IN THE DISTRICT COURT OF THE UNITED STATES
FOR THE MIDDLE DISTRICT OF ALABAMA
NORTHERN DIVISION

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH FIFTEEN EMAIL ADDRESSES STORED AT PREMISES OWNED, MAINTAINED, CONTROLLED OR OPERATED BY 1 & 1 MEDIA, INC., GOOGLE, INC., MICROSOFT CORP., and YAHOO! INC.	)	Case No. 2:17CM3152-WC

ORDER

On June 15, 2017, the United States presented fifteen separate applications for search warrants related to its investigation of alleged identity theft and related fraudulent tax filings.[1] After careful review of the applications, the undersigned Magistrate Judge concludes that, for the reasons given below, the applications are due to be denied.

I. THE APPLICATIONS

In each of the fifteen applications for search warrants, the United States seeks permission to require the above-captioned electronic communications service providers ("ECSP"s) to provide the United States with information associated with a particular email account stored, maintained, controlled, or operated by the provider. The applications are based largely upon the same asserted probable cause, with variations pertaining to specific communications to and from the email account that is the subject of that specific warrant application. As presented to the undersigned, the warrant applications are structured as

[1] Because the Government requested that the warrant applications be filed under seal, they are attached as sealed exhibits to this Order.

follows: Attachment A to the search warrant describes the thing or property to be searched—i.e., the email account and the ECSP that owns, maintains, controls, or operates the email account—and Attachment B defines, in two separate parts, the "Particular Items to be Seized." Part One of Attachment B describes the information that the warrant requires the ECSP to provide to the Government, including the following:

> a. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
>
> b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
>
> c. The types of service utilized;
>
> d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
>
> e. All records pertaining to communications between [the ECSP] and any person regarding the account, including contacts with support services and records of actions taken.
>
> f. All location data associated with the account.
>
> g. All location history associated with the account, whether derived from Global Positioning System (GPS) data, cell site/cell tower triangulation/trilateration, and precision measurement information such as timing advance or per call measurement data, and Wi-Fi location. Such data

shall include the GPS coordinates and the dates and times of all location recordings.

h. All identity and contact information, including full name, e-mail address, physical address (including city, state, and zip code), date of birth, phone numbers, gender, hometown, occupation, and other personal identifiers.

Part Two of Attachment B describes the "information to be seized by the Government" as follows:

All information described above in Section 1 that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Section 1028A; Title 18, United States Code, Section 1030; and title 18, United States Code, Section 1343 since January 1, 2015, including information pertaining to:

a. Records and communications regarding the transmission of personally identifiable information, IRS Forms W-2, tax returns, prepaid debit cards, the proceeds of the transfer or use of personally identifiable information, and a conspiracy to file false tax returns using stolen identities;

b. Records and communications regarding any property derived from the proceeds of the conspiracy;

c. Records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts; and

d. Records indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner, including all geolocation information.

e. Records relating to the identities of the person(s) who communicated with the user ID about matters described in paragraph 2.a., including records that help reveal their whereabouts.

In addition to describing the probable cause underlying the Government's requests, the

affidavits in support of the search warrant provide a cursory description of the Government's planned search methodology. The affiant swears that he will use the warrant to require the ECSP "to disclose to the government copies of the records and other information (including the content of communications) particularly described in Attachment A and Section 1 of Attachment B. Upon receipt of the information described in Section 1 of Attachment B, government-authorized persons will review that information to locate the items described in Section 2 of Attachment B."

