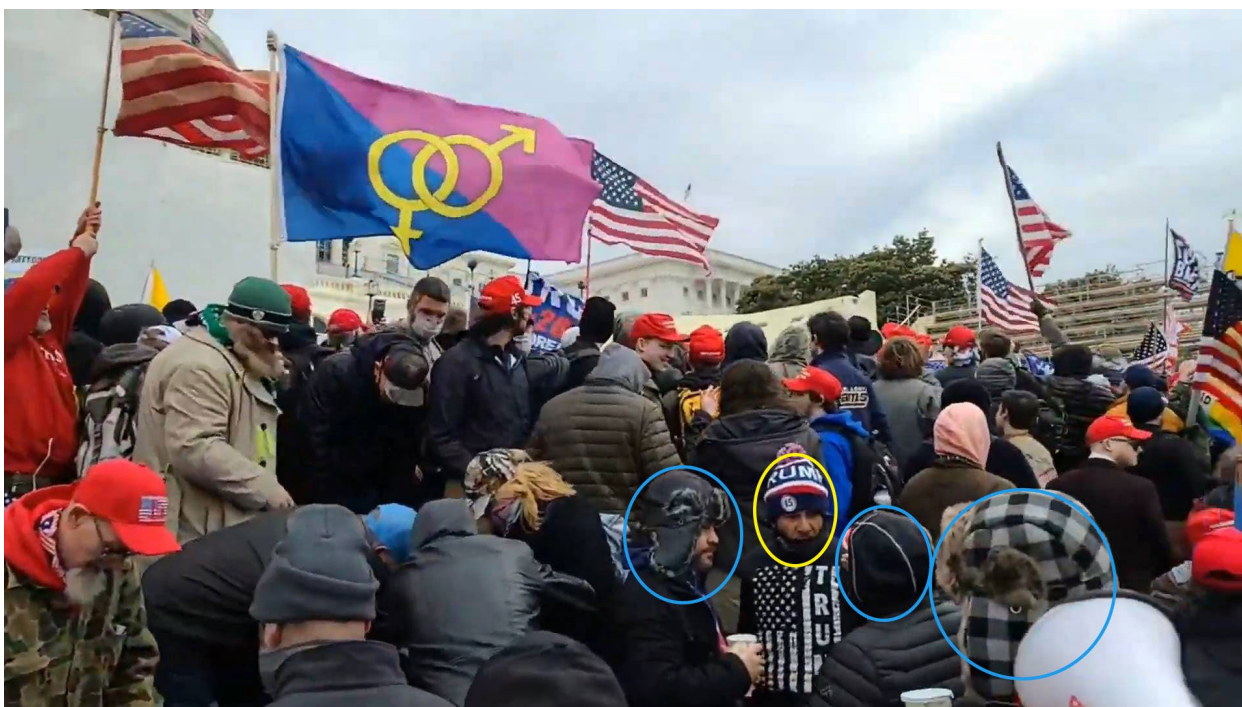


Photo 3: Screen grab from open-source video: YouTube | Buggs Media Network (buggsmedianetwork) January 6th, 2021, US Capitol showing Mario Gonzalez (highlighted inside yellow oval) with three companions (highlighted inside blue ovals).

26. MARIO GONZALEZ was positively identified by individuals who have known GONZALEZ for several years and were aware of GONZALEZ's plan to travel to Washington, D.C. on January 6, 2021. This identification was made based on photographs of GONZALEZ taken on Capitol Grounds on January 6, 2021, including Photo 1, above, a photo of GONZALEZ in front of the scaffolding on the West front of the Capitol Building (Photo 4, below), a photo of GONZALEZ taking a selfie-style photo of himself inside the scaffolding on the West front of the Capitol building (Photo 5, below), and a photo of GONZALEZ among the crowd on January 6 (Photo 6, below).



Photo 4: Screen grab from open-source video: Parler - gDUGUplC0cfv.mp4 showing Mario Gonzalez (highlighted inside yellow oval).

