

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN RE APPLICATION OF USA FOR
2703(d) ORDER FOR SIX EMAIL
ACCOUNTS SERVICED BY GOOGLE
FOR INVESTIGATION OF VIOLATION
OF 18 U.S.C. §§ 641 AND 793

SC No. 20-sc-3361

Filed Under Seal

Reference: USAO Ref. # 2017R01896; Subject Account(s): addresses identified in Attachment A¹

**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 Google LLC (“Google” or “PROVIDER”), an electronic communication service and/or remote computing service provider located at 1600 Amphitheatre Parkway, Mountain View, California, to disclose certain records and other information pertaining to the PROVIDER account(s) associated with six email addresses (“TARGET ACCOUNT 1” belonging to Reporter 1; “TARGET ACCOUNT 2” and “TARGET ACCOUNT 3” belonging to Reporter 2; TARGET ACCOUNT 4 belonging to Reporter 3; “TARGET ACCOUNT 5 and “TARGET ACCOUNT 6” belonging to Reporter 4, and collectively, “TARGET ACCOUNTS”) belonging to four reporters of a national news organization (“Publication 1”), respectively, that are identified in greater detail in Part I of Attachment A to the proposed Order, within ten days of receipt of the Order.² Google also maintains a corporate office in the District of Columbia at 25

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 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”).

Massachusetts Avenue NW, Washington, D.C. 20001.³ The records and other information to be disclosed are described in Part II of Attachment A to the proposed Order. 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 . . . 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

³ Public record searches indicate that the email domain belonging to Publication 1 is hosted by Google, Inc.

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**

Background

10. Each of the TARGET ACCOUNTS belongs to a reporter at Publication 1. In April 2017, these reporters (hereinafter “Reporters 1 2, 3, and 4”) authored an article (“the Article”) that

contained classified national defense information. The Article described the investigation conducted by the Federal Bureau of Investigation (“FBI”) concerning Hillary Clinton’s use of a private email server during her tenure as Secretary of State (“the Midyear Exam Investigation”).

[REDACTED]

[REDACTED]

[REDACTED]

11. The Article contained information classified at [REDACTED]

[REDACTED] The Classified Information was never authorized for disclosure and remains classified to this day. The Classified Information belonged to a member-agency of the United States Intelligence Community (“USIC”). The USIC member-agency made a criminal referral on or about August 1, 2017. Subsequently, the FBI, along with prosecutors from the National Security Division (“NSD”) and U.S. Attorney’s Office for the District of Columbia (“USAO-DC”), began investigating this unauthorized disclosure.

12. There is reason to believe that [REDACTED] disclosed the Classified Information to Reporter 2, in violation of 18 U.S.C. §§ 641 and 793. There is also reason to believe [REDACTED] intending for [REDACTED] to share it with the media, also in violation of 18 U.S.C. §§ 641 and 793. There is also reason to believe that [REDACTED], as well as others who had access to the Classified Information, may have communicated with the TARGET ACCOUNTS regarding the unauthorized disclosure of the Classified Information. As discussed herein, there is also cause to believe that the TARGET ACCOUNTS were used to prepare the Article and communicate with other government sources who unlawfully disclosed classified information to the Reporters. Therefore, based on the facts

and circumstances set forth herein, there are reasonable grounds to believe that the requested Google records are relevant and material to the investigation.

13. Investigation by the FBI and ██████████
██████████ possessed the Classified Information. To date, the investigation has identified approximately ██████████ ██████████ who had access to both the Classified Information and ██████████. At the time the Article was published, it is likely that only these people would have understood the significance of the Classified Information with regard to ██████████
██████████
██████████ A select number of other persons in the USIC and the U.S. Department of Justice also had access to the Classified Information.

14. The investigation has further established that ██████████
██████████
██████████
██████████
██████████
██████████

⁴ ██████████ signed a “Classified Information Nondisclosure Agreement,” as well as a “Sensitive Compartmented Information Nondisclosure Agreement.” By signing these documents, ██████████ acknowledged: (1) ██████████ obligation to maintain the secrecy of classified information; (2) that the “unauthorized disclosure . . . or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage a foreign nation”; and (3) that breach of the agreement could result in prosecution of U.S. criminal laws, including 18 U.S.C. § 793. Also on ██████████ signed an acknowledgement that ██████████ had been afforded a “Security Awareness Briefing regarding my responsibilities for having a Top Secret clearance

[REDACTED]

15. [REDACTED]

[REDACTED] Many of these contacts took place around dates on which articles were published [REDACTED]. The majority of these articles do not contain classified information. [REDACTED]

16. As discussed below, there is reason to believe that [REDACTED]

[REDACTED]

[REDACTED] The FBI conducted interviews with [REDACTED] who were read into the Classified Information and [REDACTED], and they all stated they had no interaction with [REDACTED] concerning the Classified Information.

[REDACTED] *Contacts with the Media* [REDACTED]

17. [REDACTED]

[REDACTED]

and [REDACTED] My signature below asserts that I fully comprehend my security related duties/responsibilities, and affirms my commitment to [REDACTED] security policies, regulations, and procedures.”

