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

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

**MEMORANDUM AND ORDER**

This case is before the court on defendant William Elam Barber's Motion to Suppress Fruits of Illegal Searches (Doc. 29). Defendant challenges three search warrants that led to the filing of this case: (1) a warrant issued by a magistrate judge sitting in the District of Maryland, directed to Google, Inc., in California, for the contents of an email account belonging to jesusweptone@gmail.com (not defendant's account); (2) a second warrant issued by another Maryland magistrate judge to Google for the contents of an email account belonging to bigw1991@gmail.com (defendant's account); and (3) a warrant issued by Judge O'Hara for the search of defendant's Kansas home. Defendant claims that the Maryland magistrate judges lacked jurisdiction to issue the first and second warrants—rendering the warrants void from the inception—and therefore making the items found in defendant's home the fruit of the poisonous tree. Defendant asks the court to suppress the evidence from all three warrants. The court conducted a hearing on February 15, 2016. Defendant requested additional briefing after the hearing, and the court allowed the parties to file additional briefing on the application of the good faith exception. The