UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN RE APPLICATION OF USA FOR 2703(d) ORDER FOR THREE EMAIL ACCOUNTS SERVICED BY [redacted] FOR INVESTIGATION OF VIOLATION OF 18 U.S.C. §§ 641 AND 793	**SC No. 20-sc-3355** **Filed Under Seal**

Reference: ***USAO Ref. # 2017R01896; Subject Account(s): addresses identified in Attachment A***[1]

APPLICATION OF THE UNITED STATES
FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d)

The United States of America, moving by and through its undersigned counsel, respectfully submits under seal this *ex parte* application for an Order pursuant to 18 U.S.C. § 2703(d). The proposed Order would require [redacted] or "PROVIDER"), an electronic communication service and/or remote computing service provider located at [redacted] to disclose certain records and other information pertaining to the PROVIDER account(s) associated with three [redacted] email addresses ("TARGET ACCOUNT 1" belonging to Reporter A; "TARGET ACCOUNT 2" and belonging to Reporter B; and TARGET ACCOUNT 3 belonging to Reporter C, and collectively, "TARGET ACCOUNTS") belonging to four reporters of a national news organization ("Publication 1"), identified in Attachment A ("TARGET ACCOUNTS") as set forth in Part I of Attachment A to the proposed Order, within ten days of receipt of the Order.[2] The records and other information to be disclosed

[1] In an effort to protect the Classified Information, the email accounts, which include the identity of Publication 1, are not identified in the body of the application.

[2] Public record searches indicate that the email domain belonging to Publication 1 is hosted by [redacted]

are described in Part II of Attachment A to the proposed Order.[3] In support of this application, the United States asserts:

LEGAL BACKGROUND AND JURISDICTION

1. PROVIDER is a provider of an electronic communication service, as defined in 18 U.S.C. § 2510(15), and/or a remote computing service, as defined in 18 U.S.C. § 2711(2). Accordingly, the United States may use a court order issued under § 2703(d) to require PROVIDER to disclose the items described in Part II of Attachment A. *See* 18 U.S.C. § 2703(c)(2) (Part II.A of Attachment A); 18 U.S.C. § 2703(c)(1) (Part II.B of Attachment A).

2. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated," 18 U.S.C. § 2711(3)(A)(i), and "is in . . . a district in which the provider . . . is located or in which the wire or electronic communications, records, or other information are stored." 18 U.S.C. § 2711(3)(A)(ii).

3. As discussed more fully below, acts or omissions in furtherance of the offenses under investigation occurred within Washington, D.C. *See* 18 U.S.C. § 3237.

4. A court order under section 2703(d) "shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that . . .

[redacted]

[3] Prior to seeking this process, the undersigned has consulted with the National Security Division of the U.S. Department of Justice and complied with the requirements of 28 C.F.R. §50.10 ("Policy Regarding Obtaining Information, or records of, members of the news media").

the records or other information sought . . . are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). Accordingly, the next section of this application sets forth specific and articulable facts showing that there are reasonable grounds to believe that the records and other information described in Part II of Attachment A are relevant and material to an ongoing criminal investigation.

STATUTORY AUTHORITY AND BACKGROUND

5. Under 18 U.S.C. § 641, "[w]hoever embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money, or thing of value of the United States" or "receives, conceals, or retains the same with intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined or converted" shall be fined or imprisoned not more than ten years, or both; or if the value the property does not exceed $1,000, he shall be fined or imprisoned not more than one year, or both.

6. Under 18 U.S.C. § 793(d), "[w]hoever, lawfully having possession of, access to, control over, or being entrusted with any document . . . or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted" or attempts to do or causes the same "to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it" shall be fined or imprisoned not more than ten years, or both.

7. Under 18 U.S.C. § 793(e), "[w]hoever having unauthorized possession of, access to, or control over any document . . . or information relating to the national defense which

information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted" or attempts to do or causes the same "to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it" shall be fined or imprisoned not more than ten years, or both.

