FILED

MAR - 7 2014

Clerk, U.S. District & Bankruptcy
Courts for the District of Columbia

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
[REDACTED]@MAC.COM
THAT IS STORED AT PREMISES
CONTROLLED BY APPLE, INC.

Magistrate Case. No. 14-228 (JMF)

MEMORANDUM OPINION AND ORDER

Pending before the Court is an Application for a search and seizure warrant pursuant to Rule 41 of the Federal Rules of Criminal Procedure and 18 U.S.C. § 2703(a), (b) and (c) to disclose certain records and contents of electronic communications relating to an Apple e-mail address.[1] Despite this Court's repeated prior warnings about the use of formulaic language and overbroad requests that—if granted—would violate the Fourth Amendment, this Court is once again asked by the government to issue a facially overbroad search and seizure warrant. For the reasons explained below, the government's application for a search and seizure warrant will be denied.

I. Background

As part of an investigation of a possible violation of 41 U.S.C. § 8702 (Solicitation and Receipt of Kickbacks) and 18 U.S.C. § 371 (Conspiracy) involving a defense contractor, the government has filed an application for a search warrant (the "Application") targeting a specific

[1] All references to the United States Code are to the electronic versions that appear in Westlaw or Lexis

Apple e-mail address. See Application at 3.[2] For purposes of this opinion, the details of the investigation—which remain under seal on the Court's docket—are irrelevant.[3]

Following a standard format used by the Department of Justice,[4] the Application is divided into three main parts. The first part provides background and explains the basis for probable cause. The second part—labeled Attachment A—is titled "Place to Be Searched" and specifies the location of Apple, Inc.; it also explains that the "warrant applies to information associated with the e-mail account [redacted]@mac.com which date from [December], 2013, until the present." Application at 14. Finally, the third part—labeled Attachment B—operates in a bifurcated manner: under the heading "Particular Things to be Seized," the Application distinguishes between "Information to be Disclosed by Apple" and "Information to be seized by the government." Application at 15-16.[5]

The government seeks the following:

> ATTACHMENT B
> Particular Things to be Seized
>
> I. Information to be disclosed by Apple
>
> To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A: All records or other information stored by an individual using each account, including address books, contact and buddy lists, pictures, and files;

---

[2] Because the Clerk's office does not index filings on ECF for a search warrant application until after an order has been issued granting or denying an application, this opinion cannot reference specific ECF filing numbers.

[3] This opinion addresses an investigatory tool related to an ongoing investigation, and the underlying documents must remain sealed for the time being. However, this opinion is intended to be—and shall be—made public, as it discusses the investigation in a sufficiently vague manner such as to avoid compromising the ongoing criminal investigation.

[4] In fact, the exact draft language is found in Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Department of Justice Criminal Division Computer Crimes and Intellectual Property Section, 255-262 *available at* http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009 pdf (last visited Mar. 7, 2014).

[5] As a practical matter, when a Magistrate Judge is presented with a search warrant application, the Judge signs both the application presented by the government and a standard search warrant form propagated by the Administrative Office of the United States Courts. The search warrant form has a space where the "items to be seized" are listed. Instead of specifying the items there, the government or the clerk's office typically writes in "See Attachment B." Thus, when the warrant is presented to the target—in this case Apple—that target receives both the form and Attachment B.

a. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken;

b. All records or other information regarding the identification of the accounts, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations. the date on which each account was created, the length of service, the types of service utilized, the Internet Protocol (IP) address used to register each account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and [sic] of payment (including any credit or bank account number);

c. All records or other information stored by an individual using each account, including address books, contact and buddy lists, pictures, and files;[6]

d. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and[7]

e. All records or other information pertaining to including [sic], without limitation, subscriber names, user names, screen names, or other identities, mailing addresses, residential addresses, business addresses, email addresses and other contact information, telephone numbers or other subscriber number [sic] or identity, billing records, credit card or bank account and information about the length of service and the types of service the subscriber or customer utilized, and any other identifying information, whether such records or other evidence are in electronic or other form.

II. Information to be seized by the government

All information described above in Section I that constitutes contraband, evidence, fruits and instrumentalities of violations of 41 U.S.C. § 8702 (Solicitation and Receipt of Kickbacks) and 18 U.S.C. § 371 (Conspiracy), between [December], 2013, and the present, including the following:

a. Records, emails, and other information referring or relating to a government investigation involving any or all of the following: [Specific names of individuals and corporations are redacted].

Application at 15-16.

II. Drafting Errors and The Scope of the Government's Request

It is evident from the sealed affidavit that the government is really after e-mails from December to the present. Nothing in Attachment B, however, explicitly requests that Apple give

[6] This paragraph is a repeat of the request after the colon in the initial paragraph.

