UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

IN THE MATTER OF A WARRANT FOR ALL CONTENT AND OTHER INFORMATION ASSOCIATED WITH THE EMAIL ACCOUNT xxxxxxx@GMAIL.COM MAINTAINED AT PREMISES CONTROLLED BY GOOGLE, INC.	MEMORANDUM OPINION 14 Mag. 309

On June 11, 2014, this Court was presented with an application for a search warrant pursuant to Rule 41 of the Federal Rules of Criminal Procedure and 18 U.S.C. §§ 2703(a), (b)(1)(A), and (c)(1)(A). The application sought a warrant to obtain emails and other information from a "Gmail" account, which is hosted by Google, Inc., and to permit a search of those emails for certain specific categories of evidence. The Court granted the application on the day it was presented. In light of decisions issued elsewhere in the country that have denied search warrants in similar circumstances — particularly in the District of Columbia and the District of Kansas, see, e.g., In the Matter of the Search of Information Associated with [redacted] @mac.com that is Stored at Premises Controlled by Apple, Inc., 2014 WL 1377793 (D.D.C. April 7, 2014) ("D.C. Opinion"); In the Matter of Applications for Search Warrants for Information Associated with Target Email Accounts/Skype Accounts, 2013 WL 4647554 (D. Kan. Aug. 27, 2013) ("Kansas Opinion") — we write to explain why we issued the warrant here.

I. BACKGROUND

As part of its investigation into possible violations of 31 U.S.C. §§ 5330 and 5322 (unlawful money remitting) and 18 U.S.C. §§ 371 (conspiracy to commit unlawful money remitting) and 1956 (conspiracy to commit money laundering), the Government brought an application for a search warrant seeking records relating to a "Gmail" email address, which is maintained and controlled by Google. The application includes an affidavit from an agent of the

Federal Bureau of Investigation that describes the Government's investigation and provides probable cause to believe that the target of the Government's investigation has been using the subject email account to engage in criminal activity. The affidavit also provides probable cause to believe that emails and other information in that account will provide evidence of those criminal activities. Because the investigation is ongoing and the warrant and application are sealed, this Memorandum Opinion will not provide any further information regarding the probable cause showing.

The search warrant directs Google to provide to the Government "all content and other information within the Provider's possession, custody, or control associated with" the email account, including all emails sent, received, or stored in draft form, all address book information, and a variety of other information associated with the account. The search warrant provides that law enforcement personnel "are authorized to review the records produced by the Provider in order to locate" certain specific categories of evidence described in the warrant. The warrant does not contain any search protocol and does not limit the amount of time the Government may take to review the account material disclosed by Google. The warrant also does not provide for any destruction of the material disclosed once the emails within the categories listed in the warrant are identified.

II. APPLICABLE LAW

A. The Stored Communications Act

The Government's application as well as Google's obligation to disclose the emails and related information are governed by the Stored Communications Act of 1986, 18 U.S.C. §§ 2701-2712. Section 2703 of that statute authorizes the Government to obtain the "contents" of an "electronic communication" that is in "electronic storage" or held by a "provider of remote

computing service" — such as emails — pursuant to a search warrant under the Federal Rules of Criminal Procedure. See 18 U.S.C. §§ 2703(a), 2703(b)(1)(A).[1]

B. The Fourth Amendment to the United States Constitution

The Fourth Amendment of the United States Constitution provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be 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. The Supreme Court has held that the "essential purpose of the Fourth Amendment is to shield the citizen from unwarranted intrusions into his privacy" and that "[t]his purpose is realized by Rule 41 of the Federal Rules of Criminal Procedure . . . which implements the Fourth Amendment . . . . " Jones v. United States, 357 U.S. 493, 498 (1958). "The Fourth Amendment was a response to the English Crown's use of general warrants, which often allowed royal officials to search and seize whatever and whomever they pleased while investigating crimes or affronts to the Crown." Ashcroft v. al-Kidd, 131 S. Ct. 2074, 2084 (2011); accord United States v. Galpin, 720 F.3d 436, 445 (2d Cir. 2013). "To achieve its goal, the Warrants

---

[1] As the Judge Francis of this district has noted:

> Although [the Stored Communications Act] uses the term "warrant" and refers to the use of warrant procedures, the resulting order is not a conventional warrant; rather, the order is a hybrid: part search warrant and part subpoena. It is obtained like a search warrant when an application is made to a neutral magistrate who issues the order only upon a showing of probable cause. On the other hand, it is executed like a subpoena in that it is served on the [Internet Service Provider] in possession of the information and does not involve government agents entering the premises of the [Internet Service Provider] to search its servers and seize the e-mail account in question.

In the Matter of a Warrant to Search a Certain E–mail Account Controlled and Maintained by Microsoft Corporation., 2014 WL 1661004, at *5 (S.D.N.Y. April 25, 2014).

