IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF KANSAS

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH EMAIL ADDRESSES STORED AT PREMISES CONTROLLED BY THE MICROSOFT CORPORATION	)	**Case No. 16-MJ-8036**

MEMORANDUM AND ORDER

On March 4, 2016, the government submitted to Magistrate Judge David J. Waxse an Application and Affidavit in Support of a Search Warrant to search three email accounts hosted by Microsoft ("Hotmail Accounts"). The government suspects these Hotmail Accounts are being used to further criminal activity. On March 29, 2016, Judge Waxse issued a Memorandum and Order Denying Application for Search Warrant (the "Order") (Doc. 2).

In denying the government's application, Judge Waxse concluded the warrant did not meet the probable cause and particularity requirements of the Fourth Amendment to the United States Constitution and that requests for the entirety of an individual's email account too closely resembled a general search. Judge Waxse, however, suggested these concerns could be remedied with "court-issued *ex ante* instructions" and advised the government to resubmit its application including either "a search protocol that addresses the concerns expressed in this opinion" or one of the other *ex ante* limitations recommended in the Order. Judge Waxse also expressed concern as to whether or not there was sufficient probable cause to include four individuals/identifiers in the warrant application. The government now seeks review of the Order, arguing that Judge Waxse's decision is clearly erroneous and contrary to existing law. For the reasons set forth below, the court both overrules and affirms Judge Waxse's decision and declines to grant the government's warrant in its current form.

I. Procedural History

As part of its investigation into possible violations of 18 U.S.C. §§ 371 (conspiracy), 1029 (access device fraud), 1030 (computer intrusion), 1343 (wire fraud), and 2319 (copyright infringement), the government applied for a search warrant seeking records related to three Hotmail Accounts. The government requested the Hotmail Account records from the email provider, Microsoft ("the Provider"), under 18 U.S.C. § 2703, also known as the Stored Communications Act ("SCA"). Pursuant to the warrant application, the Provider was required to disclose content from the three Hotmail Accounts including:

> The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, deleted emails, archived emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email, as well as the entirety of header information for each email;
>
> 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 with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
>
> The types of service utilized and/or associated with this account to include all identifiers for these services and any connection logs associated with the usage of these services;
>
> 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; and
>
> All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

Once the information was obtained from the Provider, the warrant application sought authorization for "government-authorized persons" to review the records to seize items that:

> constitute fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. §§ 371 (conspiracy), 1029 (access device fraud), 1030 (computer intrusion), 1343 (wire

fraud), and 2319 (copyright infringement), those violations involving [redacted],[1] and others known and unknown, and occurring since September 7, 2008, including, for each account or identifier listed above, information pertaining to the following matters:

a. Evidence of the scanning or theft of intellectual property to include copyright-protected material and those bearing trademarks;

b. Evidence of using access drive(s) to fraudulently obtain intellectual property;

c. Evidence of developing, using, or distributing tools or code to circumvent copy controls associated with intellectual property;

d. Evidence of developing, using, or distributing software, code, or script as part of a "man-in-the-middle" computer intrusion;

e. Evidence 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;

f. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

g. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s);

h. The identity of the person(s) who communicated with the user ID about matters relating to the scanning or theft of intellectual property, or the various means to steal the intellectual property such as access device fraud, computer intrusion, or circumventing copy controls, including records that help reveal their whereabouts.

As part of its application, the government included an affidavit outlining the suspected criminal activity and the reasons why the specific Hotmail Accounts were under investigation.

After reviewing the application, Judge Waxse issued a Memorandum And Order Denying Application for Search Warrant (Doc. 2). In issuing his decision, Judge Waxse focused on the origins of the Fourth Amendment and the Framers' intent to prevent general searches. Judge Waxse noted the Fourth Amendment's particularity clause was included to prevent general searches and to enable the

[1] This court has redacted sensitive information and will provide the redacted information to the government upon request.

court to "ensure 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.* at 8 (quoting *Maryland v. Garrison*, 489 U.S. 79, 84 (1987)).

In deciding whether the present warrant met the Fourth Amendment particularity requirements, Judge Waxse first acknowledged that little case law existed regarding the government's attempt to seize and search the entire contents of an individual email account. He noted that in the few cases that did exist, courts often found warrants for the entirety of an email account were not overly broad. Judge Waxse, however, expressed his disagreement with such decisions, believing these courts had not fully considered an individual's right to privacy in the contents of their email accounts.

After establishing a right to privacy in one's email, Judge Waxse found the most reasonable approach to considering the government's application to search the entirety of these Hotmail Accounts was to utilize a balancing test, weighing equally "the individual's right to privacy against the government's ability to prosecute suspected criminals effectively." *Id.* at 16. He reviewed the present application by separating it into two parts based on Rule 41 of the Federal Rules of Criminal Procedure: the place to be searched and the things to be seized.

