

**UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF KANSAS**

**In the Matter of the Search of  
premises known as:**

**Three Hotmail Email accounts:  
[redacted]@hotmail.com  
[redacted]@hotmail.com  
[redacted]@hotmail.com**

**SEARCH WARRANT**

**Belonging to and Seized from  
[redacted]**

**CASE NUMBER: 16-MJ-8036-DJW**

**MEMORANDUM AND ORDER DENYING APPLICATION FOR SEARCH WARRANT**

The United States has submitted an Application and Affidavit for Search Warrant (“Application”) pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) requiring an electronic communication services provider (“Email Provider”), to disclose copies of electronic communications, including the content of email and other account-related information, for the email accounts (“target email accounts”) identified in the Application. Here, the Email Provider is Microsoft Corporation. In the affidavit in support of probable cause, the government alleges that the target email accounts were utilized to obtain, crack, and facilitate the distribution of illicit versions of proprietary software, in violation of 18 U.S.C. §§ 371 (conspiracy), 1029 (access device fraud), 1030 (computer intrusion), 1343 (wire fraud), and 2319 (copyright infringement). The Application seeks a search warrant to obtain ESI in each target email account from Microsoft in its search for fruits, evidence and/or instrumentalities of the violation of those laws. For the reasons discussed below, the Application for search warrant is denied without prejudice.

## **I. PROPOSED SEARCH WARRANT**

The proposed search warrant is structured to identify two categories of information: (1) information to be disclosed by an Email Provider to the government under 18 U.S.C. § 2703, and (2) information to be seized by the government. The first section of the warrant orders Microsoft (the Email Provider) to disclose to the government copies of the following records and other information, including the content of the communications, for each account or identifier associated with the target email accounts:

The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft 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.

The second section of the proposed warrant provides:

Upon receipt of this information from the Provider, government-authorized persons will review that information to locate the 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],<sup>1</sup> 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 device(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.

## **II. BACKGROUND**

For clarity, the Court needs to define or more fully define some terms that will be used throughout this Memorandum Opinion. As this opinion focuses on a warrant for email, the Court will use the term “electronically stored information,” or “ESI” for short, to describe the *all*

---

<sup>1</sup> The Court has redacted sensitive information. This Court will provide the redacted information to the government upon its request.

of the possible information that may be found in an email account. This obviously includes the email communications themselves, but it also includes any other digital data that may reside, or is associated with, the email account, such as contact lists, chat transcripts, calendars, pictures, and files. Basically, anything that can be stored in an email account falls under this umbrella term. The Court will also be using the terms *ex ante* and *ex post*, which mean before and after, respectively. Magistrate judges decide *ex ante* because the facts of the case have not developed—indeed, no case has been filed other than the request for the warrant. District judges decide *ex post* because the facts of the case have developed already, as the search warrant has been executed. This Court will speak of “*ex ante* instructions,” which simply means 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. Similarly, the Court will use the term “search protocol,” which is a document submitted by the government explaining to the Court how it will conduct its search of an individual’s ESI. A search protocol may set forth how the government will search the ESI, the search software used, the keywords for which the government will search, or what the government will do with ESI that falls outside the scope of the warrant (such as returning or destroying it). Importantly, a search protocol is to inform the Court as to how the government intends to search the ESI. A search protocol may be required as part of a court’s *ex ante* instructions.

Finally, the Court will also be referring to “imaging,” which in the technological sense to which the Court is referring means making an exact, duplicate copy—the result of which is an “image.” Law enforcement commonly images a seized hard drive in order to perform a search of the data at their forensic lab. This allows the individual to retain the computer or device

(assuming they have not been arrested) and allows the government to retain an exact copy of the device as it existed in that particular moment.

### **III. RELEVANT LAW**

#### **A. The Stored Communications Act, 18 U.S.C. §§ 2701 *et seq.***

The Application seeks authorization to obtain from and search the ESI contained in the email account of a particular customer (suspect) of Microsoft pursuant to the Stored Communications Act of 1986 (“SCA”).<sup>2</sup> In the email context, a government entity may require an Email Provider to disclose the contents of a wire or electronic communication that has been in electronic storage for 180 days or less pursuant to a warrant issued in compliance with the Federal Rules of Criminal Procedure.<sup>3</sup> For contents stored for more than 180 days, the statute authorizes a government entity to require an Email Provider to disclose the contents of the communications under the procedures outlined in subsection (b).<sup>4</sup> Section 2703(b)(1)(A) authorizes a government entity to require a provider of remote computing services to disclose the contents of any wire or electronic communication without notice to the subscriber or customer if the government obtains a warrant issued pursuant to the Federal Rules of Criminal Procedure.

#### **B. Federal Rule of Criminal Procedure 41**

Federal Rule of Criminal Procedure 41 governs searches and seizures. In 2009, Rule 41 was amended to address ESI. Rule 41(e)(2)(B) sets forth a two-step procedure (“Two-Step Procedure”) for warrants seeking ESI. On Step One, “officers may seize or copy the entire storage medium;” on Step Two, officers can review—i.e. search—that copy later “to determine

---

<sup>2</sup> 18 U.S.C. §§ 2701 *et seq.*

<sup>3</sup> 18 U.S.C. § 2703(a).

<sup>4</sup> *Id.*

what electronically stored information falls within the scope of the warrant.”<sup>5</sup> This process is necessary because “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.”<sup>6</sup>

Importantly, however, the Advisory Committee 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.”<sup>7</sup>

### **C. The Fourth Amendment to the United States Constitution**

Underlying all of the above, of course, is the Fourth Amendment to the United States Constitution. The Fourth Amendment guarantees the right of citizens against unreasonable searches and seizures, providing:

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.<sup>8</sup>

The manifest purpose of the Fourth Amendment particularity requirement is to prevent the Framers’ chief evil: general searches.<sup>9</sup> A general search “le[aves] to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched . . . [and] provide[s] no judicial check on the determination of the executing officials

---

<sup>5</sup> Fed. R. Crim. P. 41(e)(2) advisory committee note.

<sup>6</sup> Fed. R. Crim. P. 41(e)(2) advisory committee note.

<sup>7</sup> Fed. R. Crim. P. 41 advisory committee note.

<sup>8</sup> U.S. Const. amend. IV.

<sup>9</sup> See also *United States v. Galpin*, 720 F.3d 436, 445 (2d Cir. 2013); *Ashcroft v. al-Kidd*, 131 S. Ct. 2074, 2084 (2011) (“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.”).

that the evidence available justified an intrusion into any particular [place].”<sup>10</sup> A warrant must provide the officer conducting the search with sufficiently precise language to allow him or her to determine which items are properly subject to seizure and which items are irrelevant.<sup>11</sup> Thus, “[t]he requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another.”<sup>12</sup> In other words, “[a]s to what is to be taken, nothing is left to the discretion of the officer executing the warrant.”<sup>13</sup> “As the text makes clear, the ultimate touchstone of the Fourth Amendment is reasonableness.”<sup>14</sup> “A search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing . . . reasonableness generally requires the obtaining of a judicial warrant.”<sup>15</sup> Such a warrant must: (1) be issued by a neutral magistrate; (2) allow the magistrate to find probable cause to believe that the evidence sought will “aid in a particular apprehension or conviction’ for a particular offense;” and (3) describe with specificity the “things to be seized, as well as the place to be searched.”<sup>16</sup>

The Supreme Court has established that judicial scrutiny of proposed search warrants “is intended to eliminate altogether searches not based on probable cause. The premise here is that

---

<sup>10</sup> *Steagald v. United States*, 451 U.S. 204, 220 (1981); *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971) (“general exploratory rummaging of a person’s belongings.”).

<sup>11</sup> See *Davis v. Gracey*, 111 F.3d 1472, 1478-79 (10th Cir. 1997) (“We ask two questions: did the warrant tell the officers how to separate the items subject to seizure from irrelevant items, and were the objects seized within the category described in the warrant?”); *United States v. Tamura*, 694 F.2d 591, 595 (9th Cir. 1982) (Stating that a request to search must be accompanied by “sufficiently specific guidelines for identifying the documents sought . . . [to be] followed by the officers conducting the search.”)

<sup>12</sup> *Stanford v. Texas*, 379 U.S. 476, 485 (1965) (quoting *Marron v. United States*, 275 U.S. 192, 196 (1927) (internal quotation marks omitted)).

<sup>13</sup> *Marron*, 275 U.S. at 196.

<sup>14</sup> *Riley v. California*, \_\_\_ U.S. \_\_\_, 134 S. Ct. 2473, 189 L. Ed. 2d 430 (2014) (quoting *Brigham City v. Stuart*, 547 U. S. 398, 403 (2006) (internal quotation marks omitted)).

<sup>15</sup> *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995).

<sup>16</sup> *Dalia v. United States*, 441 U.S. 238, 255 (1979) (quoting *Warden v. Hayden*, 387 U.S. 294, 307 (1967); *Stanford*, 379 U.S. at 485).

any intrusion in the way of search or seizure is an evil, so that no intrusion at all is justified without careful prior determination of necessity.”<sup>17</sup> Determining probable cause in a warrant requires the magistrate judge to decide “whether, given all the circumstances set forth in the affidavit before him, including the veracity and basis of knowledge of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place.”<sup>18</sup>

The Fourth Amendment particularity requirement enables the 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.”<sup>19</sup> It also assures both the court and the individual whose property is searched or seized of the lawful authority of the executing officer, the officer’s need to search, and the limits of the officer’s power to search.<sup>20</sup> “To determine if the *place* to be searched is particularly described, courts ask whether the description is sufficient ‘to enable the executing officer to locate and identify the premises with reasonable effort, and whether there is any reasonable probability that another premise might be mistakenly searched.’”<sup>21</sup> To determine if the *things* to be seized are particularly described, there must be language in the warrant that creates a nexus between the suspected crime and the things to be seized.<sup>22</sup> Thus, the description of the items to be seized must be confined to “particularly

---

<sup>17</sup> *Coolidge*, 403 U.S. at 467 (1971).

<sup>18</sup> *United States v. Warren*, 42 F.3d 647, 652 (D.C. Cir. 1994) (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983)) (internal quotation marks omitted).

<sup>19</sup> *Maryland v. Garrison*, 480 U.S. 79, 84 (1987).

<sup>20</sup> *Groh v. Ramirez*, 540 U.S. 551, 561 (2004) (internal citations omitted).

<sup>21</sup> *United States v. Lora–Solano*, 330 F.3d 1288, 1293 (10th Cir. 2003) (quoting *United States v. Pervaz*, 118 F.3d 1, 9 (1st Cir. 1997)).

<sup>22</sup> *United States v. Campos*, 221 F.3d 1143, 1147.



described evidence relating to a specific crime for which there is demonstrated probable cause.”<sup>23</sup> Taking the above together, the scope of a lawful search is:

defined by the object of the search and the places in which there is probable cause to believe that it may be found. Just as probable cause to believe that a stolen lawnmower may be found in a garage will not support a warrant to search an upstairs bedroom, probable cause to believe that undocumented aliens are being transported in a van will not justify a warrantless search of a suitcase.<sup>24</sup>

### III. DISCUSSION

Although there are many cases addressing the Fourth Amendment’s particularity requirements as to computer searches, there is little guidance on the particularity that should be applied to search warrants seeking ESI stored with an Email Provider. Due to the sealed nature of applications for search warrants, few reported opinions exist addressing the factors or standards that should be used in determining whether search warrants seeking ESI are sufficiently particular under the Fourth Amendment. In 2012<sup>25</sup> and 2013,<sup>26</sup> this Court denied search warrant applications that requested electronic communications in an email account based upon concerns that the warrants violate the Fourth Amendment’s probable cause and particularity requirements. In March<sup>27</sup> and April<sup>28</sup> of 2014, Magistrate Judge John Facciola of the United States District Court for the District of Columbia denied a similar search warrant for

---

<sup>23</sup> *Mink v. Knox*, 613 F.3d 995, 1010 (10th Cir. 2010).

