UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF KANSAS

IN THE MATTER OF APPLICATIONS FOR SEARCH WARRANTS FOR INFORMATION ASSOCIATED WITH TARGET EMAIL ACCOUNTS/SKYPE ACCOUNTS	Case Nos.	13-MJ-8163-JPO 13-MJ-8164-DJW 13-MJ-8165-DJW 13-MJ-8166-JPO 13-MJ-8167-DJW

MEMORANDUM AND ORDER

The United States has submitted five Applications and Affidavits for Search Warrant pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require five providers of electronic communication services, Google, Inc. ("Google"), GoDaddy, Verizon Internet Services ("Verizon"), Yahoo!, and Skype (collectively, "Providers"), to disclose copies of electronic communications—including the contents of all emails, instant messages, and chat logs/sessions—and other account-related information for the accounts identified in the Applications ("target accounts"). In the Affidavits in support of probable cause, the government alleges that the individual or individuals being investigated purchased computer equipment with a value well over $5,000 that had been stolen from Sprint, with the knowledge that the equipment was stolen, and that they took possession of the equipment in Kansas and then transported it to New Jersey. The government alleges that the target accounts were utilized to facilitate the purchase, receipt, and transportation of the equipment, in violation of 18 U.S.C. § 2314 (Interstate Transport of Stolen Property), 18 U.S.C. § 2315 (Receipt of Stolen Property), and 18 U.S.C. § 371 (Conspiracy). The government seeks search warrants to obtain stored electronic communications and other information from the Providers in its search for fruits, evidence and/or instrumentalities of the violation of these laws. For the reasons discussed below, the Applications for Search Warrant are denied without prejudice.

I. Proposed Search Warrants

The proposed search warrants are structured so that they identify two categories of information: (1) information to be disclosed by the Providers to the government under 18 U.S.C. § 2703, and (2) information to be seized by the government. The first section of each proposed warrant orders the Provider to disclose to the government the following information, including the content of communications, for each account or identifier associated with the target account(s) stored by the Provider:

> The contents of all emails, instant messages, and chat logs/sessions associated with the account, including stored or preserved copies of emails, instant messages, and chat logs/sessions sent to and from the account; draft emails; deleted emails, instant messages, and chat logs/sessions preserved pursuant to a request made under 18 U.S.C. § 2703(f); the source and destination addresses associated with each email, instant message, and chat logs/session, as well as the date and time at which each email, instant message, and chat logs/session was sent, and the size and length of 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 types of service utilized, 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);
>
> All records or other information stored 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 (Provider) and any person regarding the account, including contacts with support services and records of actions taken.

Upon the government's receipt of the requested information from the Provider, the second section of the proposed warrants further provides that the FBI will maintain all

information that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. §§ 2314, 2315, or 371 involving the target account(s) since June 2006, including the following information:

> All stored electronic mail, instant message, and chat logs/session sent to, from, and through (target account) and all related subscriber accounts from June 2006, when the conspiracy commenced until the date of the search warrant to include communications involving the transportation or receipt of stolen property;
>
> Records relating to who created, used, or communicated with the (target account) or identifiers, including records about their identities and whereabouts; and
>
> All records related to the subscriber account of (all target accounts), including account information, computer host names, Internet addresses, passwords, access telephone numbers, password files, and other identifying information.

II. Relevant Law

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

The applications for search warrants seek authorization to obtain and search electronic communications from providers of electronic communications services pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A). Under 18 U.S.C. § 2703(a), a government entity may require a provider of electronic communication services to disclose the contents of a wire or electronic communication that is in electronic storage for 180 days or less pursuant to a warrant issued in compliance with the Federal Rules of Criminal Procedure.[1] For communications stored for more than 180 days, the statute authorizes a government entity to require a provider of electronic communication services to disclose the contents of the communications under the

[1] 18 U.S.C. § 2703(a).

procedures outlined in subsection (b).[2] Section 2703(b)(1)(A) authorizes a government entity to require a provider of remote computing service 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. Section 2703(c)(1)(A) authorizes a government entity to require a provider of electronic communication service or remote computing service to disclose records or other information pertaining to a subscriber or customer if the government obtains a warrant issued pursuant to the Federal Rules of Criminal Procedure.

