Lisa Hay, OSB # 980628
Federal Public Defender
Rich Federico, IN Bar #23818-89
Assistant Federal Public Defender
101 S.W. Main Street, Suite 1700
Portland, Oregon 97204
(503) 326-2123 Telephone
(503) 326-5524 Facsimile
Lisa_Hay@fd.org
Rich_Federico@fd.org
Attorneys for Defendant Ryan Payne

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF OREGON
PORTLAND DIVISION

UNITED STATES OF AMERICA, **Plaintiff,** **v.** **RYAN PAYNE,** **Defendant.**	**Case No. 3:16-cr-00051-BR** **DEFENDANT PAYNE'S MOTION TO SUPPRESS SEIZED EMAILS**

Mr. Payne respectfully requests that the Court suppress all emails obtained from Google by the government, from accounts RyPayne1@gmail.com and operationmutualaid1@gmail.com, on the grounds that the warrant by which the emails were obtained was overly broad and in violation of the particularity requirement of the Fourth Amendment. In addition, the warrant was issued in violation of the territorial limits in Rule 41 of the Federal Rules of Criminal Procedure. For each of these reasons, the evidence obtained from the searches and any fruits thereof must be suppressed.

Co-counsel who do not have standing to challenge these seized email accounts nevertheless join this motion on the legal issues and ask for leave to file a factual statement of similarly situated accounts after resolution of this motion, if relevant.[1] Counsel conferred with the government and the government opposes this motion.

FACTUAL BACKGROUND

The search warrant compels Google to copy and provide to the government, "for the period January 2013 to the present," the entire content of the contested email accounts, including draft emails that were never sent; all information stored by the user; calendars; contact lists; and images. (*See* Exhibit A, pp. 6-7 (GB.000084-85)). While another section of the warrant purports to limit what may be "searched and seized" by the government (*see* Exhibit A, pp. 38-39 (GB.000116-117)), the warrant places no limitation by content or otherwise on the government's ability to examine every single email. The application for the warrant was submitted June 5, 2014 (*see* Exhibit A, p. 42 (GB.000120)).

The search warrant was issued by a magistrate judge in the District of Nevada. The warrant identifies the property to be searched as located in the State of California. (Exhibit A, p. 6, (GB.000084)).

ARGUMENT

A. Violation of Fourth Amendment Specificity and Particularity Requirements.

The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be

[1] Mr. Payne's counsel also request leave to supplement the record with other related accounts if they are later identified.

violated, and no Warrants shall issue, but upon probable cause supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const., Amend. IV. Compelling an entity such as Google to turn over an individual's emails triggers the protections afforded to that individual by the Fourth Amendment. *See United States v. Warshak*, 631 F.3d 266, 285-88 (6th Cir. 2010) (reasonable expectation of privacy in emails); *United States v. Cotterman*, 709 F.3d 952, 957 (9th Cir. 2013) (en banc) (noting Fourth Amendment applies to digital form of "papers"). The "clear and precise words" of the Fourth Amendment "reflect the determination of those who wrote the Bill of Rights that the people of this new Nation should forever 'be secure in their persons, houses, papers, and effects' from intrusion and seizure by officers acting under the unbridled authority of a general warrant." *Stanford v. State of Texas*, 379 U.S. 476, 481 (1965). A principal protection against general warrants is the particularly requirement of the Fourth Amendment. *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). This requirement protects against general warrants by prohibiting "general, exploratory rummaging in a person's belongings." *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971).

The warrant in this case presents the issues of the application of the particularity requirement and of the prohibition against general or overly broad warrants in the context of the seizure and search of email accounts. The constitutional implications of wholesale searching of email accounts were well-recognized at the time the application for this warrant was submitted. *See generally* Nicole Friess, *When Rummaging Goes Digital: Fourth Amendment Particularity and Stored E-mail Surveillance*, 90 Nebraska L. Rev. 971 (2012). Indeed, in a published opinion, a magistrate judge within the Ninth Circuit had rejected as unreasonable the "seize first, search second" methodology proposed in this application. *In re [REDACTED]@gmail.com*, 62 F.Supp.3d 1100, 1102 (N.D. Cal. 2014). Similar opinions had been widely publicized in the media. *See, e.g.,*

Low Level Federal Judges Balking At Law Enforcement Requests For Electronic Evidence, The Washington Post, April 24, 2014 (Referring To The "Magistrates' Revolt" against unconstitutional government applications for electronic data).

The manner in which the government proposed to search email accounts for evidence of alleged criminal activity was to compel Google to provide the entire content of the accounts, from January 2013 to the present, to the government, and then to have the government search the accounts for items relating to specified criminal activity without any particular search protocol authorized in advance by the Court. Similar procedures have been soundly rejected:

> [This procedure] is best analogized to a warrant asking the post office to provide copies of all mail ever sent by or delivered to a certain address so that the government can open and read all the mail to find out whether it constitutes fruits, evidence or instrumentality of a crime. The Fourth Amendment would not allow such a warrant and should therefore not permit a similarly overly broad warrant just because the information sought is in electronic form rather than on paper.