Judge Waxse began by reviewing whether the warrant was sufficiently particular in the things to be seized, or, the evidence the government sought to retain during its search of the contents of the Hotmail Accounts. He found that, although the government established probable cause to seize information related to violations of the specific statutes or to certain individuals/identifiers named, the government had not established probable cause to seize any non-responsive information it received from the Provider. Judge Waxse expressed concern that in searching the vast amount of information that may be found in the entirety of an email account, the government may be exposed to far more information than it needs for its investigation, thus violating the individual's privacy. Importantly, he

also found the government had not established probable cause as to four of the individuals/identifiers listed in the warrant application—[redacted]—and that including the phrase "and others known and unknown" was not sufficiently particular.

As for the place to be searched, Judge Waxse expressed concerns regarding whether the contents of an individual's email account met the Fourth Amendment's particularity requirement. He found that although the government identified a specific place to be searched—the individual email account—the disclosure of the entirety of that account may allow the government to view, and potentially use, information for which it did not have probable cause. Judge Waxse, however, noted that although an entire email account was not a sufficiently particular description of the place to be searched, the government could remedy this by providing a search protocol "explaining to the Court how it intends [to] search the overseized-[electronically stored information, or "ESI"] and what it will do with the non-responsive data once the search has been completed." *Id.* at 37.

In addition to the search protocols, Judge Waxse also suggested a variety of other *ex ante* instructions[2] for the government to consider that would bring the warrant within the allowed parameters of the Fourth Amendment. He noted "in its previous email opinions, the Court left the suggestion of *ex ante* instructions—or as it referred to them then, 'appropriate procedural safeguard(s)'—up to the government, but the government has yet to suggest any." *Id.* at 39. Judge Waxse then proposed some "*ex ante* instruction options" including: categorical or keyword limitations, search protocol, third party search of ESI (special masters, filter teams, or court-appointed experts), and use restrictions—returning or destroying non-responsive data. Importantly, Judge Waxse did not actually impose any of these *ex ante* instructions, but rather presented them to the government as options that may remedy some of the particularity concerns he had with the warrant in its current form.

[2] Judge Waxse defines *ex ante* instructions as "a set of instructions—which may contain conditions, limitations, restrictions, or guidelines—given before the warrant is approved but which govern the warrant should it be approved." (Doc. 2, at 4.)

In denying the warrant, Judge Waxse stated, "[i]f the Court were to authorize this warrant, it would be contradicting the manifest purpose of the Fourth Amendment's particularity requirement, which is to prevent general searches." *Id.* at 48. He concluded that because of the substantial amount of data in an individual email account, the balancing test swung too far in favor of the government. He noted, however, that the government "may resubmit its Application for consideration once it includes a search protocol that addresses the concerns expressed in this opinion or agrees to one of the other *ex ante* instructions." *Id*. at 49.

The government filed a Motion to Review Denial of Search Warrant in accordance with D. Kan. Rule 72.1.4(e) (Doc. 4). As part of its motion, the government submitted an amended application/affidavit, noting "[t]he government acknowledges that it failed to discuss [the individuals/identifiers to which Judge Waxse found no probable cause] in the application/affidavit; accordingly, the facts supporting their conclusion in the proposed warrant have been added to the attached Application/Affidavit." *Id.* at n 2.

In its Motion to Review, the government asks this court to find the warrant application complies with the particularity and probable cause requirements of the Fourth Amendment and to grant the proposed warrant without any of the *ex ante* instructions proposed by Judge Waxse. The government argues the proposed warrant was sufficiently particular and did not authorize a general search and that the government has the discretion to determine how to execute the warrant, thus making any *ex ante* instructions unreasonable.

II. Standard of Review

Under the Federal Magistrates Act, 28 U.S.C. § 631, *et seq.*, magistrate judges have the authority to decide pretrial, non-dispositive matters. 28 U.S.C. § 636(b)(1)(A). Included within this pretrial authority is the issuance of search warrants. *See Gomez v. United States*, 490 U.S. 858, 868

n.16 (1989). Pursuant to the Federal Magistrates Act, "a judge of the court may reconsider any pretrial matter . . . where it has been shown that the magistrate judge's order is clearly erroneous or contrary to law." 28 U.S.C. § 636(b)(1)(A).[3]

Our local rules instruct parties to follow Rule 72(a) of the Federal Rules of Civil Procedure when filing objections to a magistrate judge's pretrial, non-dispositive matter. *See* D. Kan. Rule 72.1.4(e). Under Rule 72(a), a district court "must consider timely objections and modify or set aside" any part of a magistrate judge's order on a non-dispositive pretrial matter that is "clearly erroneous or is contrary to law." Thus, because an application for a search warrant is a non-dispositive, pretrial matter, this court will review Judge Waxse's order under the clearly erroneous or contrary to law standard.