[7] This paragraph is also listed twice in the original Application

the government any e-mails. Strictly read, it instead asks for extensive non-content records about the account as well as "address books, contact and buddy lists, pictures, and files." Application at 15. However, under the subheading of "Information to be seized by the government," Attachment B states that the government will "seize" relevant "[r]ecords, *e-mails*, and other information . . ." Id. at 16 (emphasis added). The Court believes that this confusion was caused by poor drafting. Compare Application at 15-16 (repeating sections beginning "All records or other information stored . . ." and "All records pertaining to communications between Apple . . .") with Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations at 261. After all, the affidavit discusses specific e-mail conversations as the reason for seeking the warrant; it would be illogical for the government to then *not* seek these e-mails.

While it is evident from closely reading the Application and its attachments what the government is really after, it is equally evident that the government is using language that has the potential to confuse the provider—in this case Apple—which must determine what information must be given to the government. See In the Matter of the Application of the United States of America for an Order Authorizing Disclosure of Historical Cell Site Information for Telephone Number [Redacted], 1:13-MC-199, 1:13-MC-1005, 1:13-MC-1006, 2013 WL 7856601, at *4 (D.D.C. Oct. 31, 2013) (Facciola, M.J.) ("Generic and inaccurate boilerplate language will only cause this Court to reject future § 2703(d) applications."). This Court should not be placed in the position of compelling Apple to divine what the government actually seeks. Until this Application is clarified, it will be denied.

III. Analysis

A. The Court's Previous Actions Regarding Overly Broad Search Warrant Applications

This Court is increasingly concerned about the government's applications for search warrants for electronic data. In essence, its applications ask for the entire universe of information tied to a particular account, even if it has established probable cause only for certain information. To ameliorate this problem and bring the warrants in line with the Fourth Amendment, this Court has issued "Secondary Orders" to accompany search and seizure warrants for electronic records. These "Secondary Orders" explicitly require that contents and records of electronic communications that are not relevant to an investigation must be returned or destroyed and cannot be kept by the government. See, e.g., In the Matter of the Search of Information Associated with [Redacted] That is Stored at Premises Controlled by Yahoo! Inc., 13-MJ-728, [#4] (D.D.C. Sept. 25, 2013) (sealed) (Facciola, M.J.) ("All contents and records that the United States government determines are not within the scope of Attachment B (II)(A), (B), and (C) shall be either returned to Yahoo!, Inc., or, if copies, destroyed."). Without such an order, this Court is concerned that the government will see no obstacle to simply keeping all of the data that it collects, regardless of its relevance to the specific investigation for which it is sought. See In the Matter of the Search of Information Associated with the Facebook Account Identified by the Username Aaron.Alexis That Is Stored at Premises Controlled by Facebook, Inc., 13-MJ-742, 2013 WL 7856600, at *7 (D.D.C. Nov. 26, 2013) (Facciola, M.J.) (hereinafter "Facebook Opinion").

That, however, has not been the extent of the Court's concerns. In the Court's November 2013 Facebook Opinion involving the search of the Facebook account of Navy Yard shooter Aaron Alexis, the Court raised serious concerns about the government's use of the two-step procedure under Rule 41 of the Federal Rules of Criminal Procedure. See Facebook Opinion, 2013 WL 7856600, at *6. ("Under that Rule, a warrant 'may authorize the seizure of electronic

storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or other information consistent with the warrant.'") (citing Fed. R. Crim. P. 41(e)(2)(B)). Under this approach, "the initial section of the warrants authorizing the electronic communications service provider to disclose all email communications (including all content of the communications), and all records and other information regarding the account is too broad and too general." In re Applications for Search Warrants for Information Associated with Target Email Accounts/Skype Accounts, Nos. 13–MJ–8163, 13–MJ–8164, 13–MJ–8165, 13–MJ–8166, 13–MJ–8167, 2013 WL 4647554, at *1 (D.Kan. Aug. 27, 2013) ("In re App."). Despite the Court raising its concerns and urging the government to adopt a different approach, the government continues to ask for all electronically stored information in e-mail accounts, irrespective of the relevance to the investigation.

To ameliorate these problems with respect to Alexis's Facebook account, the Court modified the search warrant to ensure that no third-party communications were turned over to the government, see Facebook Opinion, 2013 WL 7856600, at *3, and to require that the government destroy "[a]ll records and content that the government determines are NOT within the scope of the investigation." Id. at *7.

While those minimization procedures satisfied the Court in that particular case, it warned the government to "adopt stricter search parameters in future applications" or the Court would be "unwilling to issue any search and seizure warrants for electronic data that ignore the constitutional obligations to avoid 'general' electronic warrants." Facebook Opinion, 2013 WL 7856600, at *8. The Court recommended several different approaches, including key word searches, using an independent special master to conduct searches, or segregating the people who are performing the search from those who are conducting the investigation. Id. As the present

Application makes clear, the government has not taken the intervening months to address these concerns. Instead, it persists in its entitlement to the entire email account, without suggesting how the items that may be seized because there is probable cause to believe that they are evidence of a crime can be segregated from those that are not.