<sup>24</sup> *Garrison*, 480 U.S. at 84–85 (citing *United States v. Ross*, 456 U.S. 798, 824 (1982)).

<sup>25</sup> *In re Applications for Search Warrants for Info. Associated with Target Email Address*, No. 12-MJ-8119-DJW, 2012 WL 4383917 (D. Kan. Sept. 21, 2012) [hereinafter, *Email I*].

<sup>26</sup> *See In re Applications for Search Warrants for Info. Associated with Target Email Accounts/Skype Accounts*, 2013 WL 4647554 (D. Kan. Aug. 27, 2013) [hereinafter, *Email II*].

<sup>27</sup> *Matter of the Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.*, 25 F. Supp. 3d 1, 4 (D.D.C. Mar. 7, 2014).

<sup>28</sup> *Matter of Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.*, 13 F. Supp. 3d 145, 147 (D.D.C. Apr. 7, 2014) *vacated sub nom. Matter of Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.*, 13 F. Supp. 3d 157 (D.D.C. 2014);

the same reasons.<sup>29</sup> Both courts have extended their rationale to search warrants of other electronic devices and web-based services.<sup>30</sup> Outsiders wondered if this was the beginning of a “magistrates’ revolt.”<sup>31</sup>

### A. Developments Since Email II

Since then, other federal magistrate judges have entered the fray.<sup>32</sup> In *NDCal Email*, the court denied a similar search warrant for email. It wrote:

The court is nevertheless unpersuaded that the particular seize first, search second proposed here is reasonable in the Fourth Amendment sense of the word. On past occasions, the government at least submitted a date restriction. Here, there is no date restriction of any kind. The activity described in the application began in 2010; Gmail has been broadly available since 2007 and in beta release since 2004. Nor has the government made any kind of commitment to return or destroy evidence that is not relevant to its investigation. This unrestricted right to retain and use every bit Google coughs up undermines the entire effort the application otherwise makes to limit the obvious impact under the plain view doctrine of providing such unfettered government access.<sup>33</sup>

---

<sup>29</sup> The two opinions were subsequent opinions in the same case.

<sup>30</sup> See, e.g., *In re Cellular Telephones*, No. L4-MJ-8017-DJW, 2014 WL 7793690 (D. Kan. Dec. 30, 2014); *In re Search of premises known as Three Cellphones & One Micro-SD Card*, No. L4-MJ-8013-DJW, 2014 WL 3845157 (D. Kan. Aug. 4, 2014); *In re Search of Nextel Cellular Telephone*, 2014 WL 2898262 (D. Kan. June 26, 2014); *Matter of Black iPhone 4*, 27 F. Supp. 3d 74, 76 (D.D.C. 2014); *Matter of Search of ODYS LOOX Plus Tablet Serial No. 4707213703415 In Custody of United States Postal Inspection Serv., 1400 New York Ave NW, Washington, DC*, 28 F. Supp. 3d 40 (D.D.C. 2014) [hereinafter *Odys Loox*]; see also *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.*, 21 F.Supp.3d 1, 9–10, 2013 WL 7856600, at \*7 (D.D.C. Nov. 26, 2013) (Facciola, M.J.) [hereinafter *DC Facebook*].

<sup>31</sup> See Reid Day, Comment, *Let the Magistrates Revolt: A Review of Search Warrant Applications for Electronic Information Possessed by Online Services*, 64 U. Kan. L. Rev. 491 (2015); see generally Ann E. Marimow and Craig Timberg, Washington Post, available at [https://www.washingtonpost.com/local/crime/low-level-federal-judges-balking-at-law-enforcement-requests-for-electronic-evidence/2014/04/24/eec81748-c01b-11e3-b195-dd0c1174052c\\_story.html?hpid=z1](https://www.washingtonpost.com/local/crime/low-level-federal-judges-balking-at-law-enforcement-requests-for-electronic-evidence/2014/04/24/eec81748-c01b-11e3-b195-dd0c1174052c_story.html?hpid=z1) (last visited March 21, 2016); Patrick J. Cotter, The National Law Review, available at <http://www.natlawreview.com/article/magistrates-revolt-unexpected-resistance-to-federal-government-efforts-to-get-genera> (last visited March 21, 2016); Scott H. Greenfield, Simple Justice, available at <http://blog.simplejustice.us/2015/02/25/the-magistrates-revolt-continues-search-protocol/> (last visited March 21, 2016); Orin Kerr, The Volokh Conspiracy, available at <https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/03/24/judge-denies-warrant-application-because-he-thinks-the-government-doesnt-need-a-warrant/> (last visited March 21, 2016).

<sup>32</sup> *In the Matter of a Warrant for All Content & Other Info. Associated with the Email Account xxxxxx@gmail.com Maintained at Premises Controlled By Google, Inc.*, 33 F. Supp. 3d 386 (S.D.N.Y. 2014), as amended (Aug. 7, 2014) [hereinafter, *SDNY Email*]; *In re [REDACTED]@gmail.com*, 62 F. Supp. 3d 1100, 1101 (N.D. Cal. May 8, 2014) [hereinafter, *NDCal Email*].

<sup>33</sup> *NDCal Email*, 62 F. Supp. 3d at 1104.

In *SDNY Email*, however, the court granted a search warrant for email, explaining that the opinions of this Court and Magistrate Judge Facciola too narrowly construe the Fourth Amendment’s particularity requirement and are contrary to “copious precedent.” The court framed the issues as follows:

- (1) Should the email provider [there, Google; here, Microsoft] be directed to produce all the emails associated with the subject email account?
- (2) Can the court require the email provider to review the emails and provide to the government only those emails responsive to the categories listed in the warrant?<sup>34</sup>
- (3) If the answer to question number one is yes, should the court require the government follow certain protocols—whether as to length of the search, manner of the search, or length of retention of the emails—as a condition of obtaining the warrant?<sup>35</sup>

As to the first question, the court answered “no” for two reasons. First, it believes “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.”<sup>36</sup> Second, the court found that the warrant complied the Fourth Amendment because “Rule 41 embodies standards which conform with the requirements of the Fourth Amendment”<sup>37</sup> and the warrant implemented Rule 41(e)(2)(B)’s Two-Step Procedure. Moreover, the court perceived “no constitutionally significant difference between the searches of hard drives just discussed and searches of email accounts” because, in many cases, there will be less ESI in an email account

---

<sup>34</sup> Judge Gorenstein viewed this as a subsidiary question with respect to the first question. This Court breaks it into its own question because it is pertinent to later discussion.

<sup>35</sup> *SDNY Email*, 33 F. Supp. 3d at 390.

<sup>36</sup> *SDNY Email*, 33 F. Supp. 3d at 392; *see also United States v. Ganius*, 755 F.3d 125, 134–36 (2d Cir. 2014) (“[T]he ability of computers to store massive volumes of information presents logistical problems in the execution of search warrants.”).

<sup>37</sup> *United States v. Haywood*, 464 F.2d 756, 760 (D.C. Cir. 1972).

than on a personal computer hard drive.<sup>38</sup> The court concluded it is well-established that a search warrant can properly permit access to ESI for purposes of a search even where the probable cause showing does not apply to the entirety of the ESI.

As to the second question (could the court require the *Email Provider* to perform the investigatory search of the emails and produce only the responsive emails falling within the scope of the warrant?), the court found such a requirement would impose undue burdens on all parties involved. It puts the Email Provider's employees in the position of appearing to act as agents of the government. Additionally, those employees are not trained in investigatory techniques thereby hampering the government's interest in effectively investigating suspected criminals. However, the court conceded that "[t]here 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 [investigatory] skill or discretion, for example, under a warrant requiring disclosure of all emails from a particular time period."<sup>39</sup>

"No" was the court's answer to the third question—should the court require the government follow certain protocols (whether as to length of the search, manner of the search, or length of retention of the emails) as a condition of obtaining the warrant? It reasoned that "[j]udging the reasonableness of the execution of a search *ex ante*, however, is not required by Supreme Court precedent."<sup>40</sup> The court further explained that *Dalia* held "the manner in which a warrant is executed is subject to later judicial review as to its reasonableness"<sup>41</sup> and that the

---

<sup>38</sup> *SDNY Email*, 33 F. Supp. 3d at 394.

<sup>39</sup> *Id.* at 394.

<sup>40</sup> *Id.* at 396 (citing *Dalia v. United States*, 441 U.S. 238 (1979)).

<sup>41</sup> *Dalia*, 441 U.S. at 258.

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.<sup>42</sup>

In passing, the court addressed the indefinite retention of the ESI obtained by the government, one of the concerns raised in *Email II*, *DC Email*, and *NDCal Email*. It assumed without deciding two issues: (1) the court has the power to impose limitations on the retention of ESI at the time a warrant for email is approved; and (2) the court has the power to include search protocols in a warrant, such as the type of search to be conducted. The court declined to impose a search protocol because, while courts may be *empowered* to include one, courts have never been *required* to include them, especially in the ESI context.<sup>43</sup>

On the heels of those magistrate judges’ opinions, a federal district court finally weighed in. In *Matter of Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.* (“*DC District Email*”),<sup>44</sup> the Chief Judge of the United States District Court for the District of Columbia, Richard W. Roberts, vacated Magistrate Judge Facciola’s April 7 opinion, finding the government’s proposed warrant complied with the Fourth Amendment. Specifically, the court found the place to be searched—[redacted]@mac.com—and the things to be seized—ESI constituting “evidence and instrumentalities of violations of 41

---

<sup>42</sup> *SDNY Email*, 33 F. Supp. 3d at 396–97 (quoting *United States v. Grubbs*, 547 U.S. 90, 97–98 (2006)).

<sup>43</sup> 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.”); see also *In re Search Warrant*, 193 Vt. 51, 71 A.3d 1158 (2012) (“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.”) (emphasis in original) [hereinafter *Vermont Warrant*]).

<sup>44</sup> 13 F. Supp. 3d 157, 159 (D.D.C. Aug. 8, 2014).

U.S.C § 8702 (Solicitation and Receipt of Kickbacks) and 18 U.S.C. § 371 (Conspiracy), dated between January 14, 2014, to the present, including e-mails referring or relating to a government investigation involving any or all of the following: [individuals and entities have been redacted]”—were described with sufficient particularity.<sup>45</sup> Like *SDNY Email*, the court relied upon the warrant’s implementation of Rule 41(e)(2)(B)’s Two-Step Procedure. In its final point, the court acknowledged that searches for ESI may present increased risks to an individual’s right to privacy, and thus courts must strike the proper balance “between protecting an individual’s right to privacy and ensuring that the government is able to prosecute suspected criminals effectively.”<sup>46</sup> However, the court did not attempt to balance those interests. While the court wrote “with these considerations in mind,” it only listed one consideration:

[because] searches for electronic data present unique challenges for law enforcement . . . the practical realities of searches for electronic records may require the government to examine information outside the scope of the search warrant to determine whether specific information is relevant to the criminal investigation and falls within the scope of the warrant.<sup>47</sup>

No counterpoint(s) regarding Americans’ right to privacy in their ESI was even mentioned, let alone analyzed. The court simply jumped to the conclusion that, on balance, the unique challenges for law enforcement officials in searching ESI outweighs an individual’s right to privacy.

Despite differing conclusions, every court (including this one) that has participated in this discussion agrees on three points: (1) individuals have a right to privacy with respect to email;<sup>48</sup> (2) magistrate judges have the *authority* to impose search protocols but the Fourth Amendment

---

<sup>45</sup> *D.C. District Email*, 13 F. Supp. 3d at 161.

<sup>46</sup> *United States v. Adjani*, 452 F.3d 1140, 1152 (9th Cir. 2006).

<sup>47</sup> *D.C. District Email*, 13 F. Supp. 3d 157, 166.