Clause requires particularity and forbids overbreadth." United States v. Cioffi, 668 F. Supp. 2d 385, 390 (E.D.N.Y. 2009); accord United States v. Zemlyansky, 945 F. Supp. 2d 438, 450 (S.D.N.Y. 2013). "Particularity is the requirement that the warrant must clearly state what is sought. Breadth deals with the requirement that the scope of the warrant be limited to the probable cause on which the warrant is based." United States v. Hill, 459 F.3d 966, 973 (9th Cir. 2006) (citation omitted). "In determining whether a warrant is overbroad, courts must focus on whether there exists probable cause to support the breadth of the search that was authorized." Zemlyansky, 945 F. Supp. 2d at 464 (citation and quotation marks omitted).

As the Supreme Court has repeatedly held, "the ultimate touchstone of the Fourth Amendment is 'reasonableness.'" Brigham City v. Stuart, 547 U.S. 398, 403 (2006); accord Riley v. California, – U.S. – , 2014 WL 2864483, at *6 (U.S. June 25, 2014); Ohio v. Robinette, 519 U.S. 33, 39 (1996). Thus, the "manner in which the government executes [a] warrant must comport with the Fourth Amendment's reasonableness standard." United States v. Metter, 860 F. Supp. 2d 205, 212 (E.D.N.Y. 2012) (citation omitted); accord Hill, 459 F.3d at 978.

III. DISCUSSION

In addition to the D.C. Opinion and the Kansas Opinion previously cited, the Court is aware of other decisions emanating from these courts that have denied applications for warrants authorizing searches of email accounts.[2] We address in this Memorandum Opinion two issues

[2] See, e g., In the Matter of the Search of Information Associated with [redacted] @mac.com that is Stored at Premises Controlled by Apple, Inc., 2014 WL 945563 (D.D.C. March 7, 2014) ("March 7 Opinion"); In the Matter of the Search of Information Associated with [Redacted] @mac.com that is Stored at Premises Controlled by Apple, Inc., 2014 WL 1759576 (D.D.C. March 7, 2014); In the Matter of Applications for Search Warrants for Case Nos. 12-MJ-8119-DJW and Information Associated with 12-MJ-8191-DJW Target Email Address, 2012 WL 4383917 (D. Kan. Sept. 21, 2012). In addition, an unpublished decision from the Northern District of California denied a warrant in part on the ground that the Government

that were central to the results reached in these cases. First, is it appropriate to issue a search warrant that allows the Government to obtain all emails in an account even though there is no probable cause to believe that the email account consists exclusively of emails that are within the categories of items to be seized under the search warrant? As a subsidiary issue, we will also consider whether we may in the alternative require the email host — in this case, Google — to conduct a review of the emails and provide to the Government only those emails responsive to categories listed in the warrant. Second, assuming we permit delivery of the entire email account to the Government, should the Court require that the Government follow certain protocols — whether as to length of search, manner of search, or length of retention of the emails — as a condition of obtaining the search warrant?

A. Whether Google Should Be Directed to Produce All the Emails Associated with the Email Account

The D.C. Opinion refused to issue a warrant requiring disclosure of the entire contents of an email account on the ground that the Government will "actually seize large quantities of e-mails for which it has not established probable cause . . . . " 2014 WL 1377793, at *5 (emphasis omitted). As the D.C. Opinion put it:

---

had not made a "commitment to return or destroy evidence that is not relevant to its investigation." See In re:[REDACTED]@gmail.com, No. 14-70655 (PSG) (N.D. Cal. May 9, 2014), at 6.

Other recent cases have denied search warrant applications for electronic devices that rely on the same reasoning as has been articulated in the cases involving email accounts. See, e.g., In re Nextel Cellular Telephone, 2014 WL 2898262 (D. Kan. June 26, 2014); In the Matter of the Search of ODYX LOOX Plus Tablet, 2014 WL 1063996 (D.D.C. March 20, 2014). In In re U.S.'s Application For A Search Warrant To Seize and Search Electronic Devices From Edward Cunnius, 770 F. Supp. 2d 1138, 1139 (W.D. Wash. 2011), a court denied a search warrant of electronic devices based on the Government's failure to provide for review of the electronic evidence by a "filter team" and forswear reliance on the plain view doctrine.

> Here, the warrant describes only certain emails that are to be seized — and the government has only established probable cause for those emails. Yet it seeks to seize all e-mails by having them "disclosed" by [the email host]. This is unconstitutional because "[t]he government simply has not shown probable cause to search the contents of all emails ever sent to or from the account."

Id. (quoting In re Search of Target Email Address, 2012 WL 4383917, at *9 (D. Kan. Sept. 21, 2012)). The Kansas Opinion similarly criticized the warrant sought in that case on the ground that it required an email host to disclose "all email communications in their entirety" and "fail[ed] to limit the universe of electronic communications and information to be turned over to the government to the specific crimes being investigated." 2013 WL 4647554, at *8.

