IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF KANSAS

UNITED STATES OF AMERICA **Plaintiff,** **v.** **WILLIAM ELAM BARBER,** **Defendant.**	**Case No. 15-40043-CM**

GOVERNMENT'S RESPONSE IN OPPOSITION TO DEFENDANT'S REPLY

The United States of America, by and through Barry R. Grissom, United States Attorney for the District of Kansas, and Christine E. Kenney, Assistant United States Attorney for said District, submits this response in opposition to Defendant's Reply to Government's Response in Opposition to Motion to Suppress. (Doc. 38.) Due to the timing of the disclosure of certain documents, the defendant raises for the first time a particularity challenge to the Maryland warrants.[1] The defendant also asserts additional arguments pertaining to whether the email warrants were issued under the Stored Communications Act, and to his standing to challenge the search of "jesusweptone@gmail.com" email. The government incorporates by reference and reasserts all arguments and authorities set forth in its original response (Doc. 35), and requests this Court to overrule and deny the motion to suppress.

1. Because the other arguments contained in Defendant's Reply generally are in response to the government's arguments, those are not further addressed in this pleading.

A. The Maryland Warrants particularly describe what law enforcement was authorized to search.

The defendant's first challenge is to the Maryland search for information associated with the email account, "jesusweptone@gmail.com." The face of the search warrant seeks to search property "located in the District of Maryland" described as, "Email Accounts maintained by Google Inc., 1600 Amphitheatre Parkway, Mountain View, California 94043 and as further described in ATTACHMENT A," and to seize "evidence of the commission of criminal offenses, as further described in the attached affidavit in support of search warrant incorporated fully herein including ATTACHMENT B." (Ex. 1.) Attachment A identified the items to be seized and searched as, "information associated with the email accounts, . . . jesusweptone@gmail.com . . . which is stored at premises owned, maintained, controlled, or operated by Google Inc., a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043." (Ex. 2, page 11.) Attachment B set forth a two-step process identifying the items to be seized. Section I identified the information to be disclosed by Google Inc. for the identified email account listed in Attachment A. Section II identified the information to be seized by the government that "constitutes fruits, evidence and instrumentalities of violations of Title 18, U.S.C. §§ 2251 and 2252A." (Ex. 2, Page 12 – 13.)

The defendant's second challenge is to the Maryland search for information associated with the email account, "bigw1991@gmail.com." The face of the search warrant seeks to search property "located in the District of Maryland" described as, "Email Accounts maintained by Google Inc., BIGW1991@gmail.com . . . See ATTACHMENT A," and to seize the property identified in ATTACHMENT B. (Ex. 3.) Attachment A identified the items to be seized and searched as, "information associated with the email accounts, . . . bigw1991@gmail.com . . . which is stored at premises owned, maintained, controlled, or operated by Google Inc., a company

headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043." (Ex. 4, page 8.) Attachment B outlined the same two-step process setting forth the items to be seized. Section I identified the information to be disclosed by Google Inc. for the identified email account listed in Attachment A. Section II identified the information to be seized by the government that "constitutes fruits, evidence and instrumentalities of violations of Title 18, U.S.C. §§ 2251 and 2252A." (Ex. 4, Page 9 – 11.)

The defendant argues in his reply that the Maryland search warrants violate the Fourth Amendment's particularity requirement by compelling the disclosure of the entire contents of the email accounts. The defendant claims his position is supported by precedent in this Circuit and this District. However, the defendant does not discuss the one case from this district that is directly on point.

The same challenge the defendant raises to the search warrants in the instant case was raised by the defendant in *United States v. Deppish*, 994 F.Supp.2d 1211 (D. Kan. 2014). In *Deppish*, the defendant argued that, because the search warrant authorized disclosure of his entire email account, the search warrant for the contents of his email account did not properly limit the scope by particularly describing the evidence related to a specific crime. *Id*. at 1219. The challenged warrant in *Deppish* was very similar to those in the instant case. The *Deppish* Attachment A identified the property to be searched as information associated with the email account stored at premises owned, maintained, controlled, or operated by Yahoo headquartered in Sunnyvale, CA. (Ex. 10, page 14.) The *Deppish* Attachment B set forth the same two-step process as described in both the Maryland search warrants. (Ex. 10, page 15 – 16.)

The Hon. Julie A. Robinson denied the defendant's particularity challenge. Judge Robinson noted:

> When large amounts of data are collected in a source, it follows that the scope of the disclosure and search would need to be broader rather than narrower. Otherwise, the Government would be severely limited—if not altogether precluded—from searching for and seizing the evidence sought. There would be only two options. Either the communications provider searches the email account for evidence, or the communications provider discloses the account to law enforcement for their search and seizure of evidence.