B. The Government Seeks an Unconstitutional General Warrant

This Court is also troubled that the government seeks a broad search and seizure warrant for e-mails and all other content related to this e-mail account. The Supreme Court has recognized two constitutional protections served by the warrant requirement of the Fourth Amendment. "First, the magistrate's scrutiny is intended to eliminate altogether searches not based on probable cause. The premise here is that any intrusion in the way of search or seizure is an evil, so that no intrusion at all is justified without a careful prior determination of necessity." Coolidge v. N.H., 403 U.S. 443, 467 (1971). Thus, it is this Court's duty to reject any applications for search warrants where the standard of probable cause has not been met. Second, as the Supreme Court has also said, "[T]hose searches deemed necessary should be as limited as possible. Here, the specific evil is the 'general warrant' abhorred by the colonists, and the problem is not that of intrusion per se, but of a general, exploratory rummaging in a person's belongings." Id. To follow the dictates of the Fourth Amendment and to avoid issuing a general warrant, a court must be careful to ensure that probable cause exists to seize each item specified in the warrant application.

With respect to searches of electronic information, careful attention must be paid to the dictates of the particularity requirements of the Fourth Amendment, which limits the "authorization to search to the specific areas and things for which there is probable cause to search." Md. v. Garrison, 480 U.S. 79, 84 (1987). As the Supreme Court has recognized, "the

requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." Id. Any search of an electronic source has the potential to unearth tens or hundreds of thousands of individual documents, pictures, movies, or other constitutionally protected content. It is thus imperative that the government "describe the items to be seized with as much specificity as the government's knowledge and circumstances allow." United States v. Leary, 846 F.2d 592, 600 (10th Cir. 1988).

Here, the government has adequately described the "items to be seized"—but it has done so in the wrong part of the warrant and in a manner that will cause an unconstitutional seizure. By abusing the two-step procedure under Rule 41, the government is asking Apple to disclose the entirety of three months' worth of e-mails and other e-mail account information. See Application at 14-15. Yet, on the very next page, it explains that it will only "seize" specific items related to its criminal investigation; it goes so far as to name specific individuals and companies that, if mentioned in an e-mail, would make that e-mail eligible to be seized. Id. at 15. Thus, the government has shown that it *can* "describe the items to be seized with [] much specificity"; it has simply chosen not to by pretending that it is not actually "seizing" the information when Apple discloses it. See Facebook Opinion [#5] at 9-10 ("By distinguishing between the two categories, the government is admitting that it does not have probable cause for all of the data that Facebook would disclose; otherwise, it would be able to 'seize' everything that is given to it.").

As this Court has previously noted, any material that is turned over to the government is unquestionably "seized" within the meaning of the Fourth Amendment. See Brower v. Cnty. of Inyo, 489 U.S. 593, 596 (1989) (noting that a "seizure" occurs when an object is intentionally

detained or taken). The two-step procedure of Rule 41 cannot be used in situations like the current matter to bypass this constitutional reality because the data is seized by the government as soon as it is turned over by Apple. Even if, as Professor Orin Kerr has stated, a search does not occur until "the data is exposed to possible human observation," Orin Kerr, Searches and Seizures in a Digital World, 119 Harv. L. Rev. 531, 551 (2005), the seizure of a potentially massive amount of data without probable cause has still occurred—and the end result is that the government has in its possession information to which it has no right. See In re App., 2013 WL 4647554, at *9 ("The Court notes that while nothing in Section 2703 or Fed.R.Crim.P. 41 may specifically preclude the government from requesting the full content of electronic communications in a specific email account, the Fourth Amendment may do so and does here."). What the government proposes is that this Court issue a general warrant that would allow a "general, exploratory rummaging in a person's belongings"—in this case an individual's e-mail account. Coolidge, 403 U.S. at 467. This Court declines to do so.

C. The Electronic Communications Service Provider Should Perform the Search

In the Facebook Opinion, this Court urged the government to adopt a procedure that would allow it to obtain the information it legitimately needs for criminal investigations while respecting the Fourth Amendment, such as:

1. Asking the electronic communications service provider to provide specific limited information such as emails or faxes containing certain key words or emails sent to/from certain recipients;
2. Appointing a special master with authority to hire an independent vendor to use computerized search techniques to review the information for relevance and privilege;
3. 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;

4. Magistrate judges should insist that the government waive reliance upon the plain view doctrine in digital evidence cases; and
5. The government's search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents.