<sup>48</sup> *See United States v. Warshak*, 631 F.3d 266, 282-88 (6th Cir. 2010).

does not *require* them;<sup>49</sup> and (3) the Fourth Amendment does not *require* the government to delegate its investigatory search of ESI within the target email account to the Email Provider to ascertain what ESI falls under the scope of the warrant. This Court, however, continues to disagree with cases that find the proposed warrants were not overly broad in their authorization for the Email Provider to disclose—without limitation or any concern for the privacy rights of the account holder or any person communicating with that account—all ESI in or associated with the target email account.

### **B. General Warrant Equals Invasion of Privacy**

The chief aim of this Court’s email (and cellular phone) opinions has been preventing the issuance of general warrants in the context of ESI. This Court has discussed the abhorrence of “general warrants,” which were the chief evil the Framers were concerned with when drafting the Fourth Amendment.<sup>50</sup> These days, courts discuss general warrants in boilerplate fashion: a quote or two in the legal standards section of an opinion, backed up with the same general case citations, and with the seemingly sole purpose of reiterating the fact that the court knows it should protect against general warrants. The problem with this framing is that the term “general warrants” fails to grasp courts’ attention, having been beaten into rote regurgitation. Perhaps the time has come to reframe the discussion in terms of Americans’ right to privacy.<sup>51</sup> Privacy has become the main thrust of the Fourth Amendment since Justice Harlan’s concurrence in *United*

---

<sup>49</sup> See *Vermont Warrant*, 193 Vt. at 71.

<sup>50</sup> *Ashcroft*, 131 S. Ct. at 2084.

<sup>51</sup> Indeed, *privacy* has taken center-stage in the public eye recently because Apple, Inc. objected to FBI search warrants. See generally *In re Apple, Inc.*, No. 15-MC-1902 (JO), 2016 WL 783565 (E.D.N.Y. Feb. 29, 2016); *In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203*, No. ED 15-0451M), Order Compelling Apple, Inc. to Assist Agents in Search (C.D. Cal. Feb. 16, 2016).

*States v. Katz*,<sup>52</sup> which outlined the “reasonable expectation of privacy” standard.<sup>53</sup> As Justice Scalia wrote: “[T]here is nothing new in the realization that the Constitution sometimes insulates the criminality of a few in order to protect the privacy of us all.”<sup>54</sup> The proper question is “where the proper balance should be struck.”<sup>55</sup> The Ninth Circuit believes that courts must strike the proper balance “between protecting an individual’s right to privacy and ensuring that the government is able to prosecute suspected criminals effectively.”<sup>56</sup>

The first question is whether an individual has a right to privacy in his or her ESI. The answer is unequivocally yes. The Supreme Court has found privacy interests in telephone communications,<sup>57</sup> regular mail,<sup>58</sup> text messages on a pager,<sup>59</sup> and cellular phones.<sup>60</sup> The Sixth Circuit has found privacy interests in email, a decision that remains uncontested.<sup>61</sup> Having established an individual has a right to privacy in his or her ESI (here, an email account), the next question is how should the court weigh the individual’s right to privacy against the government’s ability to prosecute suspected criminals effectively.

---

<sup>52</sup> 389 U.S. 347 (1967).

<sup>53</sup> See generally Christopher Slobogin, *A Defense of Privacy As the Central Value Protected by the Fourth Amendment’s Prohibition on Unreasonable Searches*, 48 Tex. Tech L. Rev. 143 (2015) (advocating the use of a “privacy standard,” otherwise known as the *Katz* test). Extending that premise further, the privacy standard could also encompass seizures, which would eliminate the ambiguity in whether disclosure under § 2703 is a search, seizure, both, or none and the effects such a classification would have.

<sup>54</sup> *Arizona v. Hicks*, 480 U.S. 321, 329 (1986).

<sup>55</sup> *Id.*

<sup>56</sup> *United States v. Adjani*, 452 F.3d 1140, 1152 (9th Cir. 2006).

<sup>57</sup> *Katz v. United States*, 389 U.S. 347 (1967) (finding that telephone users were “surely entitled to assume that the words . . . utter[ed] into the mouthpiece w[ould] not be broadcast to the world”).

<sup>58</sup> *United States v. Jacobsen*, 466 U.S. 109 (1984) (finding that “[l]etters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy”).

<sup>59</sup> *City of Ontario, California v. Quon*, 130 S.Ct. 2619, 2630 (2010). Technically, the Court did not directly decide the issue; rather, the Court assumed *arguendo* that the employee had a reasonable expectation of privacy in text messages sent and received on the government employer-owned pager.

<sup>60</sup> *Riley*, 134 S.Ct. at 2494–95 (holding that law enforcement must get a warrant before searching a cellular phone that was lawfully seized incident to arrest).

<sup>61</sup> *Warshak*, 631 F.3d at 266.



Before balancing the interests involved, the Court must first answer a preliminary question: what is privacy? In this context, *Vermont Warrant* is particularly helpful, as it discusses privacy in great detail.<sup>62</sup> There, the state and dissent argued that allowing information to be viewed by a third party (e.g. special master, court-appointed expert, filter team, etc.)—even one behind a firewall—eliminates the individual’s legitimate privacy interest. But the Supreme Court of Vermont rejected that argument, wisely noting that not all exposures of data are created equal because “privacy concerns not only our interest in determining *whether* personal information is revealed to another person but also our interest in determining *to whom* such information is revealed.”<sup>63</sup> Exposure of the same information to one person may harm the individual’s privacy more than to another. “If an embarrassing or humiliating piece of personal information must be revealed to someone, it is surely worse to have it revealed to the neighborhood busybody or to one’s boss than it is to have it revealed to a stranger.”<sup>64</sup> If a boss discovers embarrassing information about us, the harm may be greater because it may impair our

---

<sup>62</sup> Indeed, the Court is tempted to quote whole pages of the opinion. See generally *Vermont Warrant*, 193 Vt. at 51.

<sup>63</sup> *Id.* at 80 (emphasis in original) (citing *Nat’l Cable & Telecomms. Ass’n v. FCC*, 555 F.3d 996, 1001 (D.C. Cir. 2009) (“It is widely accepted that privacy deals with determining for oneself when, how and to whom personal information will be disclosed to others.”); *Stone v. State Farm Mut. Auto. Ins. Co.*, 185 P.3d 150, 155 (Colo. 2008) (“[Privacy] includes ‘the power to control what we shall reveal about our intimate selves, to whom, and for what purpose.’” (quoting *Martinelli v. Dist. Ct. ex rel. City & Cnty. of Denver*, 199 Colo. 163, 612 P.2d 1083, 1091 (1980))); C. Fried, *Privacy*, 77 Yale L.J. 475, 482 (1968) (“It is not true, for instance, that the less that is known about us the more privacy we have. Privacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves.”); K. Karst, “*The Files*”: *Legal Controls over the Accuracy and Accessibility of Stored Personal Data*, 31 Law & Contemp. Probs. 342, 344 (1966) (“Meaningful discussion of privacy ... requires the recognition that ordinarily we deal not with an interest in total nondisclosure but with an interest in selective disclosure.”); R. Parker, *A Definition of Privacy*, 27 Rutgers L.Rev. 275, 281 (1974) (“[P]rivacy is control over when and by whom the various parts of us can be sensed by others.”); D. Solove, *Conceptualizing Privacy*, 90 Cal. L.Rev. 1087, 1108–09 (2002) (“[E]quating privacy with secrecy ... fails to recognize that individuals want to keep things private from some people but not others. . . . Secrecy as the common denominator of privacy makes the conception of privacy too narrow.”).

<sup>64</sup> *Id.* at 82 (citing *Beaumont v. Brown*, 401 Mich. 80, 257 N.W.2d 522, 531 (1977) (“Communication of embarrassing facts about an individual to a public not concerned with that individual and with whom the individual is not concerned obviously is not a ‘serious interference’ with plaintiff’s right to privacy, although it might be ‘unnecessary’ or ‘unreasonable.’ An invasion of a plaintiff’s right to privacy is important if it exposes private facts to a public whose knowledge of those facts would be embarrassing to the plaintiff.”), *overruled in part on other grounds by Bradley v. Saranac Cmty. Sch. Bd. of Educ.*, 455 Mich. 285, 565 N.W.2d 650, 658 (1997)).

relationship with that boss. Put another way: “Our interests in privacy have to do with relating to others on our own terms.”<sup>65</sup>

The relationship between an individual and a police officer is inherently “asymmetric and laden with potential consequences. Unlike virtually any other person, an investigating police officer has the power to place a citizen at the mercy of the State. We have the greatest interest in keeping our private information from someone who could do the most damage with it.”<sup>66</sup>

Because law enforcement is engaged in the competitive enterprise of ferreting out crime, police officers are, by definition, not a detached individual because they carry a certain perspective. A truly detached individual, like a magistrate judge,

might authorize a search of a person, including his pockets, without any particular basis for thinking that evidence will be found in the person’s pocket as opposed to elsewhere on his person. But that same [judge] might permissibly refuse to authorize a search of the person’s body cavities based on evidence of similar generality. . . . This is not because a person’s rectal cavity is, in any meaningful sense, a more “particular” or “specific” location than his left pocket, but because concerns for privacy inflect our understanding of probable cause and particularity.<sup>67</sup>

For these reasons, this Court agrees with that court in that one “can[not] draw a categorical line between the probable cause inquiry and considerations of privacy.”<sup>68</sup> Privacy interests of the person to be searched are always relevant to a judicial officer issuing a warrant because “[p]articularity is not defined in purely physical terms but in terms of how human behavior delineates zones of privacy.”<sup>69</sup> This is why the Tenth Circuit has repeatedly warned about

---

<sup>65</sup> *Id.*

<sup>66</sup> *Id.*

<sup>67</sup> *Id.* at 71 (citing *United States v. Nelson*, 36 F.3d 758, 760 (8th Cir.1994) (holding that probable cause to search defendant’s “person” did not include probable cause to perform a body cavity search and that this case clearly exhibits “[t]he need to provide specificity in a warrant”)) (internal citation and footnotes omitted).

<sup>68</sup> *Id.* at 71.

<sup>69</sup> *Id.* at 71 n. 14.

searches of ESI found on computers.<sup>70</sup> The privacy implications are enormous, as Judge Kleinfeld poignantly points out:

There are just too many secrets on people's computers, most legal, some embarrassing, and some potentially tragic in their implications, for loose liberality in allowing search warrants. Emails and history links may show that someone is ordering medication for a disease being kept secret even from family members. Or they may show that someone's child is being counseled by parents for a serious problem that is none of anyone else's business. Or a married mother of three may be carrying on a steamy email correspondence with an old high school boyfriend. Or an otherwise respectable, middle-aged gentleman may be looking at dirty pictures. Just as a conscientious public official may be hounded out of office because a party guest found a homosexual magazine when she went to the bathroom at his house, people's lives may be ruined because of legal but embarrassing materials found on their computers. And, in all but the largest metropolitan areas, it really does not matter whether any formal charges ensue—if the police or other visitors find the material, it will be all over town and hinted at in the newspaper within a few days. . . . Sex with children is so disgusting to most of us that we may be too liberal in allowing searches when the government investigates child pornography cases. The privacy of people's computers is too important to let it be eroded by sexual disgust.<sup>71</sup>

The Supreme Court has begun addressing the impact of technology on privacy. In each case, the Court found that, on balance, an individual's right to privacy outweighed the government's interest in effectively prosecuting suspected criminals. In *Kyllo v. United States*, the Court found a privacy interest in an individual's heat signatures in part because of the implications that data

---

<sup>70</sup> See, e.g., *United States v. Burgess*, 576 F.3d 1078, 1093 (10th Cir. 2009) (“As the description of such places and things becomes more general, the method by which the search is executed become more important—the search method must be tailored to meet allowed ends. And those limits must be functional. . . . Respect for legitimate rights to privacy in papers and effects requires an officer executing a search warrant to first look in the most obvious places and as it becomes necessary to progressively move from the obvious to the obscure.”); *United States v. Carey*, 172 F.3d 1268, 1275 (10th Cir. 1999) (“Where officers come across relevant documents so intermingled with irrelevant documents that they cannot feasibly be sorted at the site, the officers may seal or hold the documents pending approval by a magistrate of the conditions and limitations on a further search through the documents. . . . The magistrate should then require officers to specify in a warrant which type of files are sought.”); *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009) (“The modern development of the personal computer and its ability to store and intermingle a huge array of one's personal papers in a single place increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs, and accordingly makes the particularity requirement that much more important.”).