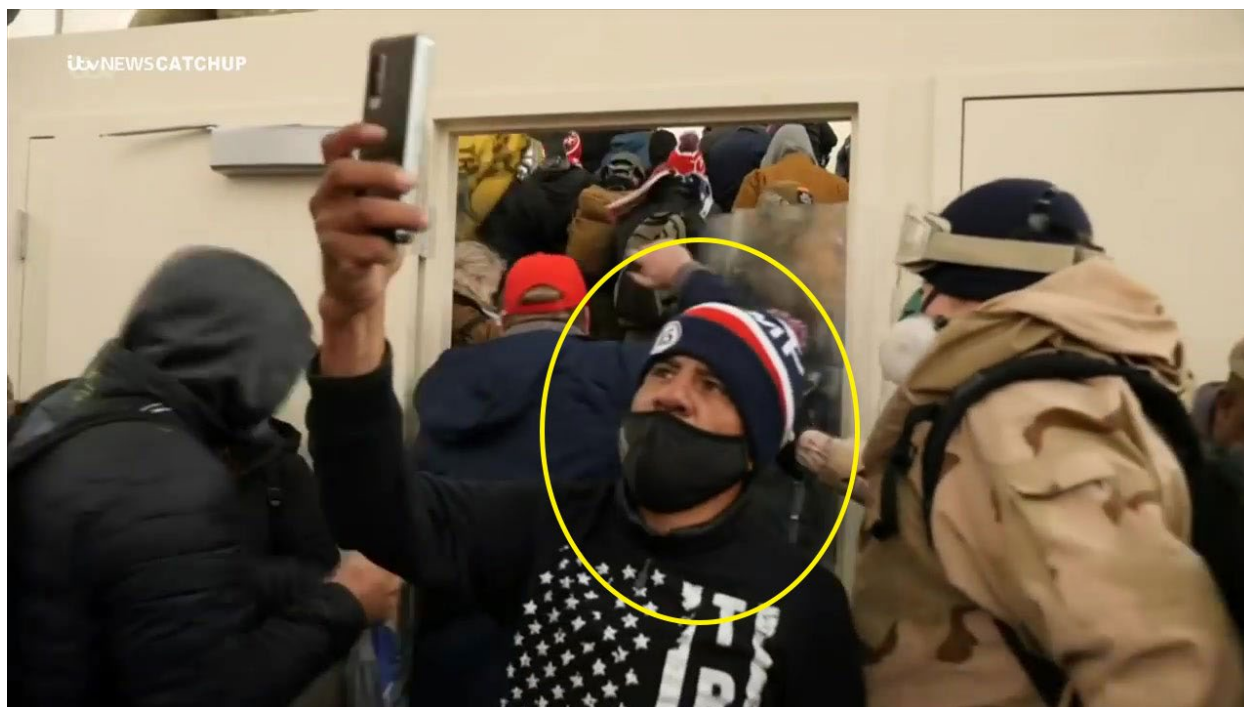


Photo 5: Screen grab from open-source video: YouTube | ITV News - jJiSmVkty4.mp4 showing Mario Gonzalez (highlighted inside yellow oval).



e my live stream was censored all day. This is what I wou
Photo 6: Screen grab from open-source video: YouTube | Southcoast Reality TV (UCFtStM5x27APovTtb25G0Tw) “Washington DC Jan 6, 2021 Live stream of Trump Rally and Capitol Riot as I saw it” showing Mario Gonzalez (highlighted inside yellow oval).

27. I know, based on my investigation into MARIO GONZALEZ's actions on January 6, 2021 and my review of open-source photos and videos from January 6, 2021, including specifically Photos 1, 3, 5, and 6 included above, that he entered the Capitol grounds wearing a red, white, and blue beanie hat with a red pompom on top, the word "TRUMP" written in white lettering on a blue background, and the number "45" on the lower navy band around the bottom of the hat; a black shirt with a stylistic American-style flag in white with a stripe replaced with the word "TRUMP" written vertically down the shirt; olive green pants with thick black bands around the knees, dark shoes, and (on occasion) a dark gray facemask with black lining.

28. An open-source video shows GONZALEZ at the Capitol on January 6, 2021 in possession of a smart phone in a silvery-gray case that he appeared to use to take a selfie-style photograph or record a video of himself. A screen shot from that video showing GONZALEZ with the phone is included above as Photo 5.

29. As shown in open-source videos, while on Capitol Grounds, MARIO GONZALEZ joined the mob that gathered on the Lower West Terrace of the Capitol. Specifically, MARIO GONZALEZ approached and entered the northern scaffolding around the inauguration stage where police were attempting to prevent the rioters from gaining access to the steps beneath the scaffolding leading up to the Capitol's Upper West Terrace. As the rioters succeeded in pushing the police line back and up the steps, MARIO GONZALEZ appeared to film the altercation with police and appeared to take selfie-style recordings of himself using his cell phone.

30. MARIO GONZALEZ then emerged from the scaffolding carrying a fire extinguisher and proceeded to spray the fire extinguisher in the direction of the police line that held the crowd at bay.

31. Shortly after he sprayed the fire extinguisher at the police line, the police deployed a chemical riot control agent in the direction of MARIO GONZALEZ. Once the riot control agent made contact with MARIO GONZALEZ, he dropped the fire extinguisher and retreated back into the crowd. A screenshot from that video showing GONZALEZ spraying the fire extinguisher is included below as Photo 7.



Photo 7: Screen grab from open-source video: Court Case Files | Nicholas DeCarlo and Nicholas Ochs (Nicholas Ochs) showing Mario Gonzalez (highlighted inside yellow oval).