B. The Fourth Amendment and its Application to Stored Electronic Communications

The Fourth Amendment of the United States Constitution guarantees the right of citizens against unreasonable searches and seizures:

> 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.[3]

The fundamental purpose of the Fourth Amendment "is to safeguard the privacy and security of individuals against arbitrary invasions by government officials."[4]

Not all government actions are invasive enough to implicate the Fourth Amendment. A search is defined in terms of a person's "reasonable expectation of privacy" and is analyzed

---

[2] Id.

[3] U.S. Const. amend. IV.

[4] Camara v. Mun. Court of City & Cnty. of San Francisco, 387 U.S. 523, 528 (1967).

under a two-part test first set out *Katz v. United States*.[5] This standard involves two discrete inquiries: First, has the individual manifested a subjective expectation of privacy in the object of the challenged search? Second, is society willing to recognize that expectation as reasonable?[6]

The Supreme Court has not addressed whether there is reasonable expectation of privacy in email communications stored with third-party electronic communication service providers. It has held that there is a reasonable expectation of privacy in other forms of communication, such as telephone and mail. In *Katz v. United States*,[7] the Court found that telephone users were "surely entitled to assume that the words . . . utter[ed] into the mouthpiece w[ould] not be broadcast to the world," leading to a holding that has brought telephone conversations fully under the shelter of the Fourth Amendment.[8] In *United States v. Jacobsen*,[9] the Court found 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," based on the premise that a search arises any time the government "infringes upon 'an expectation of privacy that society is prepared to consider reasonable."'[10] In the more recent 2010 case, *City of Ontario, California v. Quon*,[11] the Supreme Court addressed the reasonableness of a government employer's search of text messages sent and

---

[5] 389 U.S. 347, 361 (1967).

[6] *California v. Ciraolo*, 476 U.S. 207, 211 (1986) (citing *Smith v. Maryland*, 442 U.S. 735, 740 (1979)).

[7] 389 U.S. 347 (1967).

[8] *Id.* at 352.

[9] 466 U.S. 109 (1984).

[10] *Id.* at 113.

[11] 130 S.Ct. 2619, 2630 (2010).

received on an employee's pager. While it did not directly decide the issue, 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.[12] The Court commented that "[t]he judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."[13]

Although the Supreme Court has not addressed whether there is reasonable expectation of privacy in electronic communications such as email, the Sixth Circuit in *United States v. Warshak*[14] has extended Fourth Amendment protection to emails stored with third-party electronic communication service providers. The court held that the reasonable expectation of privacy for communication via telephone and postal mail, recognized by the Supreme Court respectively in *Katz* and *Jacobsen*, extends to emails stored with third parties, bringing stored emails within the protection of the Fourth Amendment.[15] In *Warshak*, the court addressed whether law enforcement officers violated the defendant's Fourth Amendment rights by obtaining the content of the defendant's emails from his internet service provider without a warrant. In analyzing the issue and reaching its decision, the *Warshak* court reasoned that emails are analogous to phone calls and letters, and an internet service provider is the functional equivalent of a telephone company or the post office, thereby entitling email communications to the same strong Fourth Amendment protections traditionally afforded to telephone and letter

---

[12] *Id.* at 2630.

[13] *Id*. at 2629.

[14] 631 F.3d 266, 282-88 (6th Cir. 2010).

[15] *Id.* at 285-87 (citing *Katz*, 389 U.S. at 352, and *Jacobsen*, 466 U.S. at 113).

communications.[16] The court emphasized that the police cannot intercept a letter without a warrant even after that letter has been handed over to a third-party intermediary such as a mail carrier for delivery.[17] The court found the same to be true of phone calls, which must be transmitted through a service provider that has the capacity to monitor and record the calls.[18] "Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection."[19] Based on this analysis, the court held that "a subscriber enjoys a reasonable expectation of privacy in the contents of emails 'that are stored with, or sent or received through, a commercial [internet service provider].'"[20] The government may not compel a commercial internet service provider to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause.[21] Therefore, because the government failed to obtain a warrant, its agents violated the Fourth Amendment when they obtained the contents of the defendant's emails.[22] The court also observed that "the mere *ability* of a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy."[23]

---

[16] *Id*. (discussing *Katz*, 389 U.S. at 352-53 and *Ex Parte Jackson*, 96 U.S. 727, 733 (1877)).

[17] *Id.* at 285 (citing *Ex Parte Jackson*, 96 U.S. at 733).

[18] *Id.* (citing *Katz*, 389 U.S. at 352).