The D.C. Opinion's characterization of the Government's application as an improper "seizure" of documents for which it had not shown probable cause cites to Coolidge v. New Hampshire, 403 U.S. 443 (1971). Coolidge, in a discussion of the "plain view" exception to the search warrant requirement, noted that the warrant requirement serves to ensure that "those searches deemed necessary should be as limited as possible," id. at 467. Coolidge referred to the history of "general warrants" in colonial times, and stated that "the problem is not that of intrusion per se, but of a general, exploratory rummaging in a person's belongings." Id. As the Supreme Court later explained:

> The general warrant specified only an offense — typically seditious libel — and left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched. Similarly, the writs of assistance used in the Colonies noted only the object of the search — any uncustomed goods — and thus left customs officials completely free to search any place where they believed such goods might be. The central objectionable feature of both warrants was that they provided no judicial check on the determination of the executing officials that the evidence available justified an intrusion into any particular home.

Steagald v. United States, 451 U.S. 204, 220 (1981).

In the D.C. Opinion's view, "any e-mails that are turned over to the government are

unquestionably 'seized' within the meaning of the Fourth Amendment." 2014 WL 1377793, at *3. Thus, by making an application to "seize an entire e-mail account even though it had only established probable cause for some of the e-mails," the Government was viewed in the D.C. Opinion as having asked the court "to issue a general warrant that would allow a general, exploratory rummaging in a person's belongings' – in this case an individual's email account." Id. (citing Coolidge, 403 U.S. at 467) (additional citation omitted).

This Court respectfully disagrees with the D.C. Opinion on this point because we believe it too narrowly construes the Fourth Amendment's particularity requirement and is contrary to copious precedent. As an initial matter, we note that "[a]mple case authority sanctions some perusal, generally fairly brief, of . . . documents (seized during an otherwise valid search) . . . in order for the police to perceive the relevance of the documents to crime." United States v. Mannino, 635 F.2d 110, 115 (2d Cir. 1980) (quoting United States v. Ochs, 595 F.2d 1247, 1257 n.8 (2d Cir. 1979)); accord Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976) ("In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized."). As the Second Circuit has noted, "allowing some latitude in this regard simply recognizes the reality that few people keep documents of their criminal transactions in a folder marked 'drug records.'" United States v. Riley, 906 F.2d 841, 845 (2d Cir. 1990). With respect to the execution of search warrants seeking physical evidence, courts "permit[] the government to examine paper documents that might otherwise fall outside the scope of a search warrant to make that determination, recognizing that different types of evidence present different tactical issues." Metter, 860 F. Supp. 2d at 213. In other words, courts have long recognized the practical need for law enforcement to exercise dominion over documents not within the scope of the warrant in

order to determine whether they fall within the warrant. Such exercise of dominion essentially amounts to a "seizure" even if the seizure takes place at the premises searched and is only temporary. See, e.g., United States v. Jones, 132 S. Ct. 945, 958 (2012) ("A seizure of property occurs when there is some meaningful interference with an individual's possessory interests in that property.") (quoting United States v. Jacobsen, 466 U.S. 109, 113 (1984) (internal quotation marks omitted)).

In the case of electronic evidence, which typically consists of enormous amounts of undifferentiated information and documents, courts have recognized that a search for documents or files responsive to a warrant cannot possibly be accomplished during an on-site search. Thus, "courts developed a more flexible approach to the execution of search warrants for electronic evidence, holding the government to a standard of reasonableness." Metter, 860 F. Supp. 2d at 214; accord United States v. Graziano, 558 F. Supp. 2d 304, 317 (E.D.N.Y. 2008) (courts have afforded law enforcement "leeway in searching computers for incriminating evidence within the scope of materials specified in the warrant") (citations omitted); United States v. Scarfo, 180 F. Supp. 2d 572, 578 (D.N.J. 2001) ("Where proof of wrongdoing depends upon documents . . . whose precise nature cannot be known in advance, law enforcement officers must be afforded the leeway to wade through a potential morass of information in the target location to find the particular evidence which is properly specified in the warrant."); see also United States. v. Ganias, – F.3d –, 2014 WL 2722618, at *7-*8 (2d Cir. June 17, 2014) ("[T]he ability of computers to store massive volumes of information presents logistical problems in the execution of search warrants.").

