UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of the Application of the United States Of America for a Search and Seizure Warrant for a black Apple iPhone, with IMEI No. 358634091298020, and Call Number (646) 418-3329, USAO Reference No. 2020R01003	**TO BE FILED UNDER SEAL** **Agent Affidavit in Support of Application for Search and Seizure Warrant**

SOUTHERN DISTRICT OF NEW YORK) ss.:

ELISABETH WHEELER, being duly sworn, deposes and says:

I. Introduction

A. Affiant

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") ("Investigating Agency"). As such, I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. I have been a Special Agent at the FBI since 2012, and am currently assigned to the FBI's Violent Crimes Task Force. In that position, I have had significant training and experience investigating a wide range of crimes, including violence and threats of violence, such as threats made by telephone, online, and through other electronic means. I have received training and, through my investigations, have developed experience in the execution of search warrants for, among other things, telephonic and electronic communications and data.

2. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the electronic device specified below (the "Subject Device") for the items and information described in Attachment A. This affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with

other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information ("ESI"). Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

B. The Subject Device

3. The Subject Device is particularly described as a black Apple iPhone, with IMEI No. 358634091298020, and call number (646) 418-3329.

4. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online at https://support.apple.com/en_US/specs/iphone, I know that the Subject Device has capabilities that allows it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA.

5. The Subject Device is presently located in the Southern District of New York.

C. The Subject Offenses

6. For the reasons detailed below, I believe that there is probable cause to believe that the Subject Device contains evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2261A and 2 (cyberstalking) (the "Subject Offenses").

II. Probable Cause

A. Probable Cause Regarding Subject's Commission of the Subject Offenses

7. On or about October 28, 2020, the Honorable Ona T. Wang, United States Magistrate Judge for the Southern District of New York, signed a complaint (the "Complaint") charging WILLIE DENNIS, the defendant in this case, with four counts of cyberstalking, in

violation of Title 18, United States Code, Sections 2261A(2)(B) and 2. Judge Wang also signed a warrant for DENNIS's arrest. The Complaint and arrest warrant are incorporated by reference herein, and are attached hereto as Exhibit A.

8. On or about November 19, 2020, a Grand Jury returned a four-count Indictment against DENNIS, charging him with the same cyberstalking crimes. The Indictment is incorporated by reference herein, and is attached hereto as Exhibit B.

9. On or about November 16, 2021, pursuant to the arrest warrant in this case, DENNIS—a U.S. citizen—was arrested in and expelled from the Dominican Republic, where he had been residing since in or about February 2020. The Subject Device was recovered from DENNIS at the time of his arrest.

10. On or about November 18, 2021, federal agents brought DENNIS to this District, where he was presented and arraigned on the Indictment before Judge Wang. The defendant was temporarily detained; on or about November 22, 2021, he was released on bond conditions set by Judge Wang.

11. As alleged in the Complaint, and based on my review of documents obtained from victims in this case, I have learned that since in or about 2018, up to and including at least in or about March 2021, DENNIS engaged in a long-term and pervasive cyberstalking campaign of harassment, intimidation, and threats directed at colleagues at his former law firm, K&L Gates (the "Law Firm").

12. As alleged in the Complaint, and based on my review of documents collected from the Law Firm, from victims and other employees of the Law Firm, and from the defendant's personal email accounts and iCloud account seized pursuant to other search warrants, I have learned, among other things, that, as part of his cyberstalking, DENNIS sent many of his

threatening and harassing text messages to victims, and called victims, using the phone number (646) 418-3329. (*See, e.g.*, Compl. ¶¶ 15(a)-(h).)[1] Examples of such communications are discussed in paragraphs 15(a) through (h) of the Complaint.

B. Probable Cause Justifying Search of the Subject Device

13. As noted above, on or about November 16, 2021, the Subject Device was recovered from the defendant at the time of his arrest in the Dominican Republic. The Subject Device was brought back to the United States and is currently in the Southern District of New York.

14. The Subject Device was one of two Apple iPhones seized from the defendant at the time of his arrest.

15. Based on my review of subpoena returns obtained from Apple, I have learned, among other things, that the call number (646) 418-3329 is registered to an iPhone that is subscribed to in the name "Willie Dennis."

16. Based on my review of subpoena returns obtained from AT&T, I have learned, among other things, that the call number (646) 418-3329 is subscribed to in the name "Willie Dennis."

17. Based on my discussions with DENNIS's attorney, I have learned, among other things, that the Subject Device is the particular iPhone that has the call number (646) 418-3329 assigned to it.

18. As noted above and in the Complaint, the phone number assigned to the Subject Device—that is, (646) 418-3329—was used to send threatening communications to the victims in this case. Indeed, the Subject Device is itself contraband and an instrumentality of the Subject Offenses.

---

[1] The phone number is defined as "Phone Number-1" in the Complaint.

19. Like individuals engaged in any other kind of activity, individuals who engage in cyberstalking often store communications and other records relating to their illegal activity on electronic devices such as the Subject Device. Such records can include, for example, messages, calls, and emails to victims of the Subject Offenses, as well as contact information of victims, including telephone numbers, email addresses, and identifiers for instant messaging and social medial accounts.