<sup>71</sup> *United States v. Gourde*, 440 F.3d 1065, 1077–78 (9th Cir. 2006) (Kleinfeld, J., dissenting). His point about child pornography cases could not be more apt, especially here in the Tenth Circuit where computer searches often involve child pornography either because it was the target of the investigation or because law enforcement found child pornography in its computer search for evidence of unrelated charges. See, e.g., *Burgess*, 576 F.3d at 1078.

suggests—such as when the “lady of the house takes her daily sauna and bath—a detail that many would consider ‘intimate.’”<sup>72</sup> In *United States v. Jones*, the Court was concerned about GPS tracking and the data it produces about an individual such as one’s “familial, political, professional, religious, and sexual associations.”<sup>73</sup> In *Riley v. California*, the Court found a privacy interest in cellular phones because of the vast amount of data about an individual that can be found on the device.<sup>74</sup> Email is no different.

So what consequences does authorizing the seizure and/or search of an entire email account have on an individual’s privacy? Here are some examples.

- Person A is suspected of tax fraud. The warrant authorizes the search of Person A’s Hotmail account to look for evidence of tax fraud. In the course of the search, law enforcement discovers Person A has enlisted via email a hitman to kill someone. The government charges Person A with attempted murder and solicitation.
- Person B is suspected of possessing child pornography. The warrant authorizes the search of Person B’s computer hard drive. In the forensic search, law enforcement discovers Person B has conspired with others to defraud the investors of his business. The government uses that evidence against Person B in a suit for corporate conspiracy and fraud, arguing that because images can be “hidden” in many file types, the evidence is admissible under the plain view doctrine.

---

<sup>72</sup> 533 U.S. 27, 38 (2001).

<sup>73</sup> \_\_\_ U.S. \_\_\_, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring) (citing *People v. Weaver*, 12 N.Y.3d 433, 441–442, 882 N.Y.S.2d 357, 909 N.E.2d 1195, 1199 (2009) (“Disclosed in [GPS] data ... will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on”)).

<sup>74</sup> *Riley*, 134 S. Ct. at 2495 (“The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought.”). The Court will discuss *Riley* in more detail later in this opinion.

- Person C is suspected of drug trafficking. The warrant authorizes the search of Person C's email account. Law enforcement discovers emails about an affair Person C was having. In court on charges of drug trafficking, the government attempts to use the emails regarding the affair as impeachment testimony.
- Person D, a high school principal, is suspected of tax evasion. The warrant authorizes the search of Person D's email account. Law enforcement discovers emails that suggests—but does not prove—an inappropriate relationship between Person D and a student at the school. Even though law enforcement never charges Person D with any crime, including the tax evasion, the information leaks to the press or Twitter. As a result, Person D loses his job. What is more, this type of information is so damaging that Person D cannot get hired in a similar position anywhere. Person D has therefore lost his entire livelihood despite not being charged with a single crime.

While these are just hypothetical examples, the real case of *United States v. Ganius* highlight the dangers of authorizing, without limitation, the seizure and subsequent search of massive amounts of ESI. Professor Kerr recounts the facts of *Ganius*:

Ganius is an accountant whose computers were searched twice pursuant to two different warrants. First, in 2003, agents investigating Ganius's clients obtained and executed a warrant for client files stored on Ganius's computers. At the physical search stage, the agents made image copies of all three of Ganius's computer hard drives on site and brought the images into government custody for later analysis. By December 2004, the agents had searched the images and separated out the files that were responsive to the warrant from the files that were nonresponsive.

The second search occurred in 2006. By that time, agents developed probable cause to believe that Ganius himself was also guilty of crimes. Ganius had by then already deleted the incriminating data that had been stored on his computers. But this didn't stop the case as the agents already had a copy of his files from the 2003 search. The incriminating evidence was in the set of nonresponsive files from the 2003 warrant that remained in government custody. The agents sought and obtained a second warrant to search the 2003 copies of Ganius's files for

Ganias's own offenses. Executing the 2006 warrant on the copies in government custody revealed evidence of Ganias's crime.<sup>75</sup>

The Second Circuit, in a now-vacated opinion, held that the 2003 warrant authorized the indefinite seizure of responsive files, but it did not give the agents unlimited authority to indefinitely seize and then use nonresponsive files.<sup>76</sup> The Court further held that obtaining the 2006 warrant did not cure the wrongful, permanent seizure of non-responsive files because it “reduces the Fourth Amendment to a form of words.”<sup>77</sup> So even though the Court has couched its argument in terms of general warrants, the Court is simultaneously discussing Americans' right to privacy and the governmental intrusions into that privacy that these types of warrants authorize. These privacy concerns underlie the remainder of this Memorandum Opinion.

### **C. Application to the Instant Application**

The Application can be divided into two sections, reflecting Rule 41's Two-Step Procedure: Paragraphs 2 and 3 reflect Step One, and paragraph 4 reflects Step Two. Paragraph 2 states the government wishes to search “information associated with [the three target email addresses] that is stored at premises controlled by Microsoft.” Paragraph 3 directs Microsoft to disclose to the government “copies of information (including the content of communications) that is within the possession, custody, or control of [Microsoft], including any emails, records, files, logs, or information that has been deleted but is still available to [Microsoft], or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f).”<sup>78</sup> Paragraph 4 of the

---

<sup>75</sup> Kerr, *Use Restrictions*, 48 Tex. Tech L. Rev. at 31 (internal footnotes and citations omitted); *see also Ganias*, 755 F.3d at 138.

<sup>76</sup> *Ganias*, 755 F.3d at 138.

<sup>77</sup> *Ganias*, 755 F.3d at 138 (quoting *Silverthorne Lumber Co. v. United States*, 251 U.S. 385, 392 (1920)).

<sup>78</sup> The Court notes that, while the government often cites its use of preservation requests under § 2703(f), this is the first time the Court can remember the government indicating it renewed its preservation request for the one-time, additional time of 90 days, as allowed under § 2703(f)(2). It is also the first time the Court can remember the government *seeking* a search warrant within that one-time renewal period, as seems to be the intent of subsection (f).

application authorizes the government to review the information provided by Microsoft. It sets limitations on what ESI the government may seize. In this case, the government may seize evidence of the crimes under investigation (conspiracy, access device fraud, computer intrusion, wire fraud, and copyright infringement) that have occurred after a specific time period (September 7, 2008–Present) and/or relate to several named persons and usernames or a web address. None of those limitations applies to paragraphs 2 and 3. The Court will address these separately but in reverse order because the problems with particularity as to the things to be seized underscore the problems with particularity as to the place to be searched.

*1. Application Paragraph 4—Step Two, or the Things to be Seized*

Paragraph 4 of the Application authorizes the government to review the information provided by Microsoft and specifies what the government may seize for its investigation. The Court remains concerned that the warrant is overly broad as to the things to be seized. Even though the government has established probable cause to seize ESI occurring since September 7, 2008 that is related to violations of specific statutes and/or seven people or entities, the government has not established probable cause as to the rest of the ESI, which it has seized upon disclosure from Microsoft.<sup>79</sup> While nothing in § 2703<sup>80</sup> or Fed. R. Crim. P. 41 may specifically preclude the government from requesting all ESI contained within a specific email account, the Fourth Amendment does.

The Court remains concerned that each of the target email accounts may—and likely do—contain large numbers of emails and files unrelated to the alleged crimes being investigated

---

<sup>79</sup> There is considerable debate as to whether the “disclosure” under § 2703 should be characterized as a search, seizure, both, or none. *See Digital Duplications and the Fourth Amendment*, 129 Harv. L. Rev. 1046 (2016).

<sup>80</sup> *See United States v. Deppish*, 994 F.Supp.2d 1211, 1219–21 & n. 37 (D. Kan. 2014) (noting that “nothing in § 2703 precludes the Government from requesting the full content of a specified email account”). The Court notes that *Deppish* did not overrule this Court’s email opinion(s); rather, *Deppish* distinguished the case law this Court relied upon from the facts of in *Deppish*.

and/or for which the government has no probable cause to search or seize. *Email II* explained these warrants are akin to “a warrant asking the post office to provide copies of all mail ever sent by or delivered to a certain address so that the government can open and read all the mail to find out whether it constitutes fruits, evidence or instrumentality of a crime. The Fourth Amendment would not allow such a warrant and should therefore not permit a similarly overly broad warrant just because the information sought is in electronic form rather than on paper.”<sup>81</sup>

*Riley* bolsters that conclusion.<sup>82</sup> While *Riley* only decided whether a search of a cellphone incident to lawful arrest required a warrant, the Court’s dicta concerning the intersection of technology and privacy vis-à-vis the Fourth Amendment nevertheless reinforces this Court’s interpretation of the Fourth Amendment’s probable cause and particularity requirements and underscores why a search protocol is necessary.

Almost every statement made in *Riley* with respect to cell phones applies equally to email accounts. “One of the most notable distinguishing features of modern cell phones is their immense storage capacity . . . [of which] the current top-selling smart phone has a standard capacity of 16 gigabytes (and is available with up to 64 gigabytes)”<sup>83</sup> A free email account from a major provider such as Google, Yahoo!, or Microsoft comes with *at least* 15 gigabytes of storage.<sup>84</sup> “Cell phones couple that capacity with the ability to store many different types of information . . . [such as] photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on.”<sup>85</sup> Email is no different. As with

---

<sup>81</sup> *Email II*, 2013 WL 4647554, at \*8.

<sup>82</sup> *Riley*, 134 S. Ct. at 2495 (“The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought.”).

<sup>83</sup> *Id.* at 2489. Indeed, “[s]ixteen gigabytes translates to millions of pages of text, thousands of pictures, or hundreds of videos.” *Id.*

<sup>84</sup> See, e.g., [https://en.wikipedia.org/wiki/Comparison\\_of\\_webmail\\_providers](https://en.wikipedia.org/wiki/Comparison_of_webmail_providers) (last visited March 21, 2016).

<sup>85</sup> *Riley*, 134 S. Ct. at 2489.



“apps” on cellular phones, “[t]here are [emails] for Democratic Party news and Republican Party news; [emails] for alcohol, drug, and gambling addictions; [emails] for sharing prayer requests; [emails] for tracking pregnancy symptoms; [emails] for planning your budget; [emails] for every conceivable hobby or pastime; [emails] for improving your romantic life.”<sup>86</sup> Needless to say, a person’s email account may reveal their “privacies of life.”<sup>87</sup>

Like cell phones, an email account is often the home of a person’s identity—both on- and off-line, but especially on-line. An email address is required for almost every online service, including Facebook, Twitter, Instagram, Amazon, Foursquare, LinkedIn, and TurboTax. Because of this, an email account may contain such an aggregate of information from each online service so as to constructively contain an image of those outside accounts. Consider Facebook. Jane Doe may allow Facebook to send her an email for each friend request, invitation to an event, “like” or comment on their status, private message, or transfer of money to a friend. If the government is allowed to seize and search Jane’s entire email account, it could potentially reconstruct Jane’s entire Facebook account. Or consider Foursquare, which allows users to “check-in” at a location. Once an Email Provider discloses all ESI associated with a target account, the government may have that individual’s whereabouts for the past day, week, month, or even several years, which is precisely what concerned Justice Sotomayor in *United States v. Jones*.<sup>88</sup> The search of an email account “would typically expose to the government far *more* than the most exhaustive search of a house: [An email account] not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private

---

<sup>86</sup> *Riley*, 134 S. Ct. at 2490 (edited by this Court by substituting the word “emails” for the word “apps”).