[19] *Id.* at 285-86.

[20] *Id.* at 288.

[21] Id.

[22] *Id.*

[23] *Id.* at 286 (emphasis in original).

The Court finds the rationale set forth in *Warshak* persuasive and therefore holds that an individual has a reasonable expectation of privacy in emails stored with, sent to, or received thorough an electronic communications service provider. Accordingly, the Fourth Amendment protections, including a warrant "particularly describing" the places to be searched and communications to be seized, apply to a search warrant seeking such communications. A warrant seeking stored electronic communications such as emails therefore should be subject to the same basic requirements of any search warrant: it must be based on probable cause, meet particularity requirements, be reasonable in nature of breadth, and be supported by affidavit.

C. Fourth Amendment Requirements

Having determined that the Fourth Amendment protections apply to warrants seeking emails stored with an electronic communications service provider, the Court next determines whether the warrants proposed by the Government meet the particularity and breadth standards imposed by the Fourth Amendment.

The warrant clause of the Fourth Amendment commands that "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."[24] The search warrant probable cause and particularity requirements serve two constitutional protections:

> First, the magistrate's scrutiny is intended to eliminate altogether searches not based on probable cause. The premise here is that any intrusion in the way of search or seizure is an evil, so that no intrusion at all is justified without a careful prior determination of necessity. The second, distinct objective is that those searches deemed necessary should be as limited as possible. Here, the specific evil is the "general warrant" abhorred by the colonists, and the problem is not that

[24] U.S. Const. amend. IV.

> of intrusion per se, but of a general, exploratory rummaging in a person's belongings. The warrant accomplishes this second objective by requiring a "particular description" of the things to be seized.[25]

The Fourth Amendment thus categorically prohibits the issuance of any warrant except one particularly describing (1) the place to be searched, and (2) the persons or things (or in this case electronic communications) to be seized. The particularity requirement first mandates that warrants describe with particularity the place to be searched. "The test for determining the adequacy of the description of the location to be searched is 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.'"[26] In the digital realm, whether a description of a place to be searched is sufficiently particular is a complicated question because of the differences between the physical and digital worlds.[27]

The manifest purpose of the Fourth Amendment particularity requirement is to prevent general searches. [28] By limiting the authorization to search the specific areas and things for which there is probable cause to search, the particularity requirement ensures that the search will

---

[25] *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971) (citations omitted).

[26] *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)).

[27] Nichole Friess, When Rummaging Goes Digital: Fourth Amendment Particularity and Stored E-Mail Surveillance, 90 Neb. L. Rev. 971, 987 (2012).

[28] *Maryland v. Garrison*, 480 U.S. 79, 84 (1987).

be carefully tailored to its justifications, and will not become a wide-ranging, exploratory search prohibited by the Fourth Amendment.[29] Thus, 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.[30]

The purpose of the particularity requirement is not however limited to the prevention of general searches.[31] A particular warrant also provides assurances to 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.[32]

In addition to the places to be searched, the warrant must also describe the things to be seized with sufficient particularity. This is to avoid a "general exploratory rummaging of a person's belongings," and was included in the Fourth Amendment as a response to the evils of general warrants.[33] First, the description of the things to be seized must be "confined in scope to particularly described evidence relating to a specific crime for which there is demonstrated probable cause."[34] Second, a warrant must describe the things to be seized with sufficiently precise language so that it informs the officers how to separate the items that are properly subject

---

[29] Id.

[30] *Id.* at 84-85.

[31] *Groh v. Ramirez*, 540 U.S. 551, 561 (2004).

[32] *Id.* (citations omitted).

[33] *United States v. Campos*, 221 F.3d 1143, 1147 (10th Cir. 2000).

[34] *Mink v. Knox*, 613 F.3d 995, 1010 (10th Cir. 2010).

to seizure from those that are irrelevant.[35] This has been stated another way: "As to what is to be taken, nothing is left to the discretion of the officer executing the warrant."[36] A warrant is overly broad if it does not contain sufficiently particularized language that creates a nexus between the suspected crime and the things to be seized.[37]

In *United States v. Leary*,[38] the Tenth Circuit set out the general standard for evaluating when the Fourth Amendment's particularity requirement for things to be seized has been met:

> A description is sufficiently particular when it enables the searcher to reasonably ascertain and identify the things authorized to be seized. Even a warrant that describes the items to be seized in broad or generic terms may be valid when the description is as specific as the circumstances and the nature of the activity under investigation permit. However, the fourth amendment requires that the government describe the items to be seized with as much specificity as the government's knowledge and circumstances allow, and warrants are conclusively invalidated by their substantial failure to specify as nearly as possible the distinguishing characteristics of the goods to be seized.[39]

In *United States v. Carey*,[40] the Tenth Circuit applied the particularity requirement to a warrant authorizing the search of computer files. The court noted that comparing computers to closed containers or file cabinets may be inadequate and lead to oversimplification of a complex area of Fourth Amendment doctrines by ignoring the realities of massive modern computer

---

[35] *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?").