A district court must defer to a magistrate judge's ruling on a non-dispositive order unless it was clearly erroneous or contrary to law. *Allen v. Sybase, Inc.*, 468 F.3d 642, 658 (10th Cir. 2006); *see also Ocelot Oil Corp. v. Sparrow Industries*, 847 F.2d 1458, 1464 (10th Cir. 1988) (noting that under the clearly erroneous standard, unlike de novo review, the magistrate judge is accorded considerable deference.). Under the clearly erroneous standard, "the reviewing court must affirm unless it on the entire evidence is left with the definite and firm conviction that a mistake has been committed." *Id.* This standard should be applied to those factual findings made by the magistrate judge. *See* § 3069 Practice and Procedure with Regard to Nondispositive Matters, 12 Fed. Prac. & Proc. Civ. § 3069 (2d

[3] Under 28 U.S.C. § 636(b)(1), a district court's standard of review of a magistrate judge's decision depends on whether the decision is on a dispositive or non-dispositive motion. Under 28 U.S.C. § 636(b)(1)(A), a magistrate judge may "hear and determine any pretrial matter pending before the court." Exempted from this provision are eight categories of dispositive pretrial motions. *See Gomez*, 49 U.S. at 868. These include: a motion for injunctive relief, for judgment on the pleadings, for summary judgment, to dismiss or quash an indictment or information made by the defendant, to suppress evidence in a criminal case, to dismiss or to permit maintenance of a class action, to dismiss for failure to state a claim upon which relief can be granted, and to involuntarily dismiss an action. 28 U.S.C. § 636(b)(1)(A). Under 28 U.S.C. § 636(b)(1)(B), for any of the dispositive pretrial motions listed in § 636(b)(1)(A), a magistrate judge only has the authority to conduct evidentiary hearings and submit to a judge of the court proposed findings of fact and recommendations for the disposition by a judge of the court. A judge of the court may review de novo those proposed findings and recommendations on dispositive motions and may "accept, reject, or modify" the findings and also "receive further evidence or recommit the matters" to the magistrate with instructions.

ed.). By contrast, the contrary to law standard permits "plenary review as to matters of law." *Id.; see also Garcia v. Benjamin Group Enter. Inc.*, 800 F. Supp. 2d 399 (E.D.N.Y. 2011) (noting "under the contrary to law standard of review, a district court may reverse a finding only if it finds that the magistrate "failed to apply or misapplied relevant statutes, case law or rules of procedure").

III. Legal Standards

A. Fourth Amendment

The Fourth Amendment was included in the United States Constitution "partly to protect against the abuses of general warrants that had occurred in England . . . ." *Steagald v. United States*, 451 U.S. 204, 220 (1981). The Fourth Amendment 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 ultimate measure of whether government action is constitutional under the Fourth Amendment is reasonableness. *See Riley v. California*, 134 S. Ct. 2473, 2482 (2014). When government officials undertake a search to uncover evidence of criminal wrongdoing, "reasonableness generally requires the obtaining of a judicial warrant." *Id.* Under the Fourth Amendment, a warrant must: (1) be issued by a neutral, disinterested magistrate; (2) be supported by probable cause to believe "that the evidence sought will aid in a particular apprehension or conviction for a particular offense"; and (3) describe with particularity the things to be seized and the place to be searched. *See Dalia v. United States*, 441 U.S. 238, 255 (1979).

The "manifest purpose" of the particularity requirement within the Fourth Amendment is to prevent general searches. *Garrison*, 480 U.S. at 84. General warrants are those which are "left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched." *Steagald*, 451 U.S. at 220. By limiting the authorization to search to only

the places and things for which probable cause has been established, the particularity requirement "ensures 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." *Garrison*, 480 U.S. at 84.

The purpose of the particularity requirement, however, is not limited to simply the prevention of general searches. *Groh v. Ramirez*, 540 U.S. 551, 561 (2004). The particularity requirement also "assures the individual whose property is searched or seized of lawful authority of the executing officer, his need to search, and the limits of his power to search." *Id*. at 561–62.