The need to permit the Government to examine electronic materials off-site rather than require it to conduct an on-site search is most obviously demonstrated in the case of a search of a

computer hard disk drive ("hard drive"), which is the part of a computer that actually stores files and documents. In the context of suppression motions, courts have routinely upheld the seizure or copying of hard drives and other storage devices in order to effectuate a proper search for the categories of documents or files listed in a warrant. See, e.g., United States v. Schesso, 730 F.3d 1040, 1046 (9th Cir. 2013) (the challenge of "searching for digital data that was not limited to a specific, known file or set of files" and the inability to "know[] which or how many illicit files there might be or where they might be stored, or of describing the items to be seized in a more precise manner" justified "seizure and subsequent off-premises search of [defendant's] entire computer system and associated digital storage devices"); United States v. Evers, 669 F.3d 645, 652 (6th Cir. 2012) ("The federal courts are in agreement that a warrant authorizing the seizure of a defendant's home computer equipment and digital media for a subsequent off-site electronic search is not unreasonable or overbroad, as long as the probable-cause showing in the warrant application and affidavit demonstrate a sufficient chance of finding some needles in the computer haystack.") (citations and quotation marks omitted); United States v. Stabile, 633 F.3d 219, 234 (3d Cir. 2011) (rejecting requirement of "on-site" search of hard drives because the "practical realities of computer investigations preclude on-site searches"); United States v. Grimmett, 439 F.3d 1263, 1269 (10th Cir. 2006) (upholding seizure and subsequent off-site search of computer in a "laboratory setting"); United States v. Hay, 231 F.3d 630, 637 (9th Cir. 2000) (upholding seizure and search of an "entire computer system and virtually every document in [the defendant's] possession without referencing child pornography or any particular offense conduct" because, although officers "knew that [a party] had sent 19 images [of child pornography] directly to [the defendant's] computer, [they] had no way of knowing where the images were stored"); United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999) ("As a

practical matter, the seizure and subsequent off-premises search of the computer and all available disks was about the narrowest definable search and seizure reasonably likely to obtain the images [of child pornography sought].”). In other words, the seizure or “off-site imaging” (that is, copying) of computer hard drives is “a necessity of the digital era.” Metter, 860 F. Supp. 2d at 214; accord United States v. Burns, 2008 WL 4542990, at *5 (N.D. Ill. April 29, 2008) (“Courts have found that seizure of computer equipment before search is reasonable given the complexities of electronic searches, as long as the requirements of the Fourth Amendment are met.”).

In addition, the Federal Rules of Criminal Procedure were amended in 2009 to specifically provide for such a procedure. As stated in that rule:

> A warrant under Rule 41(e)(2)(A) 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 information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

Fed. R. Crim. P. 41(e)(2)(B). The Advisory Committee notes to the 2009 amendments to Rule 41 explained the need for such a procedure:

> Computers and other electronic storage media commonly contain such large amounts of information that it is often impractical for law enforcement to review all of the information during execution of the warrant at the search location. This rule acknowledges the need for a two-step process: officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant.

The Second Circuit has recently recognized that “[i]n light of the significant burdens on-site review would place on both the individual and the Government, the creation of mirror images for offsite review is constitutionally permissible in most instances, even if wholesale removal of tangible papers would not be.” Ganias, 2014 WL 2722618, at *8. Thus, we view it

as well-established that a search warrant can properly permit the Government to obtain access to electronic information for purposes of a search even where the probable cause showing does not apply to the entirety of the electronic information that is disclosed to the Government.

We perceive no constitutionally significant difference between the searches of hard drives just discussed and searches of email accounts. Indeed, in many cases, the data in an email account will be less expansive than the information that is typically contained on a hard drive. Therefore, we believe the case law we have cited concerning searches of hard drives and other storage media supports the Government's ability to access an entire email account in order to conduct a search for emails within the limited categories contained in the warrant. Notably, every case of which we are aware that has entertained a suppression motion relating to the search of an email account — other than the D.C. Opinion, the Kansas Opinion and the cases cited in footnote 2 above — has upheld the Government's ability to obtain the entire contents of the email account to determine which particular emails come within the search warrant. See United States v. Bach, 310 F.3d 1063, 1065 (8th Cir. 2002) (upholding as constitutionally reasonable the seizure of "all of the information" from defendant's email account where the service provider did not "selectively choose or review the contents of the named account"); United States v. Ayache, 2014 WL 923340, at *2-3 (M.D. Tenn. March 10, 2014) (denying motion to suppress "seizure of all emails in a defendant's account [] where there was probable cause to believe that the email account contained evidence of a crime"); United States v. Deppish, 2014 WL 349735, at *6-7 & n.37 (D. Kan. Jan. 31, 2014) (noting that "nothing in § 2703 precludes the Government from requesting the full content of a specified email account," and concluding that such a search is not a "general search"); United States v. Taylor, 764 F. Supp. 2d 230, 232, 237 (D. Me. 2011) (upholding search of "all information associated with an identified Microsoft hotmail account");