II. DISCUSSION

For the sake of brevity and convenience to the court and the Government, and to facilitate the prompt anticipated appeal of this Order, the undersigned will forego a rigorous discussion of the Fourth Amendment principles undergirding the undersigned's concern with the Government's search warrant requests. It is sufficed for present purposes to note, and the undersigned does not believe that the Government would disagree, "that indiscriminate searches and seizures conducted under the authority of 'general warrants' were the immediate evils that motivated the framing and adoption of the Fourth Amendment[,]" *Payton v. New York*, 445 U.S. 573, 583 (1980); that the Fourth Amendment's particularity requirement is the primary means by which the Constitution seeks to guard against such "indiscriminate searches and seizures," *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971); that Fourth Amendment protections—including the prohibition on general warrants—extend to the content of electronic communications like emails, *see, e.g., Vista Marketing, LLC v. Burkett*, 812 F.3d 954, 969 (11th Cir. 2016)

(citing *United States v. Warshak*, 631 F.3d 266, 268 (6th Cir. 2010)) ("the Fourth Amendment demands that the government demonstrate probable cause . . . to review the content of stored electronic communications"); and that, in this digital age, electronic communications like emails may be used for sharing and storing highly personal and sensitive information relating to the account holder and those with whom he or she communicates electronically.

In recent years, courts have begun grappling with how to balance the Government's legitimate interest in searching for evidence of alleged crimes that might be found in electronic communications like emails with the privacy rights of the email account user and those with whom the user has communicated. The practical realities of how potentially vast amounts of data may be collected, stored, transferred, and reviewed have made this balancing a difficult task. The Government's warrant applications in this case are not unique; they appear to track the Department of Justice's format for search warrant applications that has been reviewed in numerous published district court opinions in recent years. Of course, while some of these decisions have rejected applications like those presented here, one may safely presume that substantially more courts have approved of these applications, and issued search warrants, than have denied them. Nevertheless, for the reasons that follow, in this instance, the undersigned finds the applications before the court sufficiently problematic to join those courts that have rejected similar applications.[2]

---

[2] In particular, the court has found the reasoning and analysis set out in the following opinions rejecting similar search warrant applications to be particularly persuasive in analyzing the instant

As set forth in the above excerpt from the Government's applications, the Government's search warrants would require the disclosure to the Government of essentially all data, including the contents of communications, relating to the subject email accounts, without limitation as to time. After some method of review that the Government does not describe in any appreciable form, from this universe of data the Government will "seize" only what it considers "fruits, evidence, and instrumentalities" of the crimes that it is investigating "since January 1, 2015." There is no protocol requiring the destruction, discarding, return, or quarantining of data that the Government does not "seize." In the undersigned's view, these aspects of the Government's applications—that the Government's collection of data is not temporally limited despite its temporally-limited showing of probable cause (and its manifest intent to only seize evidence of specific crimes "since January 1, 2015"), and that the Government will keep and retain access indefinitely to all nonpertinent data it receives—render the Government's applications requests for unconstitutionally overbroad, general warrants.

As a preliminary matter, the undersigned notes that, irrespective of the concern articulated above, the validity of the Government's applications rests on the artifice that there is a distinction between what is disclosed to, and apparently kept by, the Government,

---

warrant applications: *In the Matter of the Search of premises known as: Three Hotmail Email accounts: [redacted]@hotmail.com, [redacted]@hotmail.com, [redacted]@hotmail.com Belonging to and Seized from [redacted]*, 2016 WL 1239916 (D. Kan. Mar. 28, 2016), *reversed in-part*, 212 F. Supp. 3d 1023 (D. Kan. 2016); *In re: [REDACTED]@gmail.com*, 25 F. Supp. 3d 1100 (N.D. Cal. 2014); and *In the Matter of the Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.*, 25 F. Supp. 3d 1 (D. D.C. 2014).

and what the Government actually "seizes." In the undersigned's view, where an ECSP is compelled to "disclose" data, and where the Government intends to search through and keep all such disclosed data regardless of relevance, there can be no doubt that all data encompassed by the warrant is effectively seized. *See, e.g., In the Matter of the Search of Info.*, 25 F. Supp. 3d at 6-7; *In the Matter of the Search of Premises*, 2016 WL 1239916, at *12. This is so regardless of the fact that the Government purports to "seize" only a more narrowly defined subset of the data disclosed to it.