<sup>87</sup> *Riley*, 134 S. Ct. at 2495.

<sup>88</sup> 565 U.S. —, —, 132 S.Ct. 945, 955, 181 L.Ed.2d 911 (2012) (Sotomayor, J., concurring) (“GPS monitoring generates a precise, comprehensive record of a person’s public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.”)

information never found in a home in any form.”<sup>89</sup> The Court is therefore concerned that targeting email addresses may be used as a way to gain a two-for-one warrant special—wherein the government gains both the email account and a reconstruction of the account holder’s other social media accounts without obtaining a separate warrant for those accounts.

With those general concerns in mind, the Court will turn to its specific concerns with the instant Application. Paragraph 4 of the application authorizes the government to review of the information provided by Microsoft. It is sufficiently particular in that it links the information to be seized to the alleged crimes—18 U.S.C. §§ 371 (conspiracy), 1029 (access device fraud), 1030 (computer intrusion), 1343 (wire fraud), and 2319 (copyright infringement). It is also sufficiently particular in that it limits the seizure of evidence to that occurring since September 7, 2008. To its credit, the government attempts to be even more particular by limiting its seizure to information “involving [redacted], and others known and unknown.” The government has established probable cause as to [redacted]. However, the government has not established probable cause as to [redacted] because those identifiers do not appear in the rest of the application. The Court could infer a connection between those identifiers and other pieces of evidence discussed in the rest of the application.<sup>90</sup> But the Court cannot find probable cause based solely on such inferences. This is especially true when dealing with internet accounts, where email addresses and usernames do not necessarily correspond with anything in particular. The government may suspect a John Smith and it may have identified a John1@hotmail.com email account. But without any direct connection between the John1 email account and the

---

<sup>89</sup> *Riley*, 134 S. Ct. at 2491.

<sup>90</sup> [redacted]’s first name matches an email account referenced in the rest of the application ([redacted]); [redacted] shares a last name with [redacted], the person who owns one of the target email accounts and for which the government has shown probable cause; and [redacted]’s first name is a partial match to the username [redacted] and his last name matches a web address ([redacted]) listed in the rest of the application. As for the [redacted], the Court could infer that it is a user of the [redacted], the place in which the government believes the illicit scheme took place.

particular John Smith the government suspects, the Court cannot find probable cause. After all, there will likely be many Hotmail email accounts using a first or last name and a number (John1, John2, John3, etc.). And *the* John Smith the government suspects may be the owner of John15@hotmail.com—not John1@hotmail.com. Given that a single character may separate the accounts of a suspect and an innocent person, and because of the massive amounts of data an email account can—and likely does—contain, courts should require a higher showing of particularity. Unlike in search warrants for physical searches, practical accuracy<sup>91</sup> may not suffice in the digital world, for the risk of searching and/or seizing innocent peoples’ communications is high.<sup>92</sup> Accordingly, the government has not shown probable cause to seize ESI related to named people, who are never mentioned in rest of the application and are only connected by inference to some other part of a piece of evidence that is referenced in the rest of the application. The same goes for the username that goes wholly unmentioned, and more importantly lacks any inferential connection to a part of a piece of evidence. For these reasons, the Court finds the government’s application lacks probable cause to search for or seize items related to [redacted].

The Court is also concerned with the inclusion of the phrase “and others known and unknown,” which follows the list of people, usernames, and the domain name. The Court believes the government included this phrase to cover the seizure of evidence that it may come across during the course of searching the target email accounts. In other words, the Court construes the phrase to mean that, should the government, in its search of the target email

---

<sup>91</sup> See *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009) (“It is true that practical accuracy rather than technical precision controls the determination of whether a search warrant adequately describes the place to be searched [or things to be seized].”) (internal quotation marks and citation omitted).

<sup>92</sup> Even a clerical typo could result in a massive privacy violation.

accounts, connect the username “Megatron135”<sup>93</sup> with either the named statutes or named people for which the government has established probable cause, it be allowed to seize that content even though “Megatron135” was not expressly named in the warrant. Or, as *SDNY Email* puts it:

[I]n 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.<sup>94</sup>

This Court believes that phrase runs afoul of the particularity requirement of the Fourth Amendment because of the difference between the physical world and the digital world. As discussed earlier, a single letter or digit could be the difference between an individual for which the government has probable cause and a person for which the government does not have probable cause. For instance, in this case, say the government observes that “pipeline” refers to a particular computer vulnerability. On those facts, this Court might agree that evidence may be seized. In contrast, “Megatron135” may in fact be an innocent third party, whose communications have now been seized even though the government has not shown probable cause that Megatron135 is related to the scheme. Put another way, words referring to drugs present little, if any, risk of constitutional infringement, whereas people’s names or usernames—obtained through a search of someone else’s email account—present a high risk of constitutional infringement regarding the third party’s right to privacy.

Similarly, if the government already suspects other names or usernames, why are they left unnamed in the application? The Court believes this is because the government may not have enough to establish probable cause as to those identifiers—indeed, the government has not

---

<sup>93</sup> This is a fictitious username the Court is using for illustrative purposes.

<sup>94</sup> *SDNY Email*, 33 F. Supp. 3d at 398 (using that example to justify indefinite retention of the seized material).

shown probable cause as to some of the people or usernames they specifically mention. While *SDNY Email* and *DC District Email* may believe this is permissible because *Dalia* gives law enforcement broad discretion in executing a warrant and such execution is later subject to judicial review as to its reasonableness, this Court is not prepared to authorize a warrant that includes a clause covering *every* third-party that interacted with a target email account. After all, “[a]s to what is to be taken, nothing is left to the discretion of the officer executing the warrant.”<sup>95</sup> Here, assuming the Court granted the Application, an executing officer has unlimited discretion. There is a simple fix that alleviates the Courts concerns: get another warrant that outlines the probable cause to seize the communications of these previously unknown but now-suspected third parties. *Riley* emphasized that technology has increased the speed and efficiency with which law enforcement may obtain a warrant.<sup>96</sup>

Given the vast amount of information potentially contained in an individual’s email account, the Court finds the current Application violates the Fourth Amendment’s probable cause and particularity requirements. But, as will be explained later, the Court believes these concerns may be alleviated through the use of *ex ante* instructions. Before discussing some of those instructions, the Court addresses its concern regarding particularity with respect to the place to be searched.

## 2. Application Paragraphs 2 & 3—Step One, or the Place to be Searched

Application paragraphs 2 and 3 implement Step One of Rule 41’s Two-Step Procedure, which, in turn, addresses the “place to be searched” as used in the Fourth Amendment. “To

---

<sup>95</sup> *Marron*, 275 U.S. at 196.

<sup>96</sup> *Riley*, 134 S. Ct. at 2493 (“Recent technological advances similar to those discussed here have, in addition, made the process of obtaining a warrant itself more efficient.”) (citing *Missouri v. McNeely*, 569 U.S. \_\_\_, \_\_\_, 133 S.Ct. 1552, 1773 (2013) (Roberts, C.J., concurring in part and dissenting in part) (describing jurisdiction where “police officers can e-mail warrant requests to judges’ iPads [and] judges have signed such warrants and e-mailed them back to officers in less than 15 minutes”)).

determine if the *place* to be searched is particularly described, courts ask whether the description is sufficient ‘to enable the executing officer to locate and identify the premises with reasonable effort, and whether there is any reasonable probability that another premise might be mistakenly searched.’”<sup>97</sup> The Court finds this Application is not sufficiently particular with respect to the *place* to be searched. *SDNY Email* and *DC District Email* both conclude that the identification of the target email address itself—here, [redacted]@hotmail.com—is a sufficiently particular description.<sup>98</sup> That view is tempting because, after all, Microsoft will only disclose the ESI of the target email address listed in the warrant, making it virtually impossible that an executing officer might mistakenly search another “premises.” But this Court disagrees for two interrelated reasons, and it is for these reasons the Court believes that these types of warrants should include *ex ante* instructions.

First, as scary as this may sound to those who value privacy, the Court is unaware of any court ever holding that the government lacked probable cause to investigate an email address (or IP address) because it was described as the place to be searched in the warrant.<sup>99</sup> Allowing the government to define the “place to be searched” as the target email address—[redacted]@hotmail.com—is problematic. As Georgetown Law Professor Paul Ohm explains,

*[A]t almost every stage of almost every criminal investigation on the Internet, the police have either probable cause or no suspicion at all, but they almost never fall somewhere in between these extremes. . . . [We] almost never stumble upon decontextualized e-mail addresses or IP addresses--the two most important types of evidence online. Instead, we find them attached to things like e-mail messages and logfiles, and thanks to some characteristics of the Internet, they are almost never “somewhat suspicious” or “out of place,” “kind of fishy” or “just not right.”*

---

<sup>97</sup> *United States v. Lora–Solano*, 330 F.3d 1288, 1293 (10th Cir. 2003) (quoting *United States v. Pervaz*, 118 F.3d 1, 9 (1st Cir.1997)).

<sup>98</sup> See, e.g., *DC District Email*, 13 F. Supp. 3d at 164.

<sup>99</sup> See also Nicole Friess, *When Rummaging Goes Digital: Fourth Amendment Particularity and Stored E-Mail Surveillance*, 90 Neb. L. Rev. 971, 983 (2012) (citing Paul Ohm, *Probably Probable Cause: The Diminishing Importance of Justification Standards*, 94 Minn. L. Rev. 1514, 1516 (2010)).

Instead, when the police find an e-mail address or IP address that they think is related to a crime, they almost always know that a request for more information about the address will lead either to information relevant to the investigation or to a dead end.<sup>100</sup>

The Court agrees with the italicized conclusion, as it strains to imagine a scenario where police would lack probable cause to search an email account.<sup>101</sup> All a magistrate judge must find for probable cause is a fair probability that contraband or evidence of a crime will be found in a particular place. If that place is an email account, there is almost always a fair probability that evidence of some sort might be found there. Indeed, a person who committed some statutory offense—knowingly or not—may have sent an email to *someone* that may be of use to the government’s investigation. Perhaps the owner sent an email about the act that violated the law, about the victim, or about some other piece of evidence; perhaps one of the account owner’s web-based services emailed back registration information that is pertinent to the investigation; or perhaps the email account will identify co-conspirators. Moreover, “steps in online investigations never lead to fragments of IP addresses or pieces of suspicious e-mail addresses.”<sup>102</sup> “An e-mail address cannot point to short men, or experienced computer users or men with moustaches” nor can it “narrow down the suspect pool without pointing the finger directly at the target, as real-world evidence often does.”<sup>103</sup> This has led commentators to conclude that the probable cause requirement of the Warrant Clause is essentially meaningless in

---

<sup>100</sup> Ohm, *Probably Probable Cause*, 94 Minn. L. Rev. at 1524–25 (emphasis added).

<sup>101</sup> For instance, consider the suspect committed common-law trespass on his neighbors land. There is a fair probability that the suspect’s email account may contain incriminating evidence regarding the incident. Perhaps there is evidence of the incident, dialogue between the suspect and the neighbor, the suspect’s state of mind, or the suspect’s personal views about the neighbor.

<sup>102</sup> Ohm, *Probably Probable Cause*, 94 Minn. L. Rev. at 1528.

<sup>103</sup> *Id.*

the digital world.<sup>104</sup> This Court agrees, but believes it may be remedied by strengthening the particularity requirement through *ex ante* instructions.