United States v. Bowen, 689 F. Supp. 2d 675, 682 (S.D.N.Y. 2010) (Fourth Amendment does not require authorities to "ascertain which e-mails are relevant before copies are obtained from the internet service provider for subsequent searching"); United States v. McDarrah, 2006 WL 1997638, at *9-10 (S.D.N.Y. July 17, 2006) (denying motion to suppress seizure of "[a]ll stored electronic mail and other stored content information presently contained in" a specified email account), aff'd, 351 F. App'x 558 (2d Cir. 2009).[3]

The D.C. Opinion offered the Government the option of seeking a warrant that would have required the email host — in that case, Apple, Inc. — to itself conduct the search of emails. 2014 WL 1377793, at *6. There might be some force to requiring an email host to cull emails from an email account where a limitation in the scope of the items to be seized would allow the email host to produce responsive material in a manner devoid of the exercise of skill or discretion, for example, under a warrant requiring disclosure of all emails from a particular time period. But in the absence of such circumstances, it is unrealistic to believe that Google or any other email host could be expected to produce the materials responsive to categories listed in a search warrant. First, the burden on Google would be enormous because duplicating the Government's efforts might require it to examine every email. See, e.g., Hill, 459 F.3d at 978 ("There is no way to know what is in a file without examining its contents, just as there is no sure way of separating talcum from cocaine except by testing it."); Scarfo, 180 F. Supp. 2d at 578 (law enforcement may need to "wade through a potential morass of information in the target

[3] The court in Cioffi suppressed email evidence seized under a warrant issued pursuant to § 2703. But it did so because the "[t]he Warrant did not, on its face, limit the items to be seized from [defendant's] personal email account to emails containing evidence of the crimes charged in the indictment or, indeed, any crime at all. Nor did it attach and incorporate the Affidavit." 668 F. Supp. 2d at 396.

location to find the particular evidence which is properly specified in the warrant."); accord United States v. Fumo, 2007 WL 3232112 at *6 (E.D. Pa. Oct. 30, 2007) ("[I]n the case of documents on computers . . . relevant documents may be intermingled with irrelevant ones.").

Second, Google employees would not be able to interpret the significance of particular emails without having been trained in the substance of the investigation. Seemingly innocuous or commonplace messages could be the direct evidence of illegality the Government had hoped to uncover. While an agent steeped in the investigation could recognize the significance of particular language in emails, an employee of the email host would be incapable of doing so. The D.C. Court's suggestion to the contrary is seemingly premised on the notion that service providers are experienced in responding to subpoenas. See March 7 Opinion, 2014 WL 945563, at *6 ("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."). But the recipient of a subpoena typically searches only its own records, of which it is expected to have a full understanding of the source and content. It is not called upon to search another party's records. We note additionally that in instances where a grand jury has been convened, the Government might be prevented from providing relevant investigative information to the email host in light of the secrecy protections afforded grand jury information pursuant to Fed. R. Crim. P. 6(e)(2)(B).

Thus, the D.C. Opinion's proposal gives insufficient consideration to the difficulty of executing a search warrant for digital information and the likelihood that the Government's investigative efforts would be severely hampered by requiring that this crucial and complex investigative activity be performed by an email host. Placing the responsibility for performing these searches on the email host would also put the host's employees in the position of appearing

to act as agents of the Government vis-à-vis their customers. Moreover, it would allow private employees — who have no constitutional responsibilities to the public — to obtain personal information about a target of an investigation that they would otherwise have no occasion to see, and with no apparent limitation on their use of this information other than limitations imposed by their employer. Not surprisingly, courts have routinely rejected arguments made in the course of suppression motions that a warrant should have required a third party to conduct searches of electronic information. See, e.g., Deppish, 2014 WL 349735, at *6 ("[N]othing in the Fourth Amendment requires law enforcement to cede to non-law enforcement their power to search and determine which matters are subject to seizure."); Taylor, 764 F. Supp. 2d at 237 ("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.") (citations omitted); Bowen, 689 F. Supp. 2d at 682 ("[T]he Fourth Amendment [does not] require the executing authorities to delegate a pre-screening 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.") (citing United States v. Vilar, 2007 WL 1075041, at *35 (S.D.N.Y. April 4, 2007)). Thus, we conclude that the warrant properly required that Google deliver all emails in the account to the Government for the purpose of allowing the Government to search the emails for items within the categories specified in the warrant.