The undersigned recognizes those court opinions indulging the Government in this fiction and concluding that this "seize then search" methodology is permitted under Rule 41 of the Federal Rules of Criminal Procedure and the Stored Communications Act. *See, e.g., In the Matter of Search of Info. Associated with Email Addresses Stored at Premises Controlled by the Microsoft Corporation*, 212 F. Supp. 1023, 1034-37 (D. Kan. 2016) (reversing in-part the Magistrate Judge's opinion denying warrant applications); *In the Matter of a Warrant for All Content and Other Info. Associated with the Email Account xxxxxxx@gmail.com Maintained at Premises Controlled by Google, Inc.*, 33 F. Supp. 3d 386, 390-94 (S.D. N.Y. 2014) (granting search warrant). Although generally uncomfortable with that conclusion as a matter of law, the undersigned does not rest this Order on a rejection of that legal premise. Rather, the undersigned only discusses the legal fiction central to the Government's requests in order to lend context to the discussion of Fourth Amendment reasonableness to follow. That is, where the legality of the Government's conduct already depends upon an attenuated construction of what

constitutes a seizure, the court should be particularly scrupulous in holding the Government to its burden to show that its conduct is reasonable.

"[R]easonableness is always the touchstone of Fourth Amendment analysis[.]" *Birchfield v. North Dakota*, 136 S.Ct. 2160, 2186 (2016). In the search and seizure context, reasonableness is measured "by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate government interests." *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999). Here, the intrusion on the email users' privacy is substantial: every significant detail relating to the email account, including the content of every communication ever sent or received, is to be provided to the Government for inspection on terms and conditions known only to the Government, and to be retained by the Government indefinitely with no manifest restriction on the Government's ability to repeatedly review the contents of all email communications. Despite the Government's assurance that it will only "seize"—meaning, apparently, segregate from other seized data for the purposes of "use" in the investigation—evidence related to the crimes it is investigating "since January 1, 2015," there is no restriction on the Government's ability to take "plain view" of material that is not pertinent to its current investigation but that might be relevant to some other criminal investigation for which the Government has not presented probable cause to search for evidence.

So, then, one side of the required reasonableness balancing is substantially weighted. However, the undersigned must weigh against the Government's intrusion the

degree to which such intrusion is "needed for the promotion of legitimate government interests." *Houghton*, 526 U.S. at 300. Although the undersigned concedes that the Government has presented probable cause to believe that persons using the subject email accounts have participated to some degree in an identity theft scheme, and therefore some intrusion is warranted, the warrant applications do not explain, and the undersigned cannot fathom, why the absolute intrusion the Government seeks is needed. As noted previously, despite that it seeks disclosure of the contents of all communications to or from each subject email account, by its own terms, the Government seeks to "seize" only information constituting "fruits, evidence and instrumentalities" of certain crimes "since January 1, 2015[.]" In view of this definitive temporal limitation on what the Government ostensibly wants, the warrant applications fail to provide a sufficient justification for the overseizure[3] sought by the Government and described in this Order.

Furthermore, apart from the Government's own temporal limitation, the actual probable cause articulated with respect to each subject email address does not support the comprehensive disclosure sought by the Government. It is important to note at this juncture that, with fifteen different email accounts at issue, the Government's showing of probable cause naturally falls along a continuum of strength depending upon the extent of the involvement of each account. Each warrant application broadly describes the identity

[3] For clarity, the undersigned again emphasizes that, in this context, "seizure" refers to what the Government intends to collect and retain in its possession, not simply what the warrant itself describes as a seizure.