To be sufficiently particular, a warrant must contain "sufficiently particularized language that creates a nexus between the suspected crime and the items to be seized." *Mink v. Knox*, 613 F.3d 995, 1010 (10th Cir. 2010). A warrant must state with specificity what is to be taken so that "nothing is left to the discretion of the officer executing the warrant." *Id.* As for the place to be searched, a warrant must "describe the premises with sufficient particularity so that the police can ascertain and identify the place to be searched." *United States v. Brakeman*, 475 F.3d 1206, 1211 (10th Cir. 2007) (noting when determining the adequacy of a warrant's description of the place to be searched, "practical accuracy rather than technical precision controls").

B. Stored Communications Act., 18 U.S.C. §§ 2701 *et seq.*

The government seeks authorization to obtain information from the Hotmail Accounts pursuant to the SCA, 18 U.S.C. § 2703. Under the SCA, the government may require an electronic communication service provider to disclose contents of an electronic communication that has been held in electronic storage for 180 days or less "only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . ." 18 U.S.C. § 2703(a). For electronic communications held for more than 180 days, the government may require a "provider of remote computing service" to disclose the requested electronic communications without notice to the

subscriber or customer if the government obtains a warrant pursuant to the Federal Rules of Criminal Procedure. *See* 18 U.S.C. § 2703(b)(1)(A).

C. Federal Rule of Criminal Procedure 41

Under the SCA, the government may only require disclosure of electronic communications if it does so pursuant to a warrant issued using the Federal Rules of Criminal Procedure. Rule 41 of the Federal Rules of Criminal Procedure governs searches and seizures. Rule 41(e)(2)(B) specifically addresses warrants seeking ESI and sets forth a two-step procedure for the search and seizure of such evidence. Rule 41(e)(2)(B) first authorizes "the seizure of electronic storage media or the seizure or copying of electronically stored information." Once the information has been seized, the rule then allows for a "later review of the media or information consistent with the warrant." The Advisory Committee Notes discuss the need for the two-step procedure for ESI, noting "computers and other electronic storage media commonly contain such large amount 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 . . . 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." Fed. R. Crim. P. 41(e)(2) advisory committee's note. The rule was designed to cover "all current types of computer-based information and to encompass future changes and developments." *Id*. Importantly, the Advisory Committee also notes, "[t]he amended rule does not address the specificity of description that the Fourth Amendment may require in a warrant for electronically stored information, leaving the application of this and other constitutional standards concerning both the seizure and the search to ongoing case law development." *Id.*

IV. Analysis

Taking into consideration the government's application, Judge Waxse's order, and the relevant legal standards, this court will determine whether Judge Waxse's decision to deny the application was clearly erroneous or contrary to law. While this court acknowledges the government's request to reverse Judge Waxse and grant the newly submitted warrant application, this court would reiterate that it has limited review over the current order and owes some deference to Judge Waxse's decision. *See Ocelot Oil Corp.*, 847 F.2d at 1464 (noting "[t]he clearly erroneous standard . . . requires that the reviewing court affirm unless it 'on the entire evidence is left with the definite and firm conviction that a mistake has been committed'").

As mentioned above, Judge Waxse denied the warrant application for lack of particularity for the place to be searched and things to be seized. Judge Waxse found the government's request for the entire contents of an individual's email account was overbroad and created the potential for the government to seize private, irrelevant information. More specifically, Judge Waxse noted the government did not establish probable cause for four of the individuals/identifiers listed in the warrant application. In finding the warrant was not sufficiently particular, Judge Waxse suggested the government could resubmit its application and include one of his recommended *ex ante* instructions.

In considering Judge Waxse's conclusions, this court needs to decide whether it was clearly erroneous or contrary to law to find that the warrant application did not meet the probable cause and particularity requirements of the Fourth Amendment. Before this court engages in that analysis, it first will discuss the issue of *ex ante* instructions. In his order, Judge Waxse stated:

> "[A]ll courts agree that magistrate judges have the authority to impose *ex ante* instructions but that *ex ante* instructions have never been required. . . . In its previous email opinions, the Court left the suggestion of *ex ante* instructions—or as it referred to them then, 'appropriate procedural safeguard(s)'—up to the government, but the government has yet to suggest any. Instead, the government continues to insist it should be entitled to all ESI in or associated with an individual's email account without limitation. Below are some *ex ante* instruction options." (Doc. 2 at 39.)

Judge Waxse then provided a thorough discussion of suggested *ex ante* instructions. He concluded his order by denying the warrant but recommended the government resubmit its application "once it includes a search protocol that addresses the concerns expressed in this opinion or agrees to one of the other *ex ante* instructions." (Doc. 2 at 49.) The government has asked this court to find that it is not required to include *ex ante* instructions in its application prior to the issuance of the warrant. In its Motion to Review, the government detailed the many reasons why it believed Judge Waxse's suggested *ex ante* instruction suggestions were unreasonable and argued it was entitled to the information sought in the warrant without the inclusion of any of these *ex ante* limitations.