Id.

Judge Robinson also noted that "the warrant sought broad disclosure of Defendant's email account, but described with particularity the objects to be seized, that is instrumentalities and evidence demonstrating violations of 18 U.S.C. §§ 2252." *Id*.

Probable cause exists to issue a warrant if the judge finds, given the totality of the circumstances, "there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 236 (1983). The Fourth Amendment requires that a warrant describe with particularity the place to be searched and the persons or things to be seized. *Deppish*, 994 F.Supp.2d at 1219, citing *United States v. Brown*, 984 F.2d 1074, 1077 (10th Cir. 1993).

As noted in the previous response to the motion to suppress, warrants for the search of the content of email accounts are governed by the Stored Communications Act ("SCA"). *Deppish*, 994 F.Supp.2d at 1219. The SCA authorizes the government to obtain the contents of electronic communications from a service provider only when the government obtains a warrant under 18 U.S.C. § 2703(d). 18 U.S.C. § 2703(c)(l)(A)-(B). A § 2703(d) order "shall only issue if the government offers specific and articulable facts showing that there are reasonable grounds to believe that . . . the records . . . are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

A § 2703 search warrant is broader than a search warrant under Fed. R. Crim. P. 41 in several respects. First, § 2703(d) allows a court in one jurisdiction to issue an order for disclosure

to an electronic service provider in another jurisdiction. Second, § 2703(c) allows the service provider to release certain information to the government for an off-site search. Otherwise, law enforcement would have to conduct the search at the service provider's, e.g., Google's, premises. Third, § 2703(g) provides that the "presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider . . ." Finally, § 2703(d) includes a mechanism for the service provider to quash or modify an order "if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider." Obtaining a § 2703 warrant otherwise involves the same procedure described in Rule 41, namely: the presentation of an affidavit for probable cause review by a neutral and detached magistrate. 18 U.S.C. § 2703(c)(1)(A). "The SCA merely requires a provider to disclose information rather than search for it." *Deppish*, 994 F.Supp.2d at 1219.

The defendant's particularity challenge rests in large part on opinions from the Hon. David J. Waxse, United States Magistrate Judge, denying previous government requests for search warrants similar to the one at issue here. *See, In re Application for Search Warrants for Information Associated with Target Email Address*, 12-MJ-8119-DJW, 12-MJ-8191-DJW (D. Kan. Sep. 21, 2012); *and see, In re Applications for Search Warrants for Info. Associated with Target Email Accounts/Skype Accounts*, 13-MJ-8163-JPO, 13-MJ-8164-DJW, 13-MJ-8165-DJW, 13-MJ-8166-JPO, 13-MJ-8167-DJW, 2013 WL 4647554 (D. Kan. Aug. 27, 2013) (hereinafter referred to as the "August 27 Order"). Judge Waxse ruled that the government's applications violated the Fourth Amendment. *Id.* at *8. However, Judge Waxse agreed that the sections of the search warrants pertaining to the government's review of the information from the service providers were sufficiently particular. *Id.*

In support of his ruling, Judge Waxse cited two opinions: *United States v. Otero*, 563 F.3d 1127 (10th Cir. 2009), and *United States v. Elias Barthelman*, CRIM.A. 13-10016-MLB, 2013 WL 3946084 (D. Kan. July 31, 2013). These cases are distinguishable from the facts in the instant case. *See Deppish*, 994 F.Supp.2d at 1221.

In *Otero*, the Tenth Circuit's concern was that the first part of the search warrant addressing the residence included limiting language identifying what the searcher would seize, but the second part of the search warrant addressing the computer did not include this limitation. *Otero*, 563 F.3d at 1132 -33. Thus, as it related to the computer, the search warrant failed to inform the searcher of the parameters of the search and was overbroad. *Id*. at 1133.[2] These facts are considerably different than the search warrants in the instant case, which included language in Section II of Attachment B to guide the searching law enforcement officer limiting the search to information that related to violations of 18 U.S.C. §§ 2251 and 2252A. (Gov. Ex. 2, 4.) Permitting the two-step process set forth in Attachment B eliminated what would otherwise have necessitated a search by government agents of the electronically stored information at Google's physical location, a process that would have essentially resulted in the same search but conducted at a different location.

Barthelman is also factually distinguishable. Judge Belot's ruling focused on the fact that the warrant failed to reference a particular criminal statute. *Barthelman*, 2013 WL 3946084 at *11. The warrant in *Barthelman* did not reference a particular criminal violation, but instead referenced an entire chapter of criminal statutes. Here, the applications and the warrants specifically referenced 18 U.S.C. §§ 2251 and 2252A. (Gov. Ex. 2, 4, 7, and 8.)