theft scheme and then describes some communications to or from the subject email account indicating that the email account was used to further the scheme. Some email accounts appear extensively involved.[4] Others appear much less involved. Indeed, one email account is described only as having received two emails and sent one email within a five-minute span one morning in February of 2017. *See* Ex. 7. Do three possibly incriminating emails spaced over five minutes one morning in 2017, supposedly in furtherance of an identity theft scheme beginning in 2015, justify the wholesale disclosure and unfettered inspection and retention of every email ever sent or received by that email account, no matter how many years prior to 2017 or 2015 such emails might have originated? If the Government can make the case that such overseizure is needed—not just desired, but *needed*—for the promotion of its interest in investigating a criminal scheme beginning in 2015, then the application before the court does not make it. Thus, it seems to the undersigned that, at this time, a reasonable balancing of the competing interests involved would permit the Government to search email content in closer temporal proximity to both the alleged criminal activity and, in particular, the email transmissions that the Government relies upon as establishing probable cause.[5]

---

[4] For example, a few email accounts are described as having exchanged dozens of emails over more than a year containing information in furtherance of the identify theft scheme.

[5] Judge Waxse's analogy is apt:

> The Court remains concerned that each of the target email accounts may—and likely do—contain large numbers of emails and files unrelated to the alleged crimes being investigated and/or for which the government has no probable cause to search or seize. . . . [T]hese warrants are akin to a warrant asking the post office to

The Government could easily strike a reasonable balance by, for example, limiting the "Information to be disclosed" in part 1.a of Attachment B of each of the proposed search warrants to "[t]he contents of all emails associated with the account *occurring after December 31, 2014*." By doing so, the Government would vindicate its interest in discerning the extent of the account user's involvement in the criminal activity under investigation without significantly prejudicing its stated objective to "seize" the "fruits evidence and instrumentalities" of certain crimes "since January 1, 2015." Perhaps a review of the content of emails occurring after 2014 would even uncover probable cause to justify a search into earlier emails, and would therefore warrant returning to the court to seek a second, broader search warrant. But there is no doubt that such a restriction would, as much as is reasonably practicable at this time, limit the Government's intrusion on the account user's expectation of privacy in their email communications. Thus, because the Government seeks at the outset to access and search potentially so much more than its specific showing of probable cause would support, the undersigned is left with the abiding conviction that what the Government actually seeks is "a general, exploratory rummaging,"

> 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 the Search of Premises Known as: Three Hotmail Accounts, 2016 WL 1239916, at *13 (quotation omitted). In other words, the mere fact that technological innovation has made such a seizure possible (or convenient) does not mean that the Fourth Amendment should now be enfeebled to accommodate it.

Coolidge, 403 U.S. at 467, through the content of all of the account users' email. The Fourth Amendment must require a stronger showing by the Government to permit intrusion of that magnitude.

In addition to concern about the overbreadth of the requested search warrants, the undersigned is concerned about the lack of any protocol for the Government's handling of non-pertinent information that the Government would compel the ECSP to disclose but that it ostensibly does not "seize." The warrant applications do not indicate that such information will be returned to the ECSP, destroyed, segregated, or quarantined from Government investigators. The Government's ability to repeatedly cull through potentially troves of highly personal—but ultimately irrelevant—information about the account users effects a continued violation of the account users' expectations of privacy for which no reasonable justification can be found in the application. This flaw is especially problematic considering that, as discussed previously, the Government seeks to compel the ECSPs to provide essentially every bit of data pertaining to the subject email accounts, without any limitation as to time or pertinence to its investigation.

The defects described in this Order present substantial jeopardy to the Fourth Amendment rights of the users of the email accounts targeted by the Government. The warrant applications fail to provide a sufficient basis for finding the defects reasonably necessary to promote the Government's interests in conducting its investigation. Moreover, it appears to the undersigned that the defects are either easily avoided or remediated. As such, the undersigned is compelled to find that these defects are fatal to

the Government's applications, and that such applications must therefore be denied at this time.

III. CONCLUSION

For all of the foregoing reasons, the undersigned DENIES the fifteen applications for search warrants related to the email accounts described in the applications presented to the undersigned on June 15, 2017.

DONE this 14th day of July, 2017.

/s/ Wallace Capel, Jr.
CHIEF UNITED STATES MAGISTRATE JUDGE