Although there is much discussion over possible *ex ante* instruction options, this court declines to rule on whether any of them, individually, are reasonable in this particular case. Although Judge Waxse included many options in his order, these were simply suggestions for the government in the future, not court-ordered *ex ante* instructions for the issuance of this specific warrant. Had Judge Waxse, for example, provisionally granted the warrant under the premise the government would submit a search protocol, or had he granted the warrant but ordered the use of a special master to search the data seized from the Provider, this court could then review those court-ordered *ex ante* limitations for reasonableness. Because no *ex ante* instructions were ordered, this court has nothing to review, and to comment on the reasonableness of each suggested limitation would result in this court issuing an advisory opinion. *See Norvell v. Sangre de Cristo Dev. Co., Inc.*, 519 F.2d 370, 375 (10th Cir. 1975) (noting "[j]udicial restraint should be exercised to avoid rendition of an advisory opinion").

And, although there are no specific *ex ante* instructions to review in this case, this court would briefly note that *ex ante* instructions, as whole, are not per se unreasonable. Various courts have held that *ex ante* instructions are permissible, but not required under the Fourth Amendment. *See In re Search Warrant*, 71 A.3d 1158 (Vt. 2012) (rejecting "any blanket prohibition on *ex ante* search warrant

instructions"); *see also In the Matter of a Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx@gmail.com Maintained at Premises Controlled By Google, Inc.*, 33 F. Supp. 3d 386, 397 (S.D.N.Y. 2014), *as amended* (Aug. 7, 2014) [hereinafter, *SDNY Email*] (noting there was no requirement that a "magistrate judge approving a warrant application *must or should* impose *ex ante* restrictions pertaining to the later execution of that warrant" (emphasis added); *United States v. Christie*, 717 F.3d 1156, 1166–67 (10th Cir. 2013) (discussing that the Fourth Amendment particularity requirement may or may not require limitations *ex ante*; however, "even if courts do not specify particular search protocol up front in the warrant application process, they retain the flexibility to assess the reasonableness of the search protocols the government actually employed in its search after the fact, when the case comes to court, and in light of the totality of the circumstances."); *United States v. Hill,* 459 F.3d 966, 978 (9th Cir. 2006) ("Moreover, in contrast to our discussion of the overbroad seizure claim above, there is no case law holding that an officer *must* justify the lack of a search protocol in order to support issuance of the warrant. As we have noted, we look favorably upon the inclusion of a search protocol; but its absence is not fatal").

Although *ex ante* instructions may be reasonable in some contexts, none were ordered here, and therefore this court will not review whether Judge Waxse's suggested *ex ante* instructions are reasonable. This court will instead shift its focus to the government's claim that the warrant meets the particularity and probable cause requirements of the Fourth Amendment.

This court first acknowledges Judge Waxse's concern with properly balancing an individual's right to privacy with the government's ability to effectively prosecute criminals. The digital storage era has caused a need for courts to reevaluate well-established Fourth Amendment standards. *See United States v. Carey*, 172 F.3d 1268, 1275 (10th Cir. 1999) (finding that "[r]elying on analogies to closed containers or file cabinets may lead courts to 'oversimplify a complex area of Fourth

Amendment doctrines and ignore the realities of massive modern computer storage.'"). Courts should now carefully consider the privacy concerns implicated when a vast amount of information is seized from various electronic sources such as computer hard drives, cell phones, and email accounts. *See United States v. Ganias*, 824 F.3d 199, 217 (2d Cir. 2016) (noting that the seizure of a computer hard drive "can give the government possession of a vast trove of personal information about the person to whom the drive belongs, much of which may be entirely irrelevant to the criminal investigation that led to the seizure").

In considering the email context specifically, courts have held an individual enjoys a right to privacy in his or her emails. *See United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) (holding "a subscriber enjoys a reasonable expectation of privacy in the contents of emails 'that are stored with, or sent or received through, a commercial ISP'").[4] Courts must respect this privacy right by requiring particularity in a warrant for an individual's email account so as to prevent a "general, exploratory rummaging" of a person's private life. *See Andresen v. Maryland*, 427 U.S. 463 (1976) (noting the particularity requirement "makes general searches. . . impossible and prevents the seizure of one thing under a warrant describing another" so that "nothing is left to the discretion of the officer executing the warrant").