32. On January 8, 2024, investigators of the FBI executed a federal search warrant (24-mj-00023-EJY), authorized by Magistrate Judge Elayna J. Youchah of the District of Nevada, at 5865 W. Post Road, Las Vegas, NV. Additionally, investigators of the FBI searched 8912 Tangerine Sky Ave., Las Vegas, Nevada after obtaining written consent by Jennifer Gonzalez, an adult resident of that premises. Pursuant to the search warrant, agents seized physical and electronic evidence, including: a black iPad (serial DMPDH0UUNTJ2), a black Samsung smartphone (IMEI 350237721681926), a red, white, and blue beanie with the word “Trump” written across it, a pair of green and black pants, and a black long-sleeved shirt with “Trump 2020” written in white vertical lettering.

33. The search warrant specifically allowed the seizure of GONZALEZ'S mobile phone and other devices used or in the control of GONZALEZ.

34. The property to be searched consist of the mobile phone (IMEI 350237721681926) and tablet (IPAD Serial DMPDH0UUNTJ2) seized during the January 8, 2024 search, hereinafter the "GONZALEZ DEVICES."

35. As described above, there is evidence that GONZALEZ had in his possession a digital device while at the U.S. Capitol on January 6, 2021. In addition, based on photos and videos of the offenses that occurred on January 6, 2021, numerous persons committing the TARGET OFFENSES possessed digital devices that they used to record and post photos and videos of themselves and others committing those offenses.

36. I also know, based on my training and experience, that cell phones are expensive, and people routinely retain their cell phones for many months or years.

37. Further, based on the investigation, numerous persons committing the TARGET OFFENSES possessed digital devices to communicate with other individuals to plan their attendance in Washington D.C. on January 6, 2021, to coordinate with other participants at the gatherings there that day, and to communicate and post on social media and digital forums about the events of January 6 after they occurred. As discussed above and as is reflected in open-source videos and photos, including Photos 1 and 3, above, MARIO GONZALEZ walked along Pennsylvania Avenue in Washington, D.C. with, and breached the Capitol grounds with three other individuals and may have communicated with those individuals regarding his actions on January 6, 2021. Based on business records obtained during the course of my investigation, I know that GONZALEZ has been associated with at least one of those individuals for a number of years.

38. Moreover, it is well-known that virtually all adults in the United States use mobile digital devices. In a fact sheet from April 7, 2021, The Pew Research Center for Internet & Technology estimated that 97% of Americans owned at least one cellular phone, and that that same 2021 report estimated that 85% of Americans use at least one smartphone. *See* Mobile Fact Sheet, <https://www.pewresearch.org/internet/fact-sheet/mobile/> (last visited November 27, 2023).

39. In addition, in my training and experience, it is common for individuals to back up or preserve copies of digital media (such as photos and videos) across multiple devices to prevent loss. Indeed, some companies provide services that seamlessly sync data across devices, such as Apple devices and the Apple iCloud service.

40. I also know based on my training and experience, that people retain the same data on different devices despite updating their smartphones to newer models, and that the data, photos, videos, and other records contained on one device are transferred onto a new model or device when an individual updates their phone.

41. Thus, there is reason to believe that evidence of the offense that originally resided on the Subject's cell phone on January 6, 2021 will also be saved to other digital devices, including his most current cell phone, located within the FBI's possession at 601 4th Street NW, Washington, DC 20535.

42. Your affiant also knows that hundreds of people have been arrested in connection to the riot that occurred at the U.S. Capitol on January 6, 2021. During searches of many those people's homes, from early 2021 through present, in multiple jurisdictions, law enforcement has recovered clothing, paraphernalia, tools, and devices that were worn, used, or carried on January 6, 2021.

43. For example, on October 30, 2023, the home of a defendant in the Eastern District of Missouri was searched, and agents recovered a hat consistent with the hat that the defendant was photographed wearing in Washington, D.C. on January 6, 2021. On November 21, 2023, a search conducted in the Northern District of Ohio yielded a subject's Bluetooth speaker that the subject was photographed carrying on January 6 and a jacket believed to be worn on January 6. On November 29, 2023, a search conducted in the District of Massachusetts yielded a window shutter slat taken from the Capitol Building, as well as a jacket and hat believed to have been worn by the subject on January 6, 2021. In the same search, officers also recovered the subject's cell phone, and a subsequent extraction from the phone yielded photos from January 6, 2021. On December 12, 2023 the home of a suspected rioter was searched in the Eastern District of Tennessee. Officers recovered black gloves, a gray hoodie-style sweatshirt, and a backpack believed to have been worn and used by the subject on January 6, 2021.

TECHNICAL TERMS

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

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

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

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

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

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

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

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

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

d. “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.

e. “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.