B. Whether the Court Should Require a Protocol For Conducting the Search of the Email Account or Limit the Length of Time the Emails Are Retained

Some courts issuing warrants for electronic information have included "secondary orders" imposing "minimization procedures" concerning the Government's handling and

retention of material disclosed by third-party custodians of electronic information. These orders have required that records not within the scope of the search warrant either be "returned" to the custodian or, in the case of copies, "destroyed." 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., 2013 WL 7856600, at *7 (D.D.C. Nov. 26, 2013) ("Facebook Opinion"); see also D.C. Opinion, 2014 WL 1377793, at *7 (noting that "[i]n September and December 2013, the Court modified approximately twenty warrants to specify that any data not within the scope of the warrant would be returned or, if copies, destroyed within a reasonable period of time"); Matter of Black iPhone 4, 2014 WL 1045812, at *5 (D.D.C. March 11, 2014) (denying application and stating that in any future application the "government must specify what will occur" with "data that is seized by the government and is outside the scope of the warrant"). Such orders are based on the concern that "the government will see no obstacle to simply keeping all of the data it collects, regardless of its relevance to the specific investigation for which it is sought and whether the warrant authorized its seizure." Facebook Opinion, 2013 WL 7856600, at *7.

"The general touchstone of reasonableness which governs Fourth Amendment analysis . . . governs the method of execution of the warrant." United States v. Ramirez, 523 U.S. 65, 71 (1998) (internal citation omitted). Thus, "[t]he off-site review of . . . mirror images [of electronic information] . . . is still subject to the rule of reasonableness." Ganias, 2014 WL 2722618, at *8 (citation omitted). Judging the reasonableness of the execution of a search ex ante, however, is not required by Supreme Court precedent. In Dalia v. United States, 441 U.S. 238 (1979), the Supreme Court held that the Warrant Clause of the Fourth Amendment does not require a court to "set forth precisely the procedures to be followed by the executing officers."

Id. at 258. Instead, Dalia held that "the manner in which a warrant is executed is subject to later judicial review as to its reasonableness." Id. More recently, the Supreme Court has repeated that "[n]othing in the language of the Constitution or in th[e] Court's decisions interpreting that language suggests that, in addition to the requirements set forth in the text [of the Fourth Amendment], search warrants also must include a specification of the precise manner in which they are to be executed." United States v. Grubbs, 547 U.S. 90, 97-98 (2006) (citation omitted; some bracketing in original). Thus, Grubbs held that the Constitution "interpos[es], ex ante, the deliberate, impartial judgment of a judicial officer" and provides "ex post, a right to suppress evidence improperly obtained and a cause of action for damages" for an unreasonable search. Id. at 99 (citation and quotation marks omitted); accord Warshak v. United States, 532 F.3d 521, 528 (6th Cir. 2008) (en banc) (in determining "reasonableness" of searches under the Fourth Amendment, "reviewing court looks at the claim . . . in the context of a developed factual record" because the Fourth Amendment "generally should be applied after [factual] circumstances unfold, not before") (vacating preliminary injunction against enforcement of 18 U.S.C. § 2703(d) without giving email user "prior notice and an opportunity to be heard" because a "pre-enforcement challenge to future e-mail searches" did not present a claim that was ripe for review).

The Second Circuit's recent decision in Ganias does not change our conclusion on this point. In that case, the Government executed a search warrant at the offices of an accountant that permitted it to obtain records of two corporate clients of the accountant. 2014 WL 2722618, at *1. The agents made forensic images of the hard drives of all three of the accountant's computers, which included files containing the accountant's "personal financial records" — records that were beyond the scope of the warrant. Id. An agent executing the warrant on

November 19, 2003, "assured" the accountant that any computer files unrelated to the investigation "would be purged once [the Government] completed [its] search" for relevant files. Id. The Government had segregated the accountant's personal financial records by December 2004 but never kept its promise to purge or delete these non-responsive files. Id., at *2, *9. In late 2004, the Government began to suspect that the accountant was personally involved in criminal activity. Id., at *2. The Government then obtained a second warrant on April 24, 2006, to search the defendant's personal financial records, images of which had remained in the Government's possession pursuant to the first warrant. Id., at *3. At the time the Government secured the second warrant, however, the images of the personal financial records "had been in the Government's possession for almost two-and-a-half years" and "would not have existed but for the Government's retention of those images" because the accountant had altered the original files in the meantime. Id. The Second Circuit noted that while "wholesale removal" of "intermingled computer records" may be permissible where off-site sorting is "necessary and reasonable," "this accommodation does not somehow authorize the Government to retain all non-responsive documents indefinitely, for possible use in future criminal investigations." Id., at *12 (citation omitted). Although the Second Circuit stated that it was constitutionally unreasonable for the Government to "seize and indefinitely retain every file on [defendant's] computer for use in future criminal investigations," id., at *10, nothing in its opinion suggests that a magistrate judge approving a warrant application must or should impose ex ante restrictions pertaining to the later execution of that warrant. As a result, we read Ganias as consistent with the principles announced in the Supreme Court's decisions in Dalia and Grubbs

concerning the need to include restrictions on the execution of a warrant.[4]