Second, by describing the place to be searched as the target email address, the government “overseiz[es] data and then using the process of identifying and segregating seizable electronic data ‘to bring constitutionally protected data . . . into plain view.’”<sup>105</sup> Many commentators are concerned with the plain view doctrine in the context of searches for ESI.<sup>106</sup> So was the *NDCal Email* court.<sup>107</sup> *Riley* implicitly shares this concern, observing that the search of a cell phone may be more revelatory than the search of a *home*.<sup>108</sup> Courts have often required<sup>109</sup>—and the government has often provided<sup>110</sup>—highly particularized descriptions of the

---

<sup>104</sup> See Friess, *Rummaging Goes Digital*, 90 Neb. L. Rev. at 983; Ohm, *Probably Probable Cause*, 94 Minn. L. Rev. at 1516.

<sup>105</sup> *Matter of Black iPhone 4*, 27 F. Supp. 3d 74, 79 (D.D.C. 2014) (quoting *United States v. Schesso*, 730 F.3d 1040, 1047 (9th Cir. 2013)); see also *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1171 (9th Cir. 2010).

<sup>106</sup> See, e.g., Ray Ming Chang, *Why the Plain View Doctrine Should Not Apply to Digital Evidence*, 12 Suffolk J. Trial & App. Advoc. 31 (2007) (arguing courts should eliminate the plain view doctrine as to digital evidence); Kaitlyn R. O’Leary, *What the Founders Did Not See Coming: The Fourth Amendment, Digital Evidence, and the Plain View Doctrine*, 46 Suffolk U. L. Rev. 211, 224 (2013) (discussing courts’ struggle with the plain view doctrine and digital evidence); Bryan K. Weir, *It’s (Not So) Plain to See: The Circuit Split on the Plain View Doctrine in Digital Searches*, 21 Geo. Mason U. Civ. Rts. L.J. 83 (2010) (recommending the abolition of the plain view doctrine); James Saylor, *Computers As Castles: Preventing the Plain View Doctrine from Becoming A Vehicle for Overbroad Digital Searches*, 79 Fordham L. Rev. 2809 (2011) (advocating *ex ante* restrictions in light of the problems the plain view doctrine presents with respect to digital searches).

Professor Orin Kerr initially advocated narrowing or potentially eliminating the plain view exception for digital searches. See Orin S. Kerr, *Searches and Seizures in A Digital World*, 119 Harv. L. Rev. 531, 576–84 (2005). Kerr concedes this position has considerable merit in light of *Riley*, but now favors “use restrictions” instead. See Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 Tex. Tech L. Rev. 1, 4 (2015).

<sup>107</sup> *NDCal Email*, 62 F. Supp. 3d at 1104 (“This unrestricted right to retain and use every bit Google coughs up undermines the entire effort the application otherwise makes to limit the obvious impact under the plain view doctrine of providing such unfettered government access.”).

<sup>108</sup> *Riley*, 134 S. Ct. at 2491 (noting cell phones “would typically expose to the government far *more* than the most exhaustive search of a house” including “a broad array of private information never found in a home in any form.”). In fact, the government has argued in other cases that the search of a computer hard drive is akin to the search of a house. *Galpin*, 720 F.3d at 447 n. 6.

<sup>109</sup> See, e.g., *United States v. Muse*, 729 F. Supp. 2d 905, 910 (E.D. Mich. 2010) (“When a single structure houses several discrete units, the terms of the search warrant will prescribe which units within that structure may be searched lawfully.”); *Kao v. Markel Ins. Co.*, 708 F. Supp. 2d 472, 478 (E.D. Pa. 2010) (finding warrant overbroad where it described “a multi-unit building without specifying any particular sub-unit”); *Jacobs v. City of Chicago*,



place to be searched in warrants to search a home. “Even in traditional contexts, a judicial officer may restrict a search to only a portion of what was requested—a room rather than an entire house, or boxes with certain labels rather than an entire warehouse.”<sup>111</sup> In other words, some ex ante constraints—of the form “ here, not there”—are perfectly acceptable. The Court wants the same degree of particularization with respect to digital searches. That is why the Court has previously requested the government provide a search protocol that explains how the government intends to search the hard drive(s). As the Supreme Court of Vermont adeptly noted: “In the digital universe, particular information is not accessed through corridors and drawers, but through commands and queries. As a result, in many cases, the only feasible way to specify a particular ‘region’ of the computer will be by specifying how to search.”<sup>112</sup> By providing a search protocol explaining how the government will separate what is permitted to be seized from what is not, the government can more easily and satisfactorily explain to the court how it will decide where it is going to search. In doing so, the government should not compromise the thoroughness of its description by trying to avoid the use of technical language. In fact, the court *wants* a “sophisticated technical explanation of how the government intends to

---

215 F.3d 758, 768 (7th Cir. 2000) (“We have consistently held that probable cause to search one apartment in a multi-unit building does not support a warrant authorizing a search of the entire building.”);

<sup>110</sup> Consider the government’s level of specificity in warrants for homes. *See, e.g., United States v. Dobbins*, 482 F. App’x 35, 39 (6th Cir. 2012) (“The target structure is located at 3007 Batavia Street. The target structure is [*sic*] one story residential triplex. The target structure is red brick with white trim. Facing the target structure from Batavia Street there are the numbers 3007 over the number 1 affixed upon a door which faces Batavia Street. Facing the target structure from Batavia Street the target door is located on the left side of the target structure. Facing this side of the target structure the target door is the door on the left. The target door is the second door from Batavia Street on this side of the target structure. The target door is tan in color. The search shall also include all outbuildings, outhouses and storage buildings, all vehicles found thereon, and all vehicles in close proximity which have a nexus to the location or persons present at the location for the aforesaid evidence. . . .”).

<sup>111</sup> Vermont Warrant, 193 Vt. at 69.

<sup>112</sup> Vermont Warrant, 193 Vt. at 71.

conduct the search so that [it] may conclude that the government is making a genuine effort to limit itself to a particularized search.”<sup>113</sup>

Both *SDNY Email* and *DC District Email* brush aside the concern about oversteering data in Rule 41’s Step One because “[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.”<sup>114</sup> In other words, courts have always allowed oversteering of documents so that the government may sift through them to decide which documents fall within the scope of the warrant and which do not. However, this Court believes that *Riley* is clear: continuing to apply that physical search precedent to digital searches is ill-suited for today’s increasingly digital world because digital searches may reveal far more than a search of a home, which “when it comes to the Fourth Amendment, the home is first among equals.”<sup>115</sup> Moreover, the precedent upon which *SDNY Email* and *DC District Email* rely held so because an on-site search of a computer for the evidence sought by a warrant is not practical or even possible in some instances because of “the technical difficulties of conducting a computer search in a suspect’s home.”<sup>116</sup> Conducting a computer search on-site—at the suspect’s home—is often more intrusive to an individual’s privacy<sup>117</sup> because the search of the vast amount of ESI found on a hard drive may take “months to complete. It would be impractical for agents to occupy an individual’s home or office, or seize an individual’s

---

<sup>113</sup> *Matter of the Search of Apple iPhone, IMEI 013888003738427*, 31 F. Supp. 3d 159 (D.D.C. 2014) (citing *Odys Loox*, 28 F. Supp. 3d 40.).

<sup>114</sup> *SDNY Email*, 33 F. Supp. 3d at 391 (citing *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)).

<sup>115</sup> *Florida v. Jardines*, 133 S. Ct. 1409, 1414 (2013).

<sup>116</sup> *Guest v. Leis*, 255 F.3d 325, 335 (6th Cir. 2001).

<sup>117</sup> *United States v. Summage*, 481 F.3d 1075, 1079–80 (8th Cir. 2007).

computer, for such long periods of time.”<sup>118</sup> Accordingly, courts have sanctioned Rule 41(e)(2)(B)’s “seize first, search later” Two-Step Procedure.<sup>119</sup> To reflect that case law, Federal Rule of Criminal Procedure 41 was amended in 2009, explicitly providing:

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.<sup>120</sup>

As the text makes clear, Rule 41(e)(2) is a codification of courts’ recognition that on-site searches of computer hard drives are infeasible and that courts should authorize later, off-site searches (often in the government’s forensic laboratories). The Advisory Committee’s notes to the 2009 amendments make this explicitly clear: “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*

---

<sup>118</sup> *Ganias*, 755 F.3d at 135 (“In 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.”) (emphasis added).

<sup>119</sup> See *SDNY Email*, 33 F. Supp. 3d at 392 (citing *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. Grimmitt*, 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].”).

<sup>120</sup> Fed. R. Crim. P. 41(e)(2)(B).

location.”<sup>121</sup> Finally, the Advisory Committee specifically instructed that “[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.”<sup>122</sup> Thus, *SDNY Email* and *DC District Email*’s reliance on Rule 41 itself as a basis to find sufficient particularity is misplaced.

In the email context, however, these concerns are completely absent. Law enforcement is never “on-site.” No officer steps foot in a suspect’s home, and no officer conducts the imaging of the email account. Simply put, Rule 41—both textually and practically—was not intended to apply to searches of email accounts. The obvious counter-argument to this is that, if Rule 41’s Two-Step Procedure does not apply, the government is required to be on-site—at Microsoft’s server facility.<sup>123</sup> It follows that it would be impractical for agents to occupy Microsoft’s facility during a search that may take months to complete. While that may be true, the Court is supposed to strike the proper balance “between protecting an individual’s right to privacy and ensuring that the government is able to prosecute suspected criminals effectively.”<sup>124</sup> The *individual* to whom the Ninth Circuit refers in that quote is the citizen under investigation—not a third party whose only relation to the case is that it stores that particular citizen’s ESI. If an individual’s use of email—a technology that society has unquestionably embraced—allows the government to circumvent the individual’s right to privacy in her ESI by obtaining that ESI through the Email Provider, the individual has—probably unknowingly—outsourced her constitutional right to

---

<sup>121</sup> Fed. R. Crim. P. 41(e)(2) advisory committee note.

<sup>122</sup> Fed. R. Crim. P. 41(e)(2) advisory committee note.

<sup>123</sup> The Court acknowledges that no officer must be present during the execution of a warrant under § 2703(g).

<sup>124</sup> *Adjani*, 452 F.3d at 1152 (9th Cir. 2006).

privacy to providers of remote computing or communications software or tools.<sup>125</sup> Americans may be unwilling to make that trade. While the issue of how courts should grapple with that Fourth Amendment oddity is outside the scope of this opinion, the Court discusses the concern because the easy compromise is allowing the government to obtain the full image of the email account from the Email Provider but subjecting it to *ex ante* instructions. Such a solution strikes the proper balance between an individual’s right to privacy and the government’s ability to prosecute suspected criminals effectively. Moreover, “the premise of the 2009 amendment—that law enforcement had to open every file and folder to search effectively—may simply no longer be true.”<sup>126</sup>

For these reasons, the Court believes the place to be searched is not sufficiently particular. The Court may sanction the use of the email address as a description of the place to be searched, but only once the government provides a search protocol explaining to the Court how it intends search the overzealous-ESI and what it will do with the non-responsive data once the search has been completed. Only then can the Court properly weigh the balance between the government’s effective investigation and sanction the wholesale seizure of all ESI in an individual’s email account.

For these reasons, the Court finds the instant Application violates the particularity requirement of the Fourth Amendment. Even though the Court finds the instant Application

---

<sup>125</sup> This underscores another difference between physical-world Rule 41 seizures and searches of computer (or device) hard drives and digital-world Rule 41 seizures and searches: notice to the individual whose belongings are seized and/or searched. In most, if not all, of the cases where courts have upheld Rule 41’s Two-Step Procedure, courts have done so in searches of physical hard drives obtained through a search warrant on a physical premise, such as a home or office. As such, the individual has notice of the seizure and subsequent search of his various computers or devices. By contrast, an individual has no notice of the seizure and subsequent search of his or her email account, even under Rule 41. Indeed, § 2703(b)(1)(A) expressly allows the government to prohibit an Email Provider from noticing its customer that his information has been disclosed to the government.

<sup>126</sup> *DC Facebook*, 21 F. Supp. 3d at 11.

violates the Fourth Amendment’s probable cause and particularity requirements, the Court believes many, if not all, of the violations could be cured with court-issued *ex ante* instructions.

