AO93 Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the
District of Arizona

REDACTED

In the Matter of the Search of
295 CANYON DRIVE, KAYENTA, ARIZONA, 86033,
And
THE PERSON OF JAMES THOMAS ANDREW MCCARTY

Case No. 20-4298MB

ELECTRONIC SEARCH AND SEIZURE WARRANT

To: 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 and property located in the District of Arizona:

As further described in Attachments A-1 and A-2.

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

As set forth in Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 12/25/2020 *(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 as I find reasonable 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 any United States Magistrate Judge on criminal duty in the District of Arizona.

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

Date and time issued: _____

Camille D. Bibles
Digitally signed by Camille D. Bibles
Date: 2020.12.11 13:25:10 -07'00'
Judge's signature

City and state: Flagstaff, Arizona

Honorable Camille D. Bibles, U.S. Magistrate Judge
Printed name and title

Return		
Case No.: 20-4298MB	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

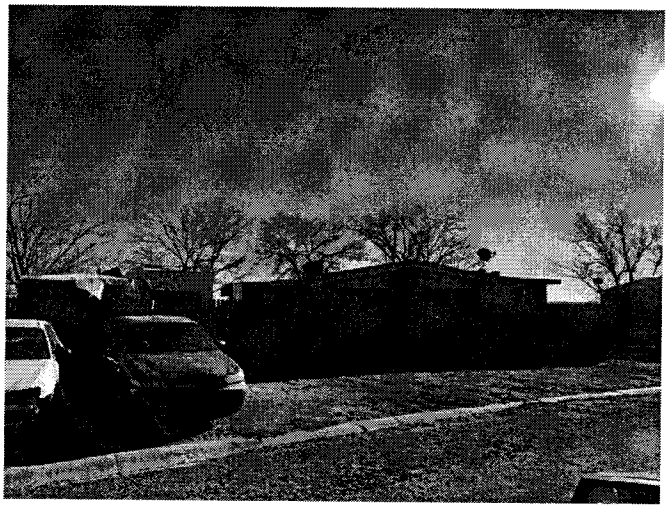
_____

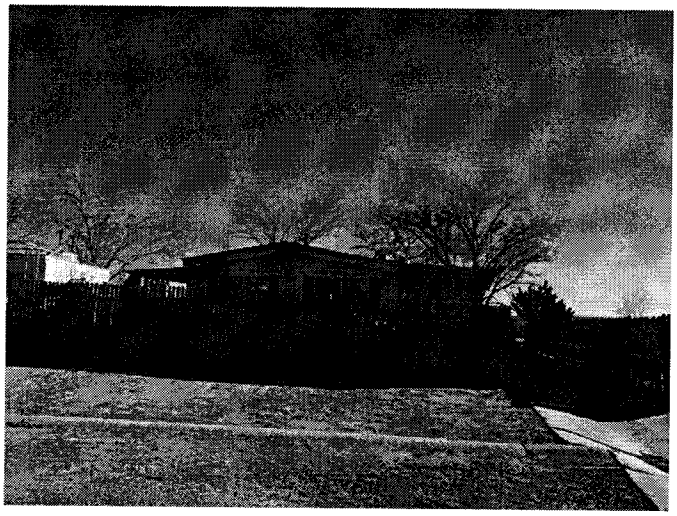
Printed name and title

ATTACHMENT A-1

Property to be searched

The premises located at 295 Canyon Dr, Kayenta, Arizona 86033, including any and all storage units, containers, safes, automobiles, carports, garages, and outbuildings (the "SUBJECT PREMISES"). The SUBJECT PREMISES, pictured below, is a single-story, single-family residence. The residence is white/grey with a satellite dish on the roof, and a brown wooden fence.





ATTACHMENT A-2

Person to be searched

The person of JAMES THOMAS ANDREW MCCARTY ("MCCARTY"), date of birth October 7, 2002. MCCARTY's Arizona Department of Motor Vehicles records list him as standing 6'01" with blonde hair and blue eyes.

The search of MCCARTY shall include any and all clothing and personal belongings, digital devices, backpacks, wallets, briefcases, purses, and bags that are within MCCARTY's immediate vicinity and control at the location where the search warrant is executed. The search shall not include a strip search or a body cavity search.

ATTACHMENT B

Property to be seized

1. All records relating to violations of 18 U.S.C. § 371 (Conspiracy), 18 U.S.C. § 1030 (Fraud and related activity in connection with computers), 18 U.S.C. 1028A (Aggravated Identity Theft), and 18 U.S.C. § 2261A (Stalking) (the "SUBJECT OFFENSES"), those violations involving JAMES THOMAS ANDREW MCCARTY and occurring after July1, 2020, including:

a. Records and information related to a conspiracy to engage in swatting;

b. Records and information related to any swatting incidents, including but not limited to photographs, videos, drawings, depicting the likenesses of any victims, their relatives, neighbors, co-workers, or friends;

c. Records and information related to communications with and the identity of any victims of swatting, stalking, or aggravated identity theft;

d. Records and information related to accessing Ring doorbells, including but not limited to login and password information for Ring accounts;

e. Records and information related to unauthorized access to online accounts of others, including but not limited to login and password information for accounts;

f. Records and information related to any victims of swatting, stalking, or aggravated identity theft, or their relatives, neighbors, co-workers, students, or friends, including their names, addresses, phone numbers, location information,

contact information, or any other personal identifying information or information about their places of work, school, or residence;

g. Records and information relating to threats to commit, or the commission of, acts of sexual or other physical violence against others;

h. Records and information relating to extortion attempts or threats to extort others, including threats to publicly post information or nude images of others online;

i. Records and information relating to the purchase, possession, or use of digital devices, including smartphones, "burner" phones, desktop computers, laptop computers, encryption software/services, virtual Private Network ("VPN") subscription services, and identity alteration or modulation devices, programs and software;

j. Records and information relating to accounts used or controlled by MCCARTY with any telephone service provider, internet service provider, or other online communication service, including but not limited to Bandwidth, TextNow, and Frontier Communications;

k. Records and information related to the use of instant and social media messages (such as Discord, Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from any digital device in connection with the SUBJECT OFFENSES;

l. Records and information related to call logs, including all telephone numbers dialed from any of the digital devices found at the SUBJECT PREMISES and all

telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

m. Records and information sufficient to show address book information, including all stored or saved telephone numbers;

n. Records and information sufficient to show indicia of occupancy, residency or ownership of the SUBJECT PREMISES and the property to be seized pursuant to the warrants, including forms of personal identification, records relating to utility bills, telephone bills, loan payment receipts, rent receipts, trust deeds, lease of rental agreements, addressed envelopes, escrow documents, keys, letters, mail, canceled mail envelopes, or clothing;

o. Records and information relating to the identity or location of the suspects; and

p. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations;

2. Computers or storage media used as a means to commit the violations described above, including unauthorized access to protected computers in violation of 18 U.S.C. § 1030(a)(2) and stalking in violation of 18 U.S.C. § 2261A.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER 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 that would allow others to control the COMPUTER, 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 lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

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

h. evidence of the times the COMPUTER was used;

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

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER'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;

m. contextual information necessary to understand the evidence described in this attachment.

4. Routers, modems, and network equipment used to connect computers to the Internet.

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 "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

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.