If the Government acts improperly in its retention of the materials, our judicial system provides remedies, including suppression and an action for damages as noted in Grubbs, 547 U.S. at 99. Additionally, any person "aggrieved" by any unlawful "deprivation of property" may move for the property's "return" pursuant to Fed. R. Civ. P. 41(g). As the Ninth Circuit has noted, Rule 41(g) "contemplate[s] that district judges may order the return of . . . any copies [] of seized evidence." United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1174 (9th Cir. 2010). The Advisory Committee notes to Rule 41(g) contemplate not only the return but also the destruction of "copies of records." See Fed. R. Crim. P. 41 advisory committee's note (1989 amendments) ("In some circumstances . . . equitable considerations might justify an order requiring the government to return or destroy all copies of records that it has seized."). Thus, if the Government has retained its copy of emails beyond a constitutionally reasonable period, Rule 41(g) would likely provide a remedy in addition to suppression and a civil damages suit once the owner of the electronic information has notice of the seizure.[5]

---

[4] Although not raised in Ganias, we note also that the retention of electronic evidence is supported by the text of Fed. R. Crim. P. 41 insofar as it discusses the inventory of property seized pursuant to a warrant. With respect to electronic evidence, the rule states:

> In a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically stored information that was seized or copied.

Fed. R. Crim. P. 41(f)(1)(B) (emphasis added). From context, it is clear that the electronically stored information at issue refers to "the entire storage medium" seized as part of the two-step procedure, as described in the 2009 Advisory Committee notes to Subdivision (e)(2).

[5] The Court in Ganias found that a Rule 41(g) motion would have been ineffective in that case because the Government had contended that the files at issue "could not feasibly have been returned or purged anyway." Ganias, 2014 WL 2722618, at *12. We do not believe, however,

We will assume, without deciding, that this Court has the power to impose limitations on retention at the time an email warrant application is approved.[6] But we did not impose them here because we recognize that the Government has a need to retain materials as an investigation unfolds for the purpose of retrieving material that is authorized by the warrant. For example, in a drug investigation, it might be obvious based on information from an informant or other source that emails referring to the purchase or importation of "dolls" refers to cocaine, but investigators might only learn as the investigation unfolds that a seemingly innocuous email referring to purchase of "potatoes" also refers to a cocaine shipment. As one court noted in denying a suppression motion in a case involving the search of electronic information, including an email account:

> [Law enforcement agents] did not cull the information down using key word searches because, in [a law enforcement agent's] experience, people sometimes use coded language to hide illegal activities, and it is difficult at the beginning of an investigation to know about any coded language persons might be using. Without knowledge of the coded language being used, it is often not feasible to use search terms to capture all files responsive to the warrants. . . .
>
> The Government's knowledge of the activity being investigated developed over time. As the Government learned new details, the Government would go back and conduct targeted searches in the Relativity database using search terms for additional documents responsive to the warrants. From time to time, and based

---

that this circumstance would arise in all cases and thus there may be instances when the Government could destroy segregable records.

[6] One commentator has argued that ex ante restrictions in a warrant of any kind are constitutionally impermissible, are not actually enforced in suppression motions, and are in any event ineffective in protecting Fourth Amendment rights. See Orin S. Kerr, Ex Ante Regulation of Computer Search and Seizure, 96 Va. L. Rev. 1241 (2010); but see Paul Ohm, Massive Hard Drives, General Warrants, and the Power of Magistrate Judges, 97 Va. L. Rev. In Brief 1 (2011) (arguing that ex ante restrictions may be necessary in searches of electronic evidence to ensure that the Fourth Amendment's particularity and probable cause requirements are met). We need not reach the question of a court's power to impose such restrictions, however, because we conclude that such restrictions were not appropriate for the warrant at issue here.

> on developing knowledge of the investigation, documents that were previously marked as irrelevant were re-reviewed and marked as relevant.

United States v. Lustyik, 2014 WL 1494019, at *5 (D. Utah April 16, 2014). Moreover, as the Advisory Committee notes to Rule 41 put it, "to arbitrarily set a presumptive time period" for the return of the materials "could result in frequent petitions to the court for additional time." See Fed. R. Crim. P. 41 advisory committee's note (2009 amendments). This is not a case — as is sometimes true for seized computer equipment that has not been imaged — where the seizure has created practical impediments to an individual's exclusive possession of the data that creates a need to conduct a search promptly so that non-responsive materials may be returned.

Additionally, it may be necessary for the Government to maintain a complete copy of the electronic information to authenticate evidence responsive to the warrant for purposes of trial.[7] For these reasons, we declined to impose a deadline on the Government's retention of the materials, believing that the remedies available to curb any improper retention — including suppression, a civil damages action, and a motion under Rule 41(g) as described above — are appropriate and adequate. See generally Metter, 860 F. Supp. 2d at 214-15 (suppressing evidence based on the Government's 15-month delay in reviewing electronic evidence it had seized).