### **C. *Ex Ante* Instructions that Help Strike the Proper Balance of Interests**

In its previous email opinions, the Court suggested some possible *ex ante* instructions, including (1) asking the Email Provider to provide specific limited information such as emails containing certain key words or emails sent to/from certain recipients, (2) appointing a special master with authority to hire an independent vendor to use computerized search techniques<sup>127</sup> to review the information for relevance and privilege, or (3) setting up a filter group to review the information for relevance and privilege.

The Court notes that the Tenth Circuit has not required a particularized computer search strategy—at least in warrants authorizing searches of computers. The Tenth Circuit has not spoken on the issue of whether email warrants—authorizing an Email Provider to disclose the content of all ESI in or associated with the account—require *ex ante* instructions, such as a search protocol or some limitations on the government’s search of that information. But the Tenth Circuit has suggested an approach for “intermingled documents,” in which law enforcement engages in an intermediate step of sorting various types of documents and then only searching the ones specified in a warrant.<sup>128</sup> Under this approach, “the magistrate judge should then require officers to specify in a warrant [the] type of files [that are being] sought.”<sup>129</sup>

---

<sup>127</sup> The Sedona Conference® Best Practices Commentary on the Use of Search and Information Retrieval Methods in E-Discovery, 8 Sedona Conf. J. 189, 210 (2007).

<sup>128</sup> *United States v. Carey*, 172 F.3d 1268, 1275 (10th Cir. 1999).

<sup>129</sup> *Id.* For instance, the search for an electronic ledger of drug transactions would permit the search of spreadsheet files (e.g. .XLS, .XLSX, .Numbers, etc.) but not image (.PNG, .JPG, .BMP, etc.) or video (.MOV, .MP4 .MKV, etc.) files.

As noted at the beginning of this opinion, all courts agree that magistrate judges have the authority to impose *ex ante* instructions but that *ex ante* instructions have never been required.<sup>130</sup> The Court also agrees that some *ex ante* instructions are unwise or impractical. The Court agrees with the Supreme Court of Vermont that eliminating the plain view doctrine is inappropriate,<sup>131</sup> and the Court agrees with *SDNY Email* and *DC District Email* that requiring the Email Provider to conduct the *entire* investigatory search is impractical and burdensome.<sup>132</sup> 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.

### ***1. Categorical or Keyword Limitations***

---

<sup>130</sup> See, e.g., *Vermont Warrant*, 193 Vt. at 73 (“It is a serious error, however, to infer from the fact that we must often evaluate *ex post* whether a search sufficiently respected a citizen’s privacy to the conclusion that we can make no *ex ante* judgments about what sort of privacy invasions are and are not warranted. There is interplay between probable cause, particularity, and reasonableness that judicial officers reviewing a warrant application must consider in authorizing a form of privacy invasion. We therefore reject any blanket prohibition on *ex ante* search warrant instructions.”).

<sup>131</sup> *Id.* at 75 (finding the *ex ante* abrogation of the plain view doctrine inappropriate because “it is beyond the authority of a judicial officer issuing a warrant to abrogate a legal doctrine in this way” and “requiring the segregation of the search from the investigation and limiting the results of the search that can be shared, obviate application of the plain view doctrine”).

<sup>132</sup> *SDNY Email*, 33 F. Supp. 3d at 394–96; *DC District Email*, 13 F. Supp. 3d 157, 165–66 (D.D.C. 2014) (“Enlisting a service provider to execute the search warrant could also present nettlesome problems. As the government argues persuasively in its challenge, it would be unworkable and impractical to order Apple to cull the e-mails and related records in order to find evidence that is relevant to the government’s investigation. To begin with, non-governmental employees untrained in the details of the criminal investigation likely lack the requisite skills and expertise to determine whether a document is relevant to the criminal investigation. Moreover, requiring the government to train the electronic service provider’s employees on the process for identifying information that is responsive to the search warrant may prove time-consuming, increase the costs of the investigation, and expose the government to potential security breaches.”).

The Court previously suggested that the government could ask the Email Provider to provide specific responsive information based on certain keywords or other criteria.<sup>133</sup> This has the advantage of limiting the amount of non-responsive ESI obtained by the government in its initial disclosure/seizure from the Email Provider. Such limitations come in two flavors: categorical and keyword. Categorical limitations limit the breadth of the ESI requested. For example, a date range—here, September 7, 2008 to the present—immediately cuts but does not eliminate the risk that the government is seizing data for which it lacks probable cause. There are other categorical limitations, such as only searching sent mail or excluding emails from certain websites like Facebook or Twitter.<sup>134</sup> Categorical limitations are well within the capability of Email Providers and require no investigatory expertise to perform. Neither the Email Provider nor the government is burdened by a categorical limitation like this. Indeed, even *SDNY Email* concedes that having the Email Provider limit the disclosure to the time period containing the evidence the government wishes to seize—here, that would be September 7, 2008 to the present—may be acceptable.<sup>135</sup> The Court believes this type of limitation should be required—indeed, it should be part of a sufficiently particularized warrant.

---

<sup>133</sup> Some call these “semantic searches.” See Athul K. Acharya, *Semantic Searches*, 63 Duke L.J. 393 (2013) (arguing the particularity requirement mandates some ex ante limitations and proposing limiting searches to “semantic zones”). The Court believes this article to be very persuasive and explains the methods discussed in this opinion with more technical precision.

<sup>134</sup> This mitigates the Court’s concern that law enforcement could obtain a two-for-one warrant special.

<sup>135</sup> *SDNY Email*, 33 F. Supp. 3d at 394 (“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.”); see also *[redacted]@mac.com*, 25 F. Supp. 3d at 6 (“By abusing the two-step procedure under Rule 41, the government is asking Apple to disclose the entirety of three months’ worth of e-mails and other e-mail account information. Yet, on the very next page, it explains that it will only “seize” specific items related to its criminal investigation; it goes so far as to name specific individuals and companies that, if mentioned in an e-mail, would make that e-mail eligible to be seized. Thus, the government has shown that it can “describe the items to be seized with [ ] much specificity”; it has simply chosen not to by pretending that it is not actually “seizing” the information when Apple discloses it.”).



Keyword limitations limit the responsive ESI to certain terms specified by the government. These terms may include people's names, usernames, email addresses, credit card numbers, dates, social security numbers, email addresses, etc. They might also include generic words like "dolls" or "potatoes."<sup>136</sup> Keyword limitations are a step beyond categorical limitations because they are fact specific. As such, they present problems, such as whether the government must apply for a new warrant if its investigation uncovers new keywords for which the government wishes to search. Other courts would argue these problems can be avoided by the district court evaluating the reasonableness of the government's search as a whole *ex post*. While it is true that is a possible remedy, this Court believes the government should include a list of keywords in its search protocol but that the Email Provider should not be obligated to search for those keywords. Thus, the Email Provider is in no danger of becoming an agent of the government performing the investigatory search. It also gives the district court an idea of what the government believes it will find before it has access to the tranche of data. In this way, it balances the interests between the individual's right to privacy and the government's interest in effectively investigating crime. Put another way: the government gets to overseize and execute its search on its own while the individual gets a document outlining what the government thought it may find *before it had access to the tranche of personal data* in order to make more concrete arguments at the suppression stage concerning the warrant's scope and the reasonableness of the search.

## ***2. Search Protocol***

---

<sup>136</sup> *SDNY Email*, 33 F. Supp. 3d at 398 (“[I]n a drug investigation, it might be obvious . . . 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.”).

A search protocol is a document submitted by the government to the Court that explains how the government intends to search the ESI it has obtained after the warrant is approved.<sup>137</sup> The Court is not requesting a search protocol in order to dictate how the government executes its warrant.<sup>138</sup> Nor is the Court requesting that a search protocol accompany every warrant for ESI to comply with the Fourth Amendment—for instance, a warrant to search a two-gigabyte USB drive will not need a search protocol because of the limited amount of ESI the government can obtain. The Court acknowledges that the government cannot identify the specific region or blocks<sup>139</sup> of the email account or hard drive that it needs to search ahead of time. That is why this Court has requested a search protocol, explaining how the government is going to conduct its search to minimize the risk that files outside the scope of the warrant will be discovered. The protocol should explain “how it will perform the search and ensure that it is only searching sectors or blocks of the drives that are most likely to contain the data for which there is probable cause.”<sup>140</sup> In requesting a search protocol, the Court is not dictating how to execute the warrant. The government is free to determine the best procedures and techniques to use, so long as the government provides notice as to what those procedures are. Indeed, this is perhaps the least intrusive *ex ante* instruction the Court could impose. All the government must do is educate the Court as to how it intends to minimize the discovery of ESI outside the scope of the warrant.

---

<sup>137</sup> *Vermont Warrant*, 193 Vt. at 71 (“In the digital universe, particular information is not accessed through corridors and drawers, but through commands and queries. As a result, in many cases, the only feasible way to specify a particular ‘region’ of the computer will be by specifying how to search.”).

<sup>138</sup> *See Dalia*, 441 U.S. at 238.

<sup>139</sup> *See generally* Seagate, Transition to Advanced Format 4K Sector Hard Drives, *available at* <http://www.seagate.com/tech-insights/advanced-format-4k-sector-hard-drives-master-ti/> (“For over 30 years, data stored on hard drives has been formatted into small logical blocks called sectors.”); *see also* Allen B. Tucker, *Computer Science Handbook*, Second Edition, CRC Press. p. 86. ISBN 9780203494455.

<sup>140</sup> *[redacted]@mac.com*, 13 F.Supp.3d at 153; *see also State v. Henderson*, 289 Neb. 271 (2014) (holding that a warrant authorizing the search of a cell phone’s call logs, texts, voicemail and “any other information that can be gained from the internal components and/or memory cards” was not particular enough to satisfy the requirements of the Fourth Amendment).

### ***3. Third Party Search of ESI—Special Masters, Filter Teams, or Court-Appointed Experts***

The Court has also suggested that third parties perform the search. The Court could appoint a special master or require filter teams, which are trained computer personnel separate from the investigators and operating behind a firewall. This Court believes the use of special masters or filter teams is the best way to balance the interests between the individual and government. Both are routinely used in civil cases to protect against confidential (e.g. trade secret, patent), privileged (e.g. attorney-client, HIPPA), or irrelevant materials.<sup>141</sup> Courts and commentators have advocated using these tools to ensure Fourth Amendment protection is not meaningless in the digital world.<sup>142</sup>

---

<sup>141</sup> *Vermont Warrant*, 193 Vt. at 83 (citing *Hicks v. Bush*, 452 F.Supp.2d 88, 103 (D.D.C. 2006) (allowing use of “filter teams” to protect attorney-client privilege with regard to mail seized from Guantanamo Bay detainees); *United States v. Grant*, No. 04 CR 207BSJ, 2004 WL 1171258 (S.D.N.Y. May 25, 2004) (endorsing government’s proposed “privilege team” to screen seized documents for privileged materials); *United States v. Triumph Capital Grp., Inc.*, 211 F.R.D. 31, 43 (D. Conn. 2002) (“The use of a taint team is a proper, fair and acceptable method of protecting privileged communications when a search involves property of an attorney.”); *United States v. Hunter*, 13 F.Supp.2d 574, 583 (D.Vt. 1998) (accepting the use of “screening procedure designed by the government” in order to “limit invasion of confidential or privileged or irrelevant material”); *Forro Precision, Inc. v. Int’l Bus. Mach. Corp.*, 673 F.2d 1045, 1054 (9th Cir.1982) (approving of use of IBM employees in performing a search where “search warrant required that technical documents be identified”); *Wilson v. Layne*, 526 U.S. 603, 611, 119 S.Ct. 1692, 143 L.Ed.2d 818 (1999) (approving of “the presence of the third parties” where their presence “directly aid[s] in the execution of the warrant”); see also *United States v. McClure*, No. 10–028, 2010 WL 3523030, at \*2 (E.D.La. Sept. 1, 2010) (“The subpoenaed documents at issue satisfy [the subpoena requirements] but only to the degree that they are probative . . . . To the extent that the requested information does not relate to [the case], the subpoena drifts in the direction of an impermissible ‘fishing expedition.’ Thus, an in camera evaluation would be appropriate to filter out information not probative . . . .”); *Konle v. Page*, 205 Wis.2d 389, 556 N.W.2d 380, 383 (Ct. App. 1996) (“Because tax returns will often contain material which is wholly irrelevant to the [case in question], we conclude that an in camera examination by the trial court is the best and proper procedure through which to filter such discovery demands.”).