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

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

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

e-mail mailbox, and a personal password selected by the subscriber. By using a modem, the subscriber can establish communication with an ISP and access the Internet by using his or her account name and password.

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

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

k. “Encryption” is the process of encoding messages or information in such a way that eavesdroppers or hackers cannot read it but authorized parties can. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any unintended party that can see the ciphertext should not be able to determine anything about the original message. An

authorized party, however, is able to decode the ciphertext using a decryption algorithm that usually requires a secret decryption key, to which adversaries do not have access.

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

COMPUTERS, ELECTRONIC/MAGNETIC STORAGE, AND FORENSIC ANALYSIS

45. As described above and in Attachment B, this application seeks permission to search for evidence, fruits, contraband, instrumentalities, and information that might be found on the GONZALEZ DEVICES, including data stored on one or more digital devices. Such devices are defined above and include any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Thus, the warrant applied for would authorize the seizure of digital devices or, potentially, the copying of stored information, all under Rule 41(e)(2)(B). 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, if digital devices are found on the PREMISES or on the Subject's person, there is probable cause to believe that the items described in Attachment B will be stored in the Device(s) for at least the following reasons:

a. Individuals who engage in criminal activity, including the TARGET OFFENSES will often use digital devices, like the Device(s), to access websites to facilitate illegal activity and to communicate with co-conspirators online; to store on digital devices, like the Device(s), 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.

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.

46. As further described in Attachment B, this application seeks permission to locate not only electronic evidence or information that might serve as direct evidence of the crimes described in this affidavit, but also for forensic electronic evidence or information that establishes how the digital device(s) were used, the purpose of their 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 any of the Device(s) at issue here 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(s) are, as described further in the attachments, called for

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

b. 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.

c. 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.

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

METHODS TO BE USED TO SEARCH DIGITAL DEVICES

47. 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.

48. The volume of data stored on many digital devices will typically be so large that it will be extremely impractical to search for data during the physical search of the premises.

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

- i. The digital devices, and/or any digital images thereof created by law enforcement sometimes with the aid of a technical expert, in an appropriate setting, in aid of the examination and review, will be examined and reviewed in order to extract and seize the information, records, or evidence described in Attachment B.
- ii. 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.
- iii. In searching the digital devices, the forensic examiners may examine as much of the contents of the digital devices as deemed necessary to make a determination as to whether the contents fall within the items to be seized as set forth in Attachment B. In addition, the forensic examiners may search for and attempt to recover “deleted,” “hidden,” or encrypted data to

determine whether the contents fall within the items to be seized as described in Attachment B. Any search techniques or protocols used in searching the contents of the seized digital devices will be specifically chosen to identify the specific items to be seized under this warrant.

BIOMETRIC ACCESS TO DEVICE(S)

49. This warrant permits law enforcement agents to obtain from the person of MARIO GONZALEZ (but not any other individuals present at the PREMISES at the time of execution of the warrant) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s) requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person(s)' physical biometric characteristics will unlock the Device(s). The grounds for this request are as follows:

50. 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, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

51. 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.

52. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain devices including those manufactured by Android, Apple, or other manufacturers. In many cases, a user registers for this feature by holding the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face.

53. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

54. 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.

55. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices, the Device(s), will be found during the search. The passcode or password that would unlock the Device(s) subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the Device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

56. 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 8 hours and the passcode or password has not been entered in the last 6 days. 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.

57. Due to the foregoing, if law enforcement personnel encounter any Device(s) that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to obtain from the aforementioned person(s) the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s), including to

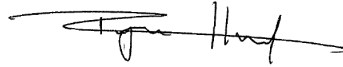
(1) press or swipe the fingers (including thumbs) of the aforementioned person(s) to the fingerprint scanner of the Device(s) found at the PREMISES; (2) hold the Device(s) found at the PREMISES in front of the face of the aforementioned person(s) to activate the facial recognition feature; and/or (3) hold the Device(s) found at the PREMISES in front of the face of the aforementioned person(s) to activate the iris recognition feature, for the purpose of attempting to unlock the Device(s) in order to search the contents as authorized by this warrant.

58. The proposed warrant does not authorize law enforcement to require that the aforementioned person(s) state or otherwise provide the password, or identify specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the Device(s). Nor does the proposed 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) would be permitted under the proposed warrant. To avoid confusion on that point, if agents in executing the warrant ask any of the aforementioned person(s) for the password to any Device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any Device(s), 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.

CONCLUSION

59. I submit that this affidavit supports probable cause for a warrant to search the GONZALEZ DEVICES described in Attachment A and to seize the data described in Attachment B.

Respectfully submitted,



RYAN HUNT
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 on 22nd day of April, 2024.

ROBIN M. MERIWEATHER
UNITED STATES MAGISTRATE JUDGE