20. In addition to probable cause to believe that the Subject Device contains evidence of the Subject Offenses, there is also probable cause to believe that the Subject Device constitutes contraband subject to seizure, in that the device contains the very threatening communications that form the basis of the charges in this case.

21. Based on the foregoing, I respectfully submit there is probable cause to believe that DENNIS is engaged in cyberstalking current and former employees of the Law Firm, and that evidence of this criminal activity is likely to be found on the Subject Device. Specifically, I believe that for the time period from at least January 1, 2019, through the present, the Subject Device is likely to contain the following evidence of this criminal activity, and of the Subject Offenses in particular[2]:

a. Evidence of WILLIE DENNIS's cyberstalking campaign, including text messages, phone calls, emails, and other communications he sent to cyberstalking victims, including current and former members of his former law firm, K&L Gates (the "Law Firm");

[2] This warrant seeks only the defendant's communications starting from January 1, 2019, but the Government reserves the right to seek a warrant to search the Subject Device for relevant communications and other data from in or about 2018 to January 2019.

b. Evidence of DENNIS's intent, motives, and state of mind with respect to the Subject Offenses;

c. Evidence of direct threats made against the cyberstalking victims and their families;

d. Evidence of any efforts DENNIS may have made to physically stalk victims, their families, and other members of the Law Firm, including any photographs DENNIS may have taken of any such individuals and/or their whereabouts;

e. Evidence reflecting the timeline of DENNIS's cyberstalking campaign;

f. Geographic location of the Subject Device during the course of the cyberstalking campaign;

g. Additional information about DENNIS's cyberstalking victims, including contact information; and

h. Evidence of user attribution showing who used the Subject Device at the time the records and items described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

III. Procedures for Searching ESI

A. Review of ESI

22. Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will review the ESI contained on the Subject Device for information responsive to the warrant.

23. In conducting this review, law enforcement may use various techniques to determine which files or other ESI contain evidence or fruits of the Subject Offenses. Such techniques may include, for example:

- surveying directories or folders 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" or reading the first few "pages" of such files in order to determine their precise contents (analogous to performing a cursory examination of each document in a file cabinet to determine its relevance);
- "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 the existence and location of search terms related to the subject matter of the investigation. (Keyword searches alone are typically inadequate to detect all information subject to seizure. For one thing, keyword searches work only for text data, yet many types of files, such as images and videos, do not store data as searchable text. Moreover, even as to text data, there may be information properly subject to seizure but that is not captured by a keyword search because the information does not contain the keywords being searched.)

24. Law enforcement personnel will make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant. Depending on the circumstances, however, law enforcement may need to conduct a complete review of all the ESI from the Subject Device to locate all data responsive to the warrant.

B. Return of the Subject Device

25. If the Government determines that the Subject Device is no longer necessary to retrieve and preserve the data on the device, and that the Subject Device is not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(c), the Government will return the Subject Device, upon request. Computer data that is encrypted or unreadable will not be returned unless law enforcement personnel have determined that the data is not (i) an instrumentality of the

offense, (ii) a fruit of the criminal activity, (iii) contraband, (iv) otherwise unlawfully possessed, or (v) evidence of the Subject Offenses.

IV. Conclusion and Ancillary Provisions

26. Based on the foregoing, I respectfully request the court to issue a warrant to seize the items and information specified in Attachment A to this affidavit and to the Search and Seizure Warrant.

_____
ELISABETH WHEELER
Special Agent
FBI

Sworn to me through the transmission of this
Affidavit by reliable electronic means,
pursuant to Federal Rules of Criminal Procedure
41(d)(3) and 4.1 this,

_____ day of December, 2021

_____
HONORABLE [redacted]
United States Magistrate Judge
Southern District of New York

Attachment A

I. Device Subject to Search and Seizure

The device that is the subject of this search and seizure warrant (the "Subject Device") is described as follows:

a black Apple iPhone, with IMEI No. 358634091298020, and call number (646) 418-3329.

II. Review of ESI on the Subject Device

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained on the Subject Device for evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2261A and 2 (cyberstalking) (the "Subject Offenses"), from the time period January 1, 2019, through the present, described as follows:

a. Evidence of WILLIE DENNIS's cyberstalking campaign, including text messages, phone calls, emails, and other communications he sent to cyberstalking victims, including current and former members of his former law firm, K&L Gates (the "Law Firm");

b. Evidence of DENNIS's intent, motives, and state of mind with respect to the Subject Offenses;

c. Evidence of direct threats made against the cyberstalking victims and their families;

d. Evidence of any efforts DENNIS may have made to physically stalk victims, their families, and other members of the Law Firm, including any photographs DENNIS may have taken of any such individuals and/or their whereabouts;

e. Evidence reflecting the timeline of DENNIS's cyberstalking campaign;

f. Geographic location of the Subject Device during the course of the cyberstalking campaign;

g. Additional information about DENNIS's cyberstalking victims, including contact information; and

h. Evidence of user attribution showing who used the Subject Device at the time the records and items described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.