Keeping in mind these privacy concerns, this court needs to determine whether the warrant was valid under the Fourth Amendment. The government seeks information from the Hotmail Accounts pursuant to the SCA. Under the SCA, email providers are required to disclose the "contents of

[4] In finding a reasonable expectation of privacy in an individual's emails, the Sixth Circuit noted the prominence of email in modern communication stating, "[s]ince the advent of email, the telephone call and the letter have waned in importance, and an explosion of Internet-based communication has taken place. People are now able to send sensitive and intimate information, instantaneously, to friends, family, and colleagues half a world away. Lovers exchange sweet nothings, and businessmen swap ambitious plans, all with the click of a mouse button. Commerce has also taken hold in email. Online purchases are often documented in email accounts, and email is frequently used to remind patients and clients of imminent appointments. In short, 'account' is an apt word for the conglomeration of stored messages that comprises an email account, as it provides an account of its owner's life. By obtaining access to someone's email, government agents gain the ability to peer deeply into his activities." *Warshak*, 631 F.3d at 284.

electronic communications" or "information pertaining to a subscriber to or customer of such service" only if the government obtains a "warrant issued using the procedures described in the Federal Rules of Criminal Procedure." *See* 18 U.S.C. §§ 2703(a), 2703(b)(A). As mentioned above, Rule 41 of the Federal Rules of Criminal Procedure governs searches and seizures. Specifically, Rule 41(e)(2)(B) governs warrants seeking ESI. This provision sets out the "seize first, search second" two-step rule created for ESI, which was developed because "computer 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." *See* Fed. R. Crim. P. 41(e)(2) advisory committee's note.

Judge Waxse concluded that Rule 41 "both textually and practically was not intended to apply to searches of email accounts obtained under the SCA." (*See* Doc. 2 at 36.) Relying on the advisory committee commentary, Judge Waxse interpreted Rule 41(e)(2) to apply only to situations in which it was impractical for law enforcement to review ESI during the execution of the warrant at the search location—i.e. at the suspect's home. Because a law enforcement officer never has to enter a suspect's home in order to retrieve the electronically stored communications and information from their email accounts, Judge Waxse believes Rule 41 has no practical purpose when seeking information electronically stored by an email provider under the SCA.

Based on the advisory committee note to Rule 41(e)(2), however, emails fall squarely within the definition of ESI. The note states that Rule 41(e)(2) covers a wide array of ESI as defined in Rule 34(a) of the Federal Rules of Civil Procedure. *See* Fed. R. Crim. P. 41(e)(2) advisory committee's note. Rule 34(a) includes a "broad and flexible" description of ESI, which includes "all current types of computer-based information" and encompasses all "future changes and developments." *See id.* The advisory committee note to Rule 34(a) of the Federal Rules of Civil Procedure definitively includes

email within the definition of ESI. *See* Fed. R. Civ. P. 34(a) advisory committee's note ("Rule 34(a)(1) is expansive and includes any type of information that is stored electronically. A common example often sought in discovery is electronic communications, such as e-mail."). Email, therefore, conclusively falls under the ESI umbrella, thus, Rule 41(e)(2) applies to the search and seizure of email accounts.

And while the two-step procedure under Rule 41(e)(2) may apply to the search and seizure of emails, Judge Waxse noted the Rule was silent on the constitutional requirements the government must meet before obtaining a warrant to initiate the Rule 41(e)(2) process. The advisory committee note for Rule 41(e)(2) states, "The amended rule does not address the specificity of description that the Fourth Amendment may require in a warrant for electronically stored information, leaving the application of this and other constitutional standards concerning both the seizure and the search to ongoing case law development." *See* Fed. R. Crim. P. 41(e)(2) advisory committee's note.

In considering the above analysis, this court would conclude the two-step procedure under Rule 41(e)(2) governs the search and seizure of emails obtained pursuant to the SCA. The advisory committee note only leaves open the particularity question to be addressed in each specific circumstance, giving judges flexibility in deciding whether the warrant meets Fourth Amendment particularity standards. Because the two-step procedure applies to the search and seizure of emails under the SCA, the question left to be decided is whether, in considering the current state of case law, the present warrant meets the particularity requirements of the Fourth Amendment.

The Tenth Circuit has held that a search should be "confined in scope to particularly described evidence relating to a specific crime for which there is demonstrated probable cause." *United States v. Brown*, 984 F.2d 1074, 1077 (10th Cir. 1993). Specifically regarding ESI, the Tenth Circuit has "adopted a somewhat forgiving stance when faced with a 'particularity' challenge to a warrant

authorizing the seizure of computers." *United States v. Grimmett*, 439 F.3d 1263, 1269 (10th Cir. 2006). And while a computer search "may be as extensive as reasonably required to locate the items described in the warrant," the warrant needs to be clear as to what evidence is being sought, and officers should "conduct the search in a way that avoids searching files of types not identified in the warrant." *Id.* at 1270.