Judge Waxse noted that "[a]lthough there are many cases addressing the Fourth

[2] However, the Court upheld the search under the good faith exception. *Id.*

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." The August 27 Order at *7. However, the Tenth Circuit cases pertaining to the search of files stored on a computer's hard drive provide such guidance.

In *United States v. Burke*, 633 F.3d 984 (10th Cir. 2011), the Court addressed the Fourth Amendment's requirement of particularity and the information that a person may store in a computer. The *Burke* Court noted that the "ability of computers 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." (Citation omitted.) *Id.*, at 992. The Court went on to state:

> We emphasize that practical accuracy rather than technical precision controls the determination of whether a search warrant adequately describes the place to be searched . . . A warrant need not necessarily survive hyper-technical sentence diagraming and comply with the best practices of *Strunk & White* to satisfy the particularity requirement . . . But, it should enable the searcher to reasonably ascertain and identify the things authorized to be seized. (Citations omitted.)

Id.

The Tenth Circuit also discussed computer searches in *United States v. Burgess*, 576 F.3d 1078 (10th Cir. 2009). In *Burgess*, law enforcement officers obtained a search warrant for the defendant's motor home and computer. The warrant authorized the seizure of any evidence "which would tend to show a conspiracy to sell drugs." *Id.* at 1090. In addressing the scope of the government's search, the Court stated: "officers must be clear as to what it is they are seeking on the computer and conduct the search in a way that avoids searching files of types not identified in the warrant." *Id.* at 1092. However, a "computer search may be as extensive as reasonably

required to locate the items described in the warrant." *Id.*; s*ee also United States v. Grimmet*, 439 F3 1263, 1270 (10th Cir. 2006); *United States v. Brooks*, 427 F3 1246, 1252 (10th Cir. 2005) (given the nature of computers, a search can be as much an art as a science).

The *Burgess* Court further noted that:

> This court has never required warrants to contain a particularized search strategy . . . Rather, the limitation on the scope of this search was explicitly constrained by content – computer files containing evidence of drug use or trafficking. . . . "[I]n the end, there may be no practical substitute for actually looking in many (perhaps all) folders and sometimes at the documents contained within those folders, and that is true whether the search is of a computer or physical files.

(emphasis added.) *Id.* at 1093-1095; s*ee also United States v. Schesso*, 2013 WL 5227071 at *6 – 7 (9th Cir. 2013) (acknowledging that the Court has moved away from search protocols, and the absence of such did not violate the Fourth Amendment); *Deppish*, 994 F.Supp.2d at 1220.

In the instant case, the location of the searches was as particularized as possible: the premises owned, maintained, controlled, or operated by Google for information associated with the email accounts jesusweptone@gmail.com and bigw1991@gmail.com. Additionally, the items to be seized from the execution of the search warrant were identified with particularity, and were identified in such a manner as to limit what the searching agent would be authorized to seize: fruits, evidence and instrumentalities of violations of Title 18, U.S.C. §§ 2251 and 2252A. (Gov. Ex. 2, 4.)

B. The Maryland warrants are not fatally defective because the warrant fails to mention 18 U.S.C. § 2703, or because the district is misidentified on its face.

In his reply, the defendant correctly points out that on the face of the Maryland warrants, the location of the property to be seized is identified as the District of Maryland. However, this fact is not fatal because the warrants, as well as the affidavits, also referenced Attachment A and

described the property as located at premises of Google, a company headquartered in California. This discrepancy did not defeat the determination that there was probable cause to issue these warrants. *See*, *Maryland v. Garrison*, 480 U.S. 79, 85 – 87 (1987) (a mistake in the address of the place to be searched did not invalidate the warrant where there was otherwise probable cause to support its issuance); *United States v. Owens*, 848 F.2d 462, 463 – 64 (4th Cir. 1988) (citing *Garrison*, finding probable cause despite an erroneous apartment number on the search warrant and the officers actually searched the correct apartment); *United States v. Johnson*, 558 F.Supp.2d 807, 812 – 13 (E.D. Tenn. 2008) (omission of a residence address from the warrant was a clerical error and did not render warrant invalid); *but see United States v. Gary*, 420 F.Supp.2d 470, 483 – 484 (E.D. VA. 2006) (error of date of trash pull in a drug case that placed the event a year before it actually happened affected staleness; however, because the error was clerical, the search was saved by the good-faith exception).

There is no question that, in the instant case there was probable cause to believe evidence of violations of 18 U.S.C. § 2251 and 2252A would be found in the email accounts "jesusweptone@gmail.com" and "bigw1991@gmail.com." There is also no question that, despite the identification on the face of the warrant that the property was located in the District of Maryland, law enforcement actually searched information obtained from Google pertaining to the correct email accounts. Further, this misidentification as to the district where the property would be located does not remove these warrants from the scope of § 2703.