<sup>142</sup> See, e.g., *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1180 (9th Cir. 2010) (Kozinski, C.J., concurring) (recommending that “[s]egregation and redaction of electronic data must be done either by specialized personnel or an independent third party”); Day, *Let the Magistrates Revolt*, 64 U. Kan. L. Rev. at 523–24 (2015) (advocating use of filtering agent or special master); J. Saylor, Note, *Computers as Castles: Preventing the Plain View Doctrine from Becoming a Vehicle for Overbroad Digital Searches*, 79 Fordham L. Rev. 2809, 2857 (2011) (advocating for a requirement that special masters be used “to segregate data that is within the scope of the warrant, while excluding non-relevant evidence unless it closely relates to the crime specified in the warrant or is contained in the same file as evidence that the warrant authorizes to be seized”); *Fourth Amendment—Plain View Doctrine—En Banc Ninth Circuit Holds that the Government Should Waive Reliance on Plain View Doctrine in Digital Contexts*, 123 Harv. L. Rev. 1003, 1010 (2010) (calling for a procedure in which “[d]esignated computer personnel or a third party would perform a search of the entire hard drive” and “[a]ll responsive

Court-appointed special masters can hire independent vendors to help sift through the tranche of data disclosed by an Email Provider. Because the special master only turns over responsive data to the government, the individual's right to privacy is protected. While it is true that an individual's right to privacy is intruded upon by the special master, this Court believes the individual would prefer a special master view such private information when the alternative is the government viewing that information. Moreover, this method prevents the government from attempting a *Ganias*-like prosecution.

Filter teams are similar, except the government gets to supply the search-conducting agents. The caveat is that there must be a complete firewall between the search-conducting agents and the investigating agents that helped secure the warrant. The search-conducting agents would supply the first round of responsive information to the investigating agents. Should the investigating agents need help, they can ask the search-conducting agents to perform another search and will be presented only with the responsive data in that search.

One of the main arguments against special masters and filter teams is cost—both in time and in money. However, this Court does not believe those arguments hold water because criminal investigations always cost the government time and money. In the old days, if police wanted to conduct surveillance, they had to use manpower, costing time and money. To tail a car twenty-four hours a day, police had to pay a police officer(s) to tail the suspect's car. Today, GPS technology has eliminated that cost. Similarly, investigators had to sift through truckloads of paper documents; now, investigators can use computers to search through that same data—faster and more efficiently.<sup>143</sup> But that does not mean *any* cost to the government is

---

information would be culled"); Friess, *Rummaging Goes Digital*, 90 Neb. L. Rev. at 1014 (advocating using filter teams).

<sup>143</sup> Over the years, one thing courts addressing searches of ESI have seemingly forgotten is that while technology has presented law enforcement with more data in which to search, technology has also presented law

unreasonable. Moreover, the SCA specifically provides compensation for Email Providers for their reasonable costs in connection with a § 2703 disclosure.<sup>144</sup> If Congress anticipated paying the Email Providers for their trouble, the Court believes paying a special master or filter team is no different. Simply put, under the Fourth Amendment, it is the government's cost of doing business.

Moreover, special masters or filter teams have been routinely authorized by courts in other contexts. For example, third-party filtering or screening teams are frequently used to protect against the disclosure of privileged documents.

An alternative to special masters or filter teams is the use of court-appointed experts under Federal Rule of Evidence 706.<sup>145</sup> Assuming the expert consented to appointment, the expert could conduct the search similar to a special master or filter team. While the use of Rule 706 is not commonplace,<sup>146</sup> use of Rule 706 “should be reserved for exceptional cases *in which the ordinary adversarial process does not suffice.*”<sup>147</sup> The italics emphasize the precise point this Court is making and why it suggests this *ex ante* instruction: at the warrant stage there is no case and no adversarial process—only *ex parte* interactions with the government.<sup>148</sup> The use of a

---

enforcement with tools that conduct the searches faster, more efficiently, and more accurately. Law enforcement uses computers, too, so they should not be the only side reaping the rewards when courts perform the balancing act of interests between the individual and the government. *See also DC Facebook*, 21 F. Supp. 3d at 11 (“[T]his Court finds it hard to believe that a law enforcement agency of remarkable technical ability such as the FBI is opening every file and folder when it seizes a computer that contains a terabyte of data. The Court cannot imagine that it has the time or personnel to do it, nor see any reason to do it when there are more efficient means to do what its agents have to do.”).

<sup>144</sup> *See* 18 U.S.C. § 2706.

<sup>145</sup> In contrast, Federal Rule of Civil Procedure 53 governs special masters.

<sup>146</sup> Indeed, if the Court appointed a court-appointed expert here, it may be the first time a court-appointed expert has been used before a case has formally been opened.

<sup>147</sup> *Commercial Law Corp., P.C. v. Fed. Deposit Ins. Corp.*, No. 10-13275, 2015 WL 7450149, at \*3 (E.D. Mich. Nov. 24, 2015) (citing *In re Johns-Manville Corp.*, 830 F. Supp. 686, 693 (S.D.N.Y. 1993) (emphasis added)).

<sup>148</sup> *See NDCal Email*, 62 F. Supp. 3d at 1103 (“In this *ex ante*, and also *ex parte* process, magistrate judges are called on to review the reasonableness of execution procedures like seize first, search second in the sterile

court-appointed expert, even at this early stage, helps balance the interests and balances the individual’s right to privacy and the government’s interest in effective prosecution—with respect to the seizure and search authorized by the warrant. The firewall between the court-appointed expert and the government mitigates the potential for Fourth Amendment violations in the first place. And employment of a court-appointed expert balances the adversarial process once it has commenced because the expert’s work and process is *testimonial*, allowing the parties’ to examine the expert as a witness at trial. Because the witness is not a government agent, the expert’s testimony appears more credible. It also removes any motivation to be dishonest or untruthful about the search in order to protect an investigation or ensure a conviction. For these reasons, the Court believes this is a viable way to ensure the proper balance of interests.

#### ***5. Use Restrictions—Returning or Destroying Non-Responsive Data***

Courts can also require, *ex ante*, that the government return or destroy the non-responsive data after a certain time. The government should not be permitted to indefinitely seize non-responsive data, especially if it is permitted to overseize ESI in the first place. As discussed earlier, the facts of *Ganias* illustrate the serious risks of what can happen when a court fails to use minimization procedures and/or procedural safeguards to limit the amount of ESI to be seized and to provide for the appropriate treatment of non-responsive data.<sup>149</sup> Retention limitations are another easily enforceable tool that helps ensure Americans’ rights under the Fourth Amendment.

---

isolation of their chambers. All that is available for review comes from the government. No defendant or defense counsel is present. Indeed, no defendant yet exists, as no case has yet been filed. There are no hearings, no witnesses, no briefs and no debate.”).

<sup>149</sup> *Ganias*, 755 F.3d at 138 (“As explained above, practical considerations may well justify a reasonable accommodation in the manner of executing a search warrant, such as making mirror images of hard drives and permitting off-site review, *but these considerations do not justify the indefinite retention of non-responsive documents.*”) (emphasis added).

*SDNY Email* believes there are already adequate remedies in place such as suppression, a civil damages action, and a motion under Rule 41(g); *DC District Email* notes that destroying or returning the evidence received from an email provider could either expose the government to accusations that it destroyed exculpatory evidence in violation of *Brady v. Maryland* or hinder the government's ability to lay a foundation for evidence and establish authenticity under Federal Rules of Evidence Rules 901 and 1001–1006.<sup>150</sup> These observations, while valid, are simply not the best options because the individual's privacy has already been violated.

Courts have a duty to uphold the Constitution. This duty is not simply to punish those who violate an individual's Constitutional rights (*ex post*); rather, it is to protect those rights from violation in the first place (*ex ante*). Courts routinely protect, *ex ante*, Americans' Constitutional rights through various means, such as protective orders, temporary restraining orders, injunctions, etc. Courts have a duty to protect Americans' right to privacy—not simply punish the government for violating that privacy. Once privacy has been lost, it is a total loss. Privacy is a bell that, once rung, cannot be un-rung. *Ex ante* instructions help ensure that a bell that should not be rung is not rung. While *ex ante* instructions may not prevent every governmental intrusion of privacy, courts violate their duty to uphold the Constitution—and thereby protect Americans—by insisting that *ex post* remedies are good enough. *Ganias* is evidence of that. *Ex post* remedies are of little help or consolation to the hypothetical school principal whose livelihood was lost despite never being charged with a crime.

In sum, the Court believes *ex ante* instructions, in any of the forms discussed above, strike the proper balance between an individual's right to privacy and the government's interest in prosecuting crime. *Riley* supports search protocols. *Ganias* illustrates the consequences of

---

<sup>150</sup> *DC District Email*, 13 F. Supp. 3d at 167 n. 10.

giving the government large quantities of ESI, most of which is non-responsive. The trend among commentators is clear: courts should use *ex ante* instructions. For now, the Court is allowing the government to choose which procedural safeguards it will use.

## V. Conclusion

If 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. Given the substantial amount of data collected by the government upon seizing and searching an individual's entire email account, to issue this warrant would swing the balance between an individual's right to privacy and the government's ability to effectively investigate and prosecute crimes too far in favor of the government. As Justice Scalia wrote: "[T]here is nothing new in the realization that the Constitution sometimes insulates the criminality of a few in order to protect the privacy of us all."<sup>151</sup> The proper question is "where the proper balance should be struck."<sup>152</sup>

Accordingly, the Court again finds that, at the very least, an explanation of the government's search techniques is required in order to determine whether the government is executing its search both in good faith and in compliance with the Fourth Amendment. The Court does not believe that this request will overburden the government. In fact, in *Riley*, the government advocated—and it can be concluded that the Supreme Court endorsed—the implementation of search protocols:

Alternatively, the Government proposes that law enforcement agencies "develop protocols to address" concerns raised by cloud computing. Probably a good idea, but the Founders did not fight a revolution to gain the right to government agency protocols.<sup>153</sup>

---

<sup>151</sup> *Arizona v. Hicks*, 480 U.S. 321, 329 (1986).

<sup>152</sup> *Id.*

<sup>153</sup> *Riley*, 134 S. Ct. at 2491–92.



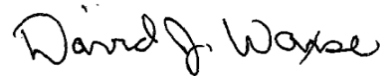
It is this Court's belief that a search protocol is the most effective mechanism for determining whether the warrant and the search proposed therein are constitutional. The alternative is the Court imposing an *ex ante* instruction that does dictate the execution of the warrant, such as appointing a special master or filter-team.

In light of this and the Court's previous opinions, the government's present search warrant application must be denied. The government continues to insist it is entitled to *all* of an individual's email communications, despite only establishing probable cause for part of it and despite admitting it is only interested in seizing evidence after September 7, 2008. 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.

**IT IS THEREFORE ORDERED BY THE COURT** that the application for Search Warrant is DENIED without prejudice. The government may resubmit applications for the requested search warrants, but any such applications should be limited as set forth in this Memorandum and Order.

**IT IS SO ORDERED.**

Dated March 28, 2016, at Kansas City, Kansas.



DAVID J. WAXSE,  
U.S. MAGISTRATE JUDGE