As mentioned above, the case law surrounding particularity challenges in the email context is sparse. What exists, however, tends to support the notion that Rule 41(e)(2) authorizes the seizure and search of an entire email account subject to an *ex post* review for reasonableness. Support comes from both cases involving the warrant applications themselves, *see SDNY Email*, 33 F. Supp. 3d at 401; *In the Matter of the Search of Information Associated with [redacted] @mac.com that is Stored at Premises Controlled by Apple, Inc.*, 13 F. Supp. 3d 157 (D.D.C. 2014) [hereinafter *DC Email*], and cases involving motions to suppress after the warrant has already been granted and executed, *see, e.g.*, *United States v. Scully*, 108 F. Supp. 3d 59 (E.D.N.Y. 2015) (holding search warrants for Yahoo email accounts were not overly broad or insufficiently particular in violation of the Fourth Amendment); *United States v. Deppish*, 994 F. Supp. 2d 1211 (D. Kan. 2014) (noting "nothing in § 2703 precludes the Government from requesting the full content of a specified email account, nor has the Tenth Circuit ever required warrants to identify a particularized search strategy"); *United States v. Taylor*, 764 F. Supp. 2d 230, 236–37 (D. Me. 2011) (finding a warrant to search emails and seize evidence related to defendant's income and financial means "reasonably limits the evidence to be seized" and was not overly broad simply because the government was authorized to search his email account).

In cases in which courts have either denied a search warrant for the entirety of an email account or suppressed evidence based on an overbroad search warrant, the warrants lacked particularity, for example, in identifying a specified date range or referencing the violation of a specific criminal statute.

See In re [REDACTED] @gmail.com, 62 F. Supp. 3d 1100, 1104 (N.D. Cal. 2014) (denying the search warrant because "there is not date restriction of any kind . . . [n]or has the government made any kind of commitment to return or destroy evidence that is not relevant to its investigation); *United States v. Barthelman*, No. 13-10016-MLB, 2013 WL 3946084, *11 (D. Kan. July 31, 2013) (holding evidence should be suppressed because the warrant was not sufficiently particular in that it failed to reference a particular criminal statute and instead requested "any and all evidence of communications used in furtherance of the violation of laws of the State of Ohio"); *see also United States v. Otero*, 563 F.3d 1127 (10th Cir. 2009) (holding a warrant for a computer was overbroad because the warrant did not contain any affirmative limitations on what a searcher would seize, thus authorizing a general search of the computer). Limitations such as these help prevent the "general rummaging" of the individual's email account. When the government includes specific details as to what it seeks within the email account, the warrant is more in line with Fourth Amendment particularity requirements.

This court acknowledges the concern Judge Waxse and others have with the potential implications of the government overseizing data that does not fall within the scope of the search warrant. *See, e.g.*, *Ganias*, 824 F.3d at 205–08. Courts, however, have developed a "more flexible approach to the execution of search warrants for electronic evidence, holding the government to a standard of reasonableness." *Scully*, 108 F. Supp. at 95. A warrant authorizing the seizure of records of criminal activity "permits officers to examine many papers in a suspect's possession to determine if they are within the described category." *United States v. Wicks*, 995 F.2d 964, 974 (10th Cir. 1993) (citing *United States v. Riley*, 906 F.2d 841, 845 (2d Cir. 1990) (noting the necessity of allowing officers conducting a search some latitude because "few people keep documents of their criminal transactions in a folder marked 'drug records'")). And unlike a warrant for a cognizable physical object—such as drugs or weapons—when officers search through papers, records, or data for evidence,

"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." *Andresen*, 427 U.S. at 482 n.11. This is not to say that the government obtains unchecked discretion simply because the warrant authorizes a search of documents or data. Broad sweeping, comprehensive searches remain unconstitutional, especially when searching personal ESI because "computers can hold so much information touching on many different areas of a person's life." *United States v. Wasler*, 275 F.3d 981, 986 (10th Cir. 2001) (quoting *United States v. Tamura*, 694 F. 2d 591, 595–96 (9th Cir. 1982)). Thus, so long as a warrant specifies with particularity what evidence the government intends to seize, establishes probable cause that the evidence is connected to a specific criminal statute, and includes some limitations (such as a date range) to prevent the potential of a general search, the warrant meets the Fourth Amendment particularity requirement. The search may be reviewed *ex post* should the government execute the warrant in an unreasonable manner. *See Dalia*, 441 U.S. at 258 (holding, "[i]t would extend the Warrant Clause to the extreme to require that, whenever it is reasonably likely that Fourth Amendment rights may be affected in more than one way, the court must set forth precisely the procedures to be followed by the executing officers. Such an interpretation is unnecessary, as we have held . . . that the manner in which a warrant is executed is subject to later judicial review as to its reasonableness").