In the Matter of Applications for Search Warrants for Information Associated with Target Email Accounts/Skype 9 Accounts, No. 13-MJ-8163-JPO, 2013 WL 4647554, at *8 (D. Kan. Aug. 27, 2013). The government chose the broadest possible method—seize everything—instead of submitting an application that met the particularity and specificity requirements of the Fourth Amendment.

Other methods to perform a constitutional search exist. "[H]aving an electronic communication service provider perform a search, using a methodology based on search terms such as date stamps, specific words, names of recipients, or other methodology suggested by the government and approved by the Court seems to be the only way to enforce the particularity requirement commanded by the Fourth Amendment." *In the Matter of the Search of Information Associated with [redacted] @mac.com that is Stored at Premises Controlled by Apple, Inc.*, 25

F.Supp.3d 1 (D.D.C. 2014); *see also In re [REDACTED]@gmail.com*, 62 F.Supp.3d at 1104 ("The court is ... unpersuaded that the particular seize first, search second proposed here is reasonable in the Fourth Amendment sense of the word.").

The Fourth Amendment violation resulting from the seizure of Mr. Payne's email accounts here is particularly egregious because the warrant imposed no requirement on the government to follow any particular screening protocol in order to prevent the exposure to the government of the entire content of Mr. Payne's email accounts, no matter how personal and how unrelated to the allegations at issue in this case. *Cf. U.S. v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1180 (9th Cir. 2010) (en banc) ("Segregation and redaction of electronic data must be done either by specialized personnel or an independent third party. If the segregation is to be done by government computer personnel, the government must agree in the warrant application that the computer personnel will not disclose to the investigators any information other than that which is the target of the warrant.") (concurring opinion of Kozinski, C.J.) (citations omitted).

Instead, the warrant refers to unnamed "government-authorized persons" who will review the seized evidence and determine whether it falls within the scope of the warrant. (Exhibit A, p. 35 (GB.000112)). There is no provision for a wall between these "government-authorized persons" and the investigation team, no limit on how the "government-authorized persons" can disseminate the information they obtain, and no requirement that non-responsive information be destroyed. The search thus exceeded any limitation in the warrant. *See, e.g., United States v. Sedaghaty*, 728 F.3d 885, 913 (9th Cir. 2013) (federal agents exceeded scope of a warrant authorizing seizure of documents relating to suspected tax fraud when they searched computer for evidence that defendant financially supported terrorist groups). For each of these reasons, the application and warrant are overbroad and the search occurred in violation of the Fourth Amendment.

The defense relies on the attached opinion of U.S. Magistrate Judge Facciola for further explication of the technological, legal, and constitutional issues at stake (*see* Exhibit B). Because the specific legal arguments will depend on the facts of this case, the defense requests permission to submit additional briefing after an evidentiary hearing, where the defense will seek to establish:

1. Whether the information provided by Google was indeed limited to information created in January 2013 or later as required by the warrant, or if, for example, email strings that pre-dated January 2013 or contacts or photographs that were added before January 2013 were provided to the government;

2. The names of the "government-authorized persons" who reviewed Mr. Payne's emails and whether these persons were part of or communicated substantively with the investigating team in any way;

3. Any later access by the government to the content of emails not seized during the initial review; and

4. Other relevant facts as become evident during the hearing.

Based on these legal principles and the facts to be further adduced at the hearing, the Court should suppress all emails obtained from the unconstitutional warrants.

B. Violation of Rule 41 Territorial Limits.

Rule 41(b) of the Federal Rules of Criminal Procedure sets out five alternative territorial limits on a magistrate judge's authority to issue a warrant. The government's application, approved by a Magistrate Judge in Nevada, does not satisfy any of them. The rule's first subsection allows a "magistrate judge with authority in the district . . . to issue a warrant to search for and seize a person or property located within the district." Fed. R. Crim. P. 41(b)(1). The government's application states on its face that the property is "stored at the premises owned, maintained,

controlled, or operated by Google, Inc., 1600 Amphitheatre Parkway, Mountain View, California 94043." (Exhibit A, p. 6, GB.00084). This property is not within the District of Nevada, where the court that issued the warrant sits. On this basis alone, the evidence obtained under the warrant must be suppressed. *See United States v. Levin*, — F. Supp. 3d —, 2016 WL 2596010, at *5 (D. Mass., May 5, 2016) (voiding a warrant under Rule 41(b) to search a computer in Massachusetts because it was issued by a magistrate in E.D. Va.); *United States v. Negrete-Gonzales,* 966 F.2d 1277, 1283 (9th Cir. 1992) (fundamental violations of Rule 41 require suppression).This argument is further developed in Mr. Payne's companion motion to suppress evidence obtained from Facebook and is incorporated here by reference.

CONCLUSION

For each of the foregoing reasons, the email evidence obtained from the unconstitutional warrants must be suppressed. An additional hearing may be required in order to determine what use the government made of the emails and whether that use resulted in evidence that should also be suppressed.

Respectfully submitted this 15th day of June, 2016.

/s/ Lisa Hay
Lisa Hay
Federal Public Defender