[REDACTED]

18. [REDACTED]

[REDACTED]

multiple articles written by Reporter 2 [REDACTED]

19. During the October 2016 time period, [REDACTED]

[REDACTED]

⁵ The FBI obtained a 2703(d) order for header information associated with [REDACTED] email account, but it appears that all substantive information was deleted from the account before the FBI served its preservation letter. Agents have been unable to determine when the information was purged. It is therefore possible [REDACTED] also had direct contact with reporters via email.

⁶ Reporter 2 and [REDACTED] communicated with Reporter 2 using Reporter 2’s Publication 1 email account (TARGET ACCOUNT 2).

[REDACTED]

The Classified Information and the [REDACTED]

20. [REDACTED]

21. [REDACTED]

22. [REDACTED]

[REDACTED]

23. After the April 22, 2017 publication of the Article, [REDACTED]

[REDACTED]

24. [REDACTED]

[REDACTED]

[REDACTED]

25. [REDACTED]

[REDACTED]

[REDACTED]

26. Between October 30, 2016, and December 31, 2016, [REDACTED]

[REDACTED]

27. [REDACTED]

[REDACTED]

[REDACTED] Provides Classified Information [REDACTED] Discusses It With Reporter 2

28. [REDACTED]

29. [REDACTED]

[REDACTED]

30. [REDACTED]

[REDACTED]

31. [REDACTED]

[REDACTED]

32. [REDACTED]

[REDACTED] had obtained and/or confirmed the Classified Information from another source. [REDACTED]

[REDACTED]

[REDACTED]

33. [REDACTED]

The Classified Information Was in the Possession of Reporters 1 and 2 During [REDACTED] Leading up to the April 22, 2017 Article

34. Beginning in early 2017, [REDACTED]

35. From February 2017 to March 2017, [REDACTED] in preparation for the April 22, 2017 article. During the course of these meetings, the reporters revealed [REDACTED] that they had come into possession of the Classified Information. [REDACTED]

36. [REDACTED]

[REDACTED]

37. When the Article was published on April 22, 2017, Reporters 1 through 4 were on the byline as authors. Investigators are aware that news articles are often worked jointly by multiple reporters, with multiple sources, and those reporters are often revealed in the byline of the article. The Article asserted that the reporters had interviewed more than thirty current and former law enforcement, congressional, and other government officials to obtain information for the Article. The Classified Information is in the Article, and is attributed as being [REDACTED]

[REDACTED]

38. After the article containing the Classified Information was published, [REDACTED]

[REDACTED]

THE TARGET ACCOUNTS

39. The TARGET ACCOUNT 2 for Reporter 2 was identified and confirmed by a review of emails sent by Reporter 2 to [REDACTED] email account. TARGET ACCOUNT 3 for Reporter 2 was identified by public statements made by Reporter 2 in April 2017 that publicized his email address so the public could communicate with him. TARGET ACCOUNT 1, TARGET ACCOUNT 4, TARGET ACCOUNT 5, and TARGET ACCOUNT 6 for Reporters 1, 3 and 4 were identified based on those reporters [REDACTED] during this same period.⁷ Thus, there is reasonable to cause to believe all of the TARGET ACCOUNTS will have information relevant to the criminal investigation, including the identity of sources with knowledge of the Classified Information who communicated with the Reporters.

TECHNICAL BACKGROUND

40. 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

⁷ Investigators are also 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 electronic communication method (email or text) and then continue discussions over more secure and encrypted communication methods. Given that all four reporters were working on this same story, they used their email to communicate with [REDACTED], and they used their email accounts during the period in question, 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.

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.

41. 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 ("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.

42. 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.

43. 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

44. 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 unlawful disclosure of highly sensitive and classified information, their methods and techniques, the acts of any conspirators, 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.

45. 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 ordered 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).⁸

46. 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 FBI [REDACTED] ongoing and confidential investigation. This investigation is also a complex, national security matter that deals with the 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 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.

47. 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).

48. 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

⁸ 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”).

that this confidential investigation will continue for the next year or longer.

49. 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 proposed Order for a period of one year (commencing on the date of the proposed Order), or the period of nondisclosure is later modified by the Court. 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.⁹

50. 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 Comm'n's, Inc.*, 435 U.S. 589, 598 (1978)). More particularly, the Court 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

51. Based on the foregoing, there are reasonable grounds to believe that the email

⁹ 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.

records of Reporters 1, 2, 3 and 4 of Publication 1 (the TARGET ACCOUNTS) sought from January 14, 2017, through April 30, 2017, are relevant and material to an ongoing criminal investigation. Specifically, the foregoing shows that the reporters obtained the Classified Information after being alerted to its existence by [REDACTED] and they used electronic media to contact persons who had the Classified Information, including [REDACTED]. The records sought will help the United States to identify additional persons who were contacted by the reporters 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
N.Y. Bar No. 4444188

[REDACTED]
Assistant United States Attorney
D.C. Bar No. [REDACTED]
National Security Section
555 4th Street, N.W., [REDACTED]
Washington, D.C. 20530
Office: [REDACTED]
[REDACTED]