UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

8105 CREEKVIEW DRIVE
SPRINGFIELD, VA 22153

Case No. 1:17SW14 UNDER SEAL

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 or property located in the Eastern District of Virginia
(identify the person or describe the property to be searched and give its location):

See Attachment A (Property to be searched).

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 (Property to be seized).

YOU ARE COMMANDED to execute this warrant on or before February 1, 2017 *(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 Theresa Carroll Buchanan
(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: [illegible]
Judge's signature

City and state: Alexandria, VA Hon. Theresa Carroll Buchanan, U.S. Magistrate Judge
Printed name and title

ATTACHMENT B

Property to be seized

1. All records relating to violations of 18 U.S.C. §2261A(2) (cyberstalking) and 18 U.S.C. §875(c) (interstate communication of a threat), those violations involving Paul A. Boyne and others and occurring after August 1, 2014, including:

   a. Email, online posts, attachments, drafts, and any other computer files or communications that relate to threatening or harassing communications or otherwise relate to violations of 18 U.S.C. §2261A (cyberstalking) and 18 U.S.C. §875(c) (interstate communication of a threat);

   b. Records and information related to the Twitter handles @JudgeBozzuto, @BadBadJudge, @NuttyJudge, or any other Twitter handles or accounts related to those identified;

   c. Records and information related to the Facebook account associated with the name "Liz Bozzo (Anti-Christ)" or any other Facebook accounts related to Elizabeth Bozzuto, her family members, her friends or those close to her, including but not limited to photos or images of Elizabeth Bozzuto, her family, friends, and those with whom she is close;

   d. Records and information, including the contents of emails, related to the email addresses charlotteobservernews@gmail.com, charlotteobservernews1@gmail.com, paboyne@gmail.com; subsafe69@yahoo.com; Danachester415@gmail.com; ctdiver2121@gmail.com

or any other email addresses or accounts, including recovery email addresses or accounts, associated with the above email accounts;

2. Records and information indicating how and when the account(s)was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the email or account owner;

3. Records and information related to the account user's or owner's state of mind as it relates to the crimes under investigation;

4. Records and information related to or indicating the identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

5. Records and information related to the identity of person(s) with whom the email account user or owner communicated regarding the family court system in Connecticut as well as the use, drafting, purpose or other information related to harassing or threatening communications concerning the family court system in Connecticut or any other entity.

a. Records and information relating to access of the computers used by Paul A. Boyne;

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

c. Records and information relating to communications with Internet Protocol address 68.100.134.96;

d. Records and information relating to malicious software;

6. Computers or storage media used as a means to commit the violations described above, including 18 U.S.C. §2261A(2) (cyberstalking) and 18 U.S.C. §875(c) (interstate

communication of a threat), those violations involving Paul A. Boyne and others and occurring after August 1, 2014;

7. 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.

8. 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.