In applying the law to the warrant at issue, this court concludes it was clearly erroneous or contrary to law for Judge Waxse to find it was not sufficiently particular. The warrant application identified with specificity the target email accounts to be searched and the evidence to be seized in connection with violations of 18 U.S.C. §§ 371 (conspiracy), 1029 (access device fraud), 1030 (computer intrusion), 1343 (wire fraud), and 2319 (copyright infringement), all occurring since September 7, 2008. The government stated with specificity the exact information it sought, thus

leaving officers with little discretion to go outside the scope of the warrant. The application also included an affidavit detailing the criminal scheme and explaining the relevance of the evidence to the investigation. Rule 41(e)(2) authorizes the "seize first, search second" two-step process, thus allowing the government to obtain all of the data to later search for relevant evidence. And while Rule 41(e)(2) leaves open the question of particularity when the government seeks ESI, the majority of case law relating to the search of an email account has upheld the Government's ability to obtain the entirety of the account to then search for relevant evidence. Based on the current state of the law, this court finds Judge Waxse's decision regarding particularity was clearly erroneous or contrary to law.

Although this court finds the warrant sufficiently particular, it agrees with Judge Waxse's conclusion that the warrant lacked probable cause to support a connection between the investigation and four of the individuals/identifiers listed in the warrant. Judge Waxse noted there was not sufficient probable cause to connect [redacted] to the criminal scheme. The government, in its motion to review, conceded it did not include the proper information to connect those individuals/identifiers to the investigation. To remedy this, the government submitted a new warrant application with its motion to review in which it included new information to establish probable cause for those individuals/identifiers. While this information may satisfy the lack of probable cause, this court may not consider new evidence while sitting in review of a magistrate judge's order on a non-dispositive pretrial order. As noted above, under Rule 72(a), a district court "must consider timely objections and modify or set aside" any part of a magistrate judge's order on a non-dispositive pretrial order that is "clearly erroneous or is contrary to law." The rule does not authorize a district court to consider new evidence when reviewing a magistrate's decision on a pretrial non-dispositive order. *Compare* Fed. R. Civ. P. Rule 72(a) *with* Fed. R. Civ. P. Rule 72(b) (noting that for dispositive motions, a judge of the court may review a magistrate's recommended disposition de novo and may "accept, reject, or modify"

the findings and also "*receive further evidence* or recommit the matters" to the magistrate with instructions) (emphasis added.) Thus, this court may not consider the newly submitted warrant application and finds there is not sufficient probable cause in the original warrant to connect [redacted] to the investigation. Judge Waxse's decision was therefore not clearly erroneous or contrary to law and this court affirms his decision to deny the warrant for lack of probable cause for those four individuals/identifiers.[5]

In conclusion, this court acknowledges the careful balance that needs to be achieved between an individual's right to privacy and the government's ability to prosecute criminals. The digital era has created new and more complicated Fourth Amendment challenges. File cabinets with folders and documents have been replaced with electronic devices with immense digital storage capabilities, thus the government should be more cognizant of the vast quantities of private material that may be intermingled with relevant evidence.

The law, however, authorizes the government to "seize first, search second" when dealing with ESI. Courts need to ensure that search warrants seeking ESI are sufficiently particular so that officers executing a warrant do not exceed their scope and perform a "general rummaging" of a person's private information. Based on the current status of case law, this court finds the present warrant is sufficiently particular under the Fourth Amendment. And while this court acknowledges that a judge may have the authority to impose reasonable *ex ante* instructions, it declines to comment on the *ex ante* instructions suggested by Judge Waxse. This court, however, will not grant the warrant as is because Judge Waxse's decision that there was insufficient probable cause as to the four individuals/identifiers

[5] This court notes that Judge Waxse also took issue with the government's inclusion of the phrase "and others known and unknown" as overbroad. The government did not raise an objection to this finding in its motion and therefore this court will not review it as "a party may not assign as error a defect in the order not timely objected to." *See* Fed R. Civ. P. Rule 72(a).

was not clearly erroneous or contrary to law. The government may resubmit its warrant application for reconsideration by a magistrate judge.

IT IS THEREFORE ORDERED that the court overrules in part and sustains in part the government's objections in its Motion to Review Denial of Search Warrant (Doc. 4). The court will not grant the original warrant due to lack of probable cause as to the four individuals/identifiers. This case is closed.

Dated this 28th day of September, 2016, at Kansas City, Kansas.

s/ Carlos Murguia
CARLOS MURGUIA
United States District Judge