See Facebook Opinion, 2013 WL 7856600, at *8 (citing In the Matter of Applications for Search Warrants for Case Nos. 12-MJ-8119-DJW and Information Associated with 12-MJ-9191-DJW Target Email Address, Nos. 12-MJ-8119, 12-MJ-8191, 2012 WL 4383917, at *10 (items 1-2); United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1180 (9th Cir. 2010) (Kozinski, J. concurring) (items 3-5)). See also In re Search Warrant, 71 A.3d 1158, 1186 (Vt. 2012) (upholding nine *ex ante* restrictions on a search warrant for electronic data but holding that the issuing officer could not prevent the government from relying on the plain view doctrine).

Despite being warned to "seriously consider how to minimize the amount of information that its search warrant applications seek to be disclosed" or "find this Court unwilling to issue any search and seizure warrants for electronic data that ignore the constitutional obligations to avoid 'general' electronic warrants," Facebook Opinion, 2013 WL 7856600, at *8, the government continues to submit overly broad warrants and makes no effort to balance the law enforcement interest against the obvious expectation of privacy e-mail account holders have in their communications. See United States v. Warshak, 631 F.3d 266, 285-86 (6th Cir. 2010) ("Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection."). In this case, balancing those interests might require that Apple perform the search for relevant e-mails. Indeed, despite any government protestation, a subpoena served on a third party, such as a bank, compels that entity to look within a record set for the particular documents sought. E-mail providers like Apple are technologically sophisticated actors; in fact, one of Apple's main

competitors, Google, has created an entire business model around searching the contents of e-mail in order to deliver targeted advertising, and it has done so for a decade. See, e.g., Jon Healey, Privacy Advocates Attack Gmail – Again – for Email Scanning, Los Angeles Times, Aug. 15, 2013, *available at* http://articles.latimes.com/2013/aug/15/news/la-ol-google-gmail-privacy-reasonable-expectation-20130814 (last visited Mar. 7, 2014) ("As Google notes, this practice has been a standard feature of Gmail since its inception in 2004."). There is no reason to believe that Apple or any other entity served with a warrant is incapable of doing what entities responding to subpoenas have done under common law.

In its "seizure" section, the Application specifies that e-mails would only be "seized" if they relate to specific people and companies. See Application at 16. On a more fundamental level, the government surely knows how it intends to ultimately sort through the information disclosed by Apple. If a wide disclosure followed by a government search violates the Fourth Amendment, then the obvious answer is to have Apple perform the search using the criteria that the government would itself use in the same way that a bank, in the example used above, might find a particular type of document in its customer files.

This Court is aware that other district courts have held that the "Fourth Amendment does not require the government to delegate a prescreening function to the internet service provider or to ascertain which e-mails are relevant before copies are obtained from the internet service provider for subsequent searching." United States v. Taylor, 764 F. Supp. 2d 230, 237 (D.Me. 2011); accord United States v. Bickle, 10-CR-00565, 2011 WL 3798225, at *20 (D.Nev. July 21, 2011); United States v. Bowen, 689 F.Supp.2d 675, 682 (S.D.N.Y. 2010). But, in light of the government's repeated submission of overly broad warrants that violate the Fourth Amendment, this Court can see no reasonable alternative other than to require the provider of an electronic

communications service to perform the searches. Under the government's demand that it be given everything, the government leaves the Court with only two options: deny the warrants—thus depriving the government of needed information—or issue warrants that are repugnant to the Fourth Amendment. Neither is viable.

Thus, having 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.

D. The Government Must Return or Destroy Irrelevant Information

The Court is particularly troubled that the Application does not specify what will occur with e-mails and other information that is, even by the government's standards, not relevant. Will that information be returned, destroyed, or kept indefinitely? The "Secondary Orders" that have been routinely issued by this Court—and a significant portion of the Facebook Opinion—have required the government to destroy all contents and records that are not within the scope of the investigation as outlined in the search warrant. See Facebook Opinion, 2013 WL 7856600, at *7. While such a clause in a search warrant application is certainly necessary for its issuance by this Court, the government should not believe that it is sufficient. In this case, its absence is grounds enough for the Court to deny the Application.

IV. Conclusion and Order

By the Court's count, it modified approximately twenty search and seizure warrants for electronic information during September and December 2013. It will no longer do so. Instead, any warrants that do not comport with the requirements of the Fourth Amendment will—like the present Application—be denied with an explanation of why they have been denied so that the

government may have an opportunity to correct its defects. To be clear: the government must stop blindly relying on the language provided by the Department of Justice's Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations manual. By doing so, it is only submitting unconstitutional warrant applications.

It is hereby **ORDERED** that the government's Application is **DENIED** without prejudice.

SO ORDERED.

Digitally signed by John M. Facciola
DN: c=US, email=john_m._facciola@dcd.uscourts.gov, o=United States District Court for the District of Columbia, cn=John M. Facciola
Date: 2014.03.07 12:21:39 -05'00'

JOHN M. FACCIOLA
UNITED STATES MAGISTRATE JUDGE