Moreover, the government can find no authority that requires the warrant cite to the court's authority to issue it. For example, Rule 41(e)(2) sets forth the contents of the warrant issued under that rule. Citation to the rule itself is not included. As noted previously, § 2703(c)(1)(A)

requires that the warrant be "issued using the procedures described in the Federal Rules of Criminal Procedure.

The magistrate judge who authorized the Maryland warrants must have been aware of the Rule 41 limitations, and therefore would know that the warrants were issued under § 2703, because the affidavits and attachments identified the location of the property at premises controlled by Google. Magistrate judges "are presumed to know fundamental principles of law." *United States v. Morgan*, 959 F.2d 232 (4th Cir. 1992).

C. The defendant had no reasonable expectation of privacy in sent emails.

The defendant argues that he maintained a reasonable expectation of privacy in the emails he sent to "jesusweptone@gmail.com," and therefore, has standing to contest those emails. The defendant's position is not supported by case law.

"A person has an expectation of privacy protected by the Fourth Amendment if he has a subjective expectation of privacy, and if society is prepared to recognize that expectation as objectively reasonable." *United States v. Miravalles*, 280 F.3d 1328, 1331 (11th Cir.2002) (citing *Katz v. United States*, 389 U.S. 347, 361, 88 S.Ct. 507, 516, 19 L.Ed.2d 576 (1967) (Harlan, J., concurring)). Those circuits that have addressed the question of whether there is a reasonable expectation of privacy in emails have generally compared emails to letters sent using the United States mail. Although letters are protected by the Fourth Amendment, "if a letter is sent to another, the sender's expectation of privacy ordinarily terminates upon delivery." *United States v. King*, 55 F.3d 1193, 1195–96 (6th Cir.1995) (citations omitted). Similarly, an individual sending an e-mail loses "a legitimate expectation of privacy in an e-mail that had already reached its recipient." *Guest v. Leis*, 255 F.3d 325, 333 (6th Cir.2001); *United States v. Lifshitz*, 369 F.3d

173, 190 (2d Cir.2004); *United States v. Charbonneau*, 979 F. Supp. 1177, 1184 (S.D. Ohio 1997) (comparing email to mailing a letter).

Once the email message is received, the sender no longer controls the message's destiny and therefore has no reasonable expectation of privacy in its contents. *Id*. Thus, the defendant cannot claim standing in the search of the "jesusweptone@gmail.com" account just because emails he sent to that account were recovered during the search.

D. Good Faith

After considering the facts in *Deppish*, Judge Robinson ruled that, even if probable cause to support the warrant was lacking, the court would uphold the warrant on good faith. *Id*. at 1221. Judge Robinson specifically rejected Deppish's claim that good faith could not apply because the warrant was so facially deficient that no reasonable officer could believe it valid. *Id*. at 1222. Judge Robinson's findings apply equally to the facts of the instant case. Also, good faith would save the Maryland warrants despite the failure to cite to the statute, and despite the misidentification that the property would be located in that district. *Gary*, 420 F.Supp.2d at 483 – 484. For these reasons, as well as the arguments and authorities previously set forth, investigators were entitled to rely in good faith on the Maryland warrants.

CONCLUSION

Based upon the above, the United States requests that this Court overrule and deny the defendant's motion to suppress on the basis that the warrant was not sufficiently particular. The warrant particularly described the location of the property as information associated with the specific email accounts stored at premises owned, maintained, controlled or operated by Google. The warrant further narrowed the information to be seized by the government as information from

those accounts that would constitute fruits, evidence and instrumentalities of violation of specific criminal statutes.

Further, the defendant does not have standing to contest the search of "jesusweptone@gmail.com" because there is no reasonable expectation of privacy once sent emails are received by another party. Moreover, clerical errors pertaining to the location of the property do not remove the warrant from the authority of the SCA.

Finally, this Court need not decide the broader issues of statutory authority, probable cause and standing because the warrants would otherwise be saved by good faith.

Respectfully submitted,

BARRY R. GRISSOM
United States Attorney

/s/ Christine E. Kenney
Christine E. Kenney, #13542
Assistant U.S. Attorney
444 SE Quincy, Room 290
Topeka, KS 66683
(785) 295-2850
christine.kenney@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on the 5th day of February, 2016, I electronically filed the foregoing with the clerk of the court by using the CM/ECF system, which will send a notice of electronic filing to all counsel of record.

s/ Christine E. Kenney
Christine E. Kenney, #13542
Assistant United States Attorney
444 S.E. Quincy, Suite 290
Topeka, KS 66683
(785) 295-2850
christine.kenney@usdoj.gov