As for whether the Court should give direction as to the manner in which the Government conducts the search of the emails, we will again assume without deciding that a court has the power to include protocols in a warrant as to the type of search to be conducted.

---

[7] While Ganias expressed skepticism about the need for retaining non-responsive files for this purpose, it was willing to "assume" the need existed and stated that in such an event, the retained material should not be used "for any other purpose" — presumably referring to the material's use in that case as the basis for a second warrant. 2014 WL 2722618, at *11.

See, e.g., United States v. Cartier, 543 F.3d 442, 447-48 (8th Cir. 2008) (acknowledging that "there may be times that a search methodology or strategy may be useful or necessary"). But as we have already noted, Grubbs teaches that "[n]othing in the language of the Constitution or in th[e] [Supreme] Court's decisions interpreting that language suggests that, in addition to the requirements set forth in the text [of the Fourth Amendment], search warrants also must include a specification of the precise manner in which they are to be executed." 547 U.S. at 97-98. Not surprisingly, in the context of computer searches, such direction is routinely held not to be required. See, e.g., United States v. Richards, 659 F.3d 527, 538 (6th Cir. 2011) ("[G]iven the unique problem encountered in computer searches, and the practical difficulties inherent in implementing universal search methodologies, the majority of federal courts have eschewed the use of a specific search protocol and, instead, have employed the Fourth Amendment's bedrock principle of reasonableness on a case-by-case basis.") (citations omitted); United States v. Khanani, 502 F.3d 1281, 1290 (11th Cir. 2007) (rejecting argument that "the lack of a written 'search protocol' required the district court to suppress all evidence agents seized as a result of the search of the defendants' computers"); United States v. Brooks, 427 F.3d 1246, 1251 (10th Cir. 2005) ("This court has never required warrants to contain a particularized computer search strategy."); United States v. Roberts, 2010 WL 234719, at *16–17 (E.D. Tenn. Jan. 14, 2010) (collecting cases); Graziano, 558 F. Supp. 2d at 315–16 (collecting cases).

Courts have also noted the impracticalities of including limitations on the mechanics or timing of a search of electronic information. See, e.g., United States v. Burgess, 576 F.3d 1078, 1094 (10th Cir. 2009) ("[I]t is folly for a search warrant to attempt to structure the mechanics of the search and a warrant imposing such limits would unduly restrict legitimate search objectives."). As one district court noted:

> "[I]n most instances, there is no way for law enforcement or the courts to know in advance how a criminal may label or code his computer files and/or documents which contain evidence of criminal activities." United States v. Graziano, 558 F. Supp. 2d 304, 315 (E.D.N.Y. 2008). To limit the government's computer search methodology ex ante would "give criminals the ability to evade law enforcement scrutiny simply by utilizing coded terms in their files or documents" or other creative data concealment techniques. Id. Accordingly, we join the Graziano court and several other federal courts in holding that the Fourth Amendment does not require a search warrant to specify computer search methodology.

Bowen, 689 F. Supp. 2d at 681(citation omitted). Our inability to predict the best mechanism for conducting a search strongly counsels against including any search protocol in a warrant.

We are aware of the case of In re Search Warrant, 193 Vt. 51 (2012), in which a Vermont state court magistrate issued a warrant that contained certain restrictions on the search protocol that law enforcement was to follow in conducting the search of electronic information on a computer. The Supreme Court of Vermont upheld the restrictions but made clear that the issue before it was "whether the warrant-issuing magistrate had the authority to issue the specific search instructions he did" — not "whether imposing the instructions is necessary to comply with the Fourth Amendment or . . . the Vermont Constitution." Id. at 64; see also id. at 65 ("WE ALSO EMPHASIZE that the general question is one of authority, and not responsibility. No party or amicus is directly claiming that ex ante instructions are ever required, and we certainly do not hold so here.") (capitalization in original). We are also aware of Preventive Medicine Assocs., Inc. v. Commonwealth, 465 Mass. 810 (2013), in which a Massachusetts court mandated a search protocol for a warrant. But that warrant was issued post-indictment and the protocol was issued because there was a serious risk that the electronic information sought would contain privileged communications. Id. at 823.

While it is possible that in some circumstances "ex ante instructions may be a way to ensure particularity," as the Vermont Supreme Court put it, In re Search Warrant, 193 Vt. at 69,

we do not believe that such instructions were necessary to ensure particularity here. Accordingly, we did not place any limits on the manner or time frame in which the emails should be searched or retained. We believe that court processes available following the execution of a warrant, such as a suppression motion, a motion under Rule 41(g), and the availability of civil actions for damages, provide the appropriate mechanisms for an individual to challenge the Government's execution of a warrant. They also provide strong incentives for the Government to treat the electronic information in a manner that complies with the Fourth Amendment.

Dated: July 18, 2014
New York, New York

_____
GABRIEL W. GORENSTEIN
United States Magistrate Judge