[36] *Marron v. United States*, 275 U.S. 192, 196 (1927).

[37] *Campos*, 221 F.3d at 1147.

[38] 846 F.2d 592, 600 (10th Cir.1988).

[39] *Id.* at 600 (internal quotations and citations omitted).

[40] 172 F.3d 1268, 1275 (10th Cir. 1999).

storage. "Since electronic storage is likely to contain a greater quantity and variety of information than any previous storage method, computers make tempting targets in searches for incriminating information."[41] It proposed that a court could alternatively acknowledge that computers often contain "intermingled documents."[42] Under this "intermingled documents" approach, law enforcement must engage in the intermediate step of sorting various types of documents and then only search the ones specified in a warrant. The court stated that the magistrate judge should then require officers to specify in a warrant what type of file is sought.[43]

In *United States v. Otero*,[44] the Tenth Circuit recognized that the Fourth Amendment's warrant particularity requirement has increased importance with respect to electronically stored information.

> 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. Because of this, our case law requires that "warrants for computer searches must *affirmatively limit* the search to evidence of specific federal crimes or specific types of material."[45]

In *Otero*, the defendant, a former postal carrier, was indicted for offenses in connection with alleged theft of credit cards, personal identification numbers, and billing statements from

---

[41] *Id.* (citing Raphael Winick, *Searches and Seizures of Computers & Computer Data*, 8 Harv. J.L. & Tech. 75, 104 (1994)).

[42] Id.

[43] Id.

[44] 563 F.3d 1127, 1132 (10th Cir. 2009).

[45] *Id.* (quoting *United States v. Riccardi*, 405 F.3d 852, 862 (10th Cir. 2005)) (emphasis in original).

residents along her delivery route. The government obtained a search warrant for her residence. The warrant contained two subsections: "Items to be Seized" and "Computer Items to be Seized."[46] Each paragraph under the first section limited the search to evidence of specific crimes or evidence pertaining to specific persons along the defendant's delivery route. Each paragraph under the second section, however, had no limiting instruction whatsoever. The court found a reading the computer items paragraphs of the warrant alone showed that they each authorize a search and seizure of "[a]ny and all" information, data, devices, programs, and other materials with no explicit or even implicit incorporation of the limitations of the first section.[47] The computer-related paragraphs did not even refer to the rest of the warrant. The court concluded that the presence of limitations in the first section but absence in the second suggested that the computer searches were not subject to those limitations.[48] The court further rejected the government's argument that under a natural reading of the warrant the portion authorizing the computer search was limited to information pertaining to the alleged mail fraud and credit card theft. [49] It concluded that the paragraphs of the warrant authorizing the computer search were subject to no affirmative limitations.[50] Recognizing that "practical accuracy rather than technical precision controls the determination of whether a search warrant adequately describes the place to be searched," the Tenth Circuit concluded that the warrant failed to describe the items to be

---

[46] *Id.* at 1132.

[47] *Id.* at 1133.

[48] *Id.*

[49] *Id.*

[50] *Id.*

seized with either "technical precision" or "practical accuracy," because the section of the warrant pertaining to seizure of the computer items did not limit the search to evidence of specific crimes or to specific persons on the defendant's delivery route.[51]

III. Whether the Proposed Search Warrants Comport with the Fourth Amendment

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 email communications stored in an account provided by an electronic communications service 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 electronic communications—such as email accounts from electronic communication service providers—are sufficiently particular under the Fourth Amendment.

This Court has previously denied an application for search warrant authorizing an electronic communications service provider, Yahoo!, to disclose the content of all emails and other account-related information without limitation as overly broad and as a result in violation of the Fourth Amendment.[52] In that case, a request to search "the contents of all emails associated with the account" as well as "all records or other information … including address

---

[51] *Id.* at 1132.

[52] *See In re Search Warrants for Info. Associated with Target Email Address*, Case Nos. 12-MJ-8119-DJW and 12-MJ-8191-DJW, 2012 U.S. Dist. LEXIS 138465 (D. Kan. Sept. 21, 2012).

books, contact and buddy lists, calendar data, pictures, and files" was denied based on the same rationale as set forth above.[53]

Since then, this District has entered a similar ruling in *United States v. Barthelman*.[54] In *Barthelman*, law enforcement officers applied for search warrants directed to Yahoo! and Apple, authorizing the search of email accounts maintained by Yahoo and Apple for, amongst other things, "the contents of any and all emails stored in the subscriber's … account from November 1, 2011 to the present day."[55] The Yahoo! search warrant was dated May 3, 2012 and the Apple search warrant was dated August 21, 2012. Defendant challenged the warrants as unsupported by probable cause and overly broad. Judge Monti Belot found that the warrants were supported by probable cause, but granted the motion to suppress the Yahoo! and Apple warrants on the basis that "the warrants were overbroad and not as particular as the Fourth Amendment requires."[56] The fact that the warrants were limited to specific accounts, to a specific time frame of six months, and to "evidence of communications used in furtherance of the violation of the laws of the State of Ohio" was not sufficiently particular according to the court.[57]

The Court was able to locate only a few other cases involving a search warrant served on an electronic communications service provider for the contents of an email account. [58] In all

---

[53] *Id*. at *3-4

[54] Case No. 13-10016-MLB, 2013 U.S. Dist. LEXIS 107123 at *31 (D. Kan. July 31, 2013).

[55] *Id*. at *4.

[56] *Id*. at *31.

[57] *Id*. at *29-30.

[58] *See United States v. Taylor*, 764 F. Supp. 2d 230, 236-37 (D. Me. 2011); *United States v.*

three cases, the defendants argued that the warrants authorizing the searches of the email accounts lacked sufficient particularity in describing the items to be seized, and in all three cases the courts denied the respective motion to suppress on those grounds.[59] All the courts further agreed that the Fourth Amendment does not require executing authorities to delegate a pre-screening function to the electronic communications service provider or to ascertain which emails are relevant before copies are obtained from the electronic communications service provider for subsequent searching. [60] This Court does not disagree with those cases with respect to the their statement that the Fourth Amendment does not require the government to delegate a pre-screening function to the electronic communications service provider to ascertain which electronic communications are relevant before obtaining them. The Court, however, does disagree with those cases to the extent that they find the warrants were not overly broad in their authorization for the electronic communications service provider to disclose the content of all emails and other account-related information without limitation.

As to the current pending applications, the Court finds that the warrants proposed by the government violate the Fourth Amendment. First, the initial section of the warrants authorizing the electronic communications service provider to disclose all email communications (including all content of the communications), and all records and other information regarding the account

---

Bickle, No. 2:10-cr-00565-RLH-PAL, 2011 WL 3798225, at *13 (D. Nev. July 21, 2011); *United States v. Bowen*, 689 F.Supp.2d 675, 682 (S.D.N.Y. 2010).

[59] In *Bickle*, 2011 WL 3798225, at *13, however, the court granted the motion to suppress as to information or emails sent, received, drafted or stored in in email account before March 1, 2009.

[60] *Taylor*, 764 F. Supp. 2d at 237; *Bickle*, 2011 WL 3798225, at *20; *Bowen*, 689 F.Supp. 2d at 682.

is too broad and too general. The warrants fail to set any limits on the email communications and information that the electronic communications service provider is to disclose to the government, but instead requires each Provider to disclose all email communications in their entirety and all information about the account without restriction. Most troubling is that these sections of the warrants fail to limit the universe of electronic communications and information to be turned over to the government to the specific crimes being investigated. Second, even if the Court were to allow a warrant with a broad authorization for the content of all email communications without a nexus to the specific crimes being investigated, the warrants would still not pass Constitutional muster. They fail to set out any limits on the government's review of the potentially large amount of electronic communications and information obtained from the electronic communications service providers. The warrants also do not identify any sorting or filtering procedures for electronic communications and information that are not relevant and do not fall within the scope of the government's probable cause statement, or that contain attorney-client privileged information. In *Bickle*,[61] the search warrant seeking the content of all emails sent to or from the defendant's Hotmail email account was supported by an affidavit that set out the government's filtering procedure for emails containing privileged communications.

Although the sections of the search warrants authorizing the government-authorized review of the information provided by the Providers are sufficiently particular in that they link the information to be seized to the alleged crimes, the sections requiring the initial disclosure by

[61] 2011 WL 3798225, at *2 (the affidavit in support of the search warrant seeking all communications made or received via defendant's email account provided that a filter agent would be assigned to review and remove any potentially privileged materials).

the electronic communications service provider under 18 U.S.C. § 2703 are not. They fail to create a nexus between the suspected crime and the email communications and related account information to be obtained and searched. The warrants order the Providers to disclose the content of *all* communications associated with the target accounts, including deleted communications, as well as all records and information regarding identification of the accounts, and other information stored by the account user, including address books, contact lists, calendar data, pictures, and files. The target accounts may contain large numbers of emails and files unrelated to the alleged crimes being investigated or for which the government has no probable cause to search and seize. The government simply has not shown probable cause to search the contents of all emails ever sent to or from the accounts or for all the information requested from the Providers. The government thus has not shown probable cause for the breadth of the warrants sought here. The warrants also fail to set any limits on the universe of information to be disclosed to and searched by the government, such as limiting the disclosure and search to information relating to the specific crimes being investigated and for which the government has demonstrated probable cause to search. The Court finds the breadth of the information sought by the government's search warrant for the target accounts—including the content of every email sent to or from the accounts—is best analogized 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.

Even had the government shown probable cause for the Providers to disclose the content of all email communications and information connected to the target accounts, the Court is concerned by the lack of any limits on the government's review of the information, such as filtering procedures for emails and information that do not fall within the scope of probable cause or contain attorney-client privileged communications. Under the government's proposed warrants, a government agent would be presumably be authorized to review the content of all the emails ever sent or received on the target accounts among a host of other information provided by the Providers. While the government's enforcement purposes should not be hindered, there must be an appropriate balance between allowing law enforcement to do its job effectively and protecting the Fourth Amendment rights of those being investigated. The warrants as currently proposed give the government virtual carte blanche to review the content of all electronic communications associated with the accounts and fail to adequately limit the discretion of the government-authorized agents executing the warrants. The absence of any limitations in the warrants on the government's review of the content of all email communications obtained from the Providers is in violation of the Fourth Amendment.

The Court notes that while nothing in Section 2703 or Fed. R. Crim. P. 41 may specifically preclude the government from requesting the full content of electronic communications in a specific email account, the Fourth Amendment may do so and does here. The Court further notes that the Tenth Circuit has not required particularized computer search strategy—at least in warrants authorizing searches of computers. The Tenth Circuit has not spoken on the issue of whether warrants such as the ones sought here— authorizing an electronic communications service provider to disclose the content of all electronic communications—

require a description of the search protocol or some other limit on the government's search of that information. The Tenth Circuit has however suggested an approach for "intermingled documents," in which law enforcement engage in the intermediate step of sorting various types of documents and then only search the ones specified in a warrant.[62] Under this approach, "the magistrate judge should then require officers to specify in a warrant [the] type of files [that are being] sought."[63] The Court is not suggesting that the warrants must have a particularized search strategy or even identify by certain key word searches the electronic communications that will be reviewed by the government, only that the warrants must contain some limits on the government's search of the electronic communications and information obtained from the electronic communications service provider. To comport with the Fourth Amendment, the warrants must contain sufficient limits or boundaries so that the government-authorized agent reviewing the communications can ascertain which email communications and information the agent is authorized to review.

The Court leaves the suggestion of an appropriate procedural safeguard up to the government. While not endorsing or suggesting any particular safeguard, some possible options would be asking the electronic communications service provider to provide specific limited information such as emails containing certain key words or emails sent to/from certain recipients, appointing a special master with authority to hire an independent vendor to use computerized

[62] *Carey*, 172 F.3d at 1275.

[63] Id.

search techniques[64] to review the information for relevance and privilege, or setting up a filter group or taint-team to review the information for relevance and privilege. Only with some such safeguard will the Fourth Amendment's protection against general warrants be insured.

IT IS THEREFORE ORDERED that the five Applications for Search Warrant are 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 in Kansas City, Kansas on this 27th day in August, 2013.

s/ David J. Waxse
David J. Waxse
U.S. Magistrate Judge

[64] 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).