8. Classified Information. Under Executive Order 13526, information in any form may be classified if it: (1) is owned by, produced by or for, or is under the control of the United States government; (2) falls within one or more of the categories set forth in the Executive Order [TOP SECRET, SECRET, and CONFIDENTIAL]; and (3) is classified by an original classification authority who determines that its unauthorized disclosure reasonably could be expected to result in damage to the national security.

9. Classified information of any designation may be shared only with persons determined by an appropriate United States government official to be eligible for access, and who possess a "need to know." Among other requirements, in order for a person to obtain a security clearance allowing that person access to classified United States government information, that person is required to and must agree to properly protect classified information by never disclosing such information to persons not entitled to receive it, by not unlawfully removing classified information from authorized storage facilities, and by not storing classified information in unauthorized locations. If a person is not eligible to receive classified information, classified information may not be disclosed to that person.

SPECIFIC AND ARTICULABLE FACTS SHOWING REASONABLE GROUNDS TO BELIEVE THAT THE RECORDS REQUESTED ARE RELEVANT AND MATERIAL

10. The United States is investigating the unauthorized disclosure of classified and proprietary information belonging to the United States. The investigation concerns possible violations of, inter alia, 18 U.S.C. §641 (Conversion of Property Belonging to the United States) and 18 U.S.C. §793 (Disclosure of National Defense Information).

11. The facts and circumstances set forth below establish specific and articulable cause to believe that between or about April 1, 2017, through on or about July 31, 2017, Reporters A, B and C of Publication 1 obtained, disclosed, or facilitated the disclosure of, classified national defense information that is the property of the U.S. government to persons unauthorized to receive that information. Specifically, there is cause to believe that Reporters A, B, and C disclosed classified national defense information provided to them by subjects who violated 18 U.S.C. § 793 and 18 U.S.C. § 641. Based on the facts and circumstances set forth herein, there is also reasonable grounds to believe that the requested [redacted] records are relevant and material to the investigation.

The Highly Classified Information Was Made Available to Congress

12. In furtherance of a Congressional Inquiry, in 2017, the U.S. Congress requested access to certain highly classified national defense information in the possession of the U.S. Intelligence Community (USIC). Given the extreme sensitivity of this information (hereinafter the "Classified Materials"), it was only made available to select Congressional Members and staff, at a secure facility within a larger USIC complex (hereinafter the "Read Room"). The material was made available in April 2017.

Portions of the Classified Materials Were Thereafter Published in the Media

13. On or about May 26, 2017, a national news outlet published an article that had three Reporters on the byline, hereinafter Reporter A, Reporter B, and Reporter C ("the May 2017 Article"). According to the USIC, the May 2017 Article revealed TOP SECRET/SCI information that was contained within the Classified Materials that had been made available to select Congressional personnel in April 2017.

14. On or about June 23, 2017, a national news outlet published an article with Reporter C, Reporter A, and Reporter B on the byline ("the June 2017 Article"). According to the USIC, the June 2017 Article revealed TOP SECRET/SCI information that was contained within the Classified Materials that had been made available to select Congress personnel in April 2017.

15. On or about July 22, 2017, a national news outlet published an article with Reporter B, Reporter A, and Reporter C on the byline ("the July 2017 Article"). According to the USIC, the July 2017 Article included TOP SECRET/SCI information that was contained within the Classified Materials that had been made available to select Congressional personnel in April 2017.

16. According to AT&T toll records [redacted] These contacts included phone calls, text messages and emails.

17. [redacted] that it had contact with Reporters A, B, and C during the period in question, and that they were attempting to obtain information to publish. [redacted]

18. Investigators are aware that news articles are often worked upon jointly by multiple Reporters, with multiple sources, and those Reporters are often revealed in byline of the article. Each of the Articles also asserted that the reporters had multiple government sources that confirmed information in their articles. [redacted] Further, their publication of the Classified Materials indicate that they were in possession of the information during the same period.

19. Based on the foregoing, there are reasonable grounds to believe that the records or other information sought concerning the TARGET ACCOUNTS are relevant and material to an ongoing criminal investigation. Specifically, these items will help the United States to identify and locate the individual(s) who illegally disclosed the Classified Information, and to determine the nature and scope of that criminal activity.

THE TARGET ACCOUNTS

20. The TARGET ACCOUNT 3 for Reporter C was identified and confirmed by [redacted] The TARGET ACCOUNT1 for Reporter A and TARGET ACCOUNT 2 for Reporter B were identified based on public statements and records published by Reporters A and B. These reporters also listed or provided these same contacts to government press offices during this same period.[4] Thus, there is reasonable cause to believe all

[4] Investigators are aware that reporters who work collectively on news stories will regularly use electronic media, including email, to communicate with sources and with one another. Investigators are also aware that reporters will often make initial contact with a source through an

the TARGET ACCOUNTS will have information relevant to the criminal investigation, including the identity of sources with knowledge of Classified Information who communicated with the Reporters.

TECHNICAL BACKGROUND

21. The Internet is a global network of computers and other devices. Devices directly connected to the Internet are identified by a unique number called an Internet Protocol, or "IP" address. This number is used to route information between devices. Generally, when one device requests information from a second device, the requesting device specifies its own IP address so that the responding device knows where to send its response. An IP address is analogous to a telephone number and can be recorded by pen-trap devices, and it indicates the online identity of the communicating device without revealing the communication's content. There are two types of IP addresses: dynamic and static. A static IP address is one that is permanently assigned to a given computer on a network. With dynamic IP addressing, however, each time a computer establishes an Internet connection, that computer is assigned a different IP address. Based on the IP address used for a given online transaction, law enforcement may be able to determine the geographical location of the Internet connection used in the transaction.

22. A network is two or more computers or other devices connected to each other that can exchange information with each other via some transmission method, such as by wires, cables, or radio waves. The equipment that connects a computer or other device to the network is commonly referred to as a network adapter. Most network adapters have a Media Access Control

---

electronic communication method (email or text) and then continue discussions over more secure and encrypted communication methods. Given that all three reporters were working on this same story [redacted] there is sufficient reason exists to believe that the reporters communicated about the Classified Information amongst themselves, and/or with their sources who had the Classified Information.

("MAC") address assigned by the manufacturer of the adapter that is designed to be a unique identifying number. An adapter's unique MAC address allows for proper routing of communications on a local area network and may be used for other purposes, such as authentication of customers by some network service providers. Unlike a device's IP address that often changes each time a device connects to the Internet, a MAC address is fixed at the time of manufacture of the adapter. Because the address does not change and is intended to be unique, a MAC address can allow law enforcement to identify whether communications sent or received at different times are associated with the same adapter.

23. On the Internet, data transferred between devices is not sent as a continuous stream, but rather it is split into discrete packets. Generally, a single communication is sent as a series of packets. When the packets reach their destination, the receiving device reassembles them into the complete communication. Each packet has two parts: a header with routing and control information, and a payload, which generally contains user data. The header contains non-content information such as the packet's source and destination IP addresses and the packet's size.

24. In addition, different Internet applications are associated with different "port numbers," or numeric identifiers. The port number is transmitted along with any communication using that application. For example, port 80 typically is associated with communications involving the World Wide Web. Port numbers are also used by many wireless carriers as a method for identifying a particular device on the wireless carrier's network.

REQUEST FOR ORDER

25. The facts set forth above show that there are reasonable grounds to believe that the records and other information described in Part II of Attachment A are relevant and material to an ongoing criminal investigation. Specifically, these items will help the United States to identify and

locate the individual(s) who are responsible for the criminal activity under investigation, their methods and techniques, and to determine the nature and scope of that criminal activity. Accordingly, the United States requests that PROVIDER be directed to produce all items described in Part II of Attachment A to the proposed Order within ten days of receipt of the Order.

26. The United States further requests that the Order direct PROVIDER not to notify any person, including the subscriber or customer of each account listed in Part I of Attachment A, of the existence of the application of the United States or the Order for one year from the date of the Court's Order unless otherwise modified by the Court. *See* 18 U.S.C. § 2705(b). This Court has authority under 18 U.S.C. § 2705(b) to issue "an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order." *See* 18 U.S.C. § 2705(b).[5]

27. In this case, the proposed Order seeks information relevant to establishing the illegal activity under investigation and identifying the individual(s) responsible. Accordingly, disclosure may reveal the existence, scope, and direction of the United States's ongoing and confidential investigation. This investigation is also a complex, national security matter that deals with the potential disclosure of classified information by senior government officials. Once alerted to this aspect of the investigation, potential target(s) could be immediately prompted to destroy or

[5] The government relies on § 2705(b) to seek a preclusion-of-notice order because the government is requesting only non-content information pursuant to § 2703(d), an action which is authorized by § 2703(c). *See* 18 U.S.C. § 2703(c)(1)(B) ("governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when [it] . . . obtains a court order for such disclosure under subsection (d) of this section"). Under § 2703(c), the government has no obligation to notify the subscriber. *See* 18 U.S.C. § 2703(c)(3) ("governmental entity receiving records or information under this section is not required to provide notice to a subscriber or customer").

conceal incriminating evidence, alter their operational tactics to avoid future detection, and otherwise take steps to undermine the investigation and avoid future prosecution. In particular, given that they are known to use electronic communication and remote computing services, the potential target(s) could quickly and easily destroy or encrypt digital evidence relating to their criminal activity.

28. Therefore, based on the foregoing, there are reasonable grounds to believe that notification of the existence of this Order would result in destruction of or tampering with evidence, or other serious jeopardy to this investigation. *See* 18 U.S.C. § 2705(b)(3) and (5).

29. Given the complex nature of the criminal activity under investigation, classified information, and also given that the criminal scheme may be ongoing, the United States anticipates that this confidential investigation will continue for the next year or longer.

30. Accordingly, this Court should command PROVIDER not to notify any other person (except attorneys for PROVIDER for the purpose of receiving legal advice) of the existence of the application of the United States or the Order for a period of one year from the date of the Court's Order. Should the court-ordered nondisclosure under Section 2705(b) become no longer needed because of the closure of the investigation or other reasons, the United States will make best efforts to notify the Court promptly and seek appropriate relief. [6]

31. In this matter, the United States also requests that the instant Application and the Order be filed under seal. The Court has the inherent power to seal court filings when appropriate, including the proposed Order. *United States v. Hubbard*, 650 F.2d 293, 315-16 (D.C. Cir. 1980) (citing *Nixon v. Warner Commn'ns, Inc.*, 435 U.S. 589, 598 (1978)). More particularly, the Court

[6] In this case, after the Provider produces the requested records, the government anticipates that it may - consistent with its obligations under 28 C.F.R. §50.10 - seek leave of the Court to notify the account holders before the one year has elapsed.

may seal the Application and Order to prevent serious jeopardy to an ongoing criminal investigation when such jeopardy creates a compelling governmental interest in confidentiality. *See Washington Post v. Robinson*, 935 F.2d 282, 287-89 (D.C. Cir. 1991). For the reasons stated above, the United States has a compelling interest in confidentiality to justify sealing the Application and Order. *See id.*

Conclusion

32. Based on the foregoing, there are reasonable grounds to believe that the email communication records of Reporters A, B, and C of Publication 1 (the TARGET ACCOUNTS) sought from April 1, 2017, through on or about July 31, 2017, are relevant and material to an ongoing criminal investigation. Specifically, the foregoing shows that the reporters published the Classified Information in this period and actively communicated with persons who had access to the Classified Information during the period, [redacted] The records sought will help the United States to identify additional persons who were contacted by the reporters about the Classified Information and locate the individual(s) who are responsible for the criminal activity under investigation, and to determine the nature and scope of that criminal activity.

Respectfully submitted,

MICHAEL R. SHERWIN
Acting United States Attorney

[redacted]

Assistant United States Attorney

[redacted]

National Security Section
555 4th Street, N.W., [redacted]
Washington, D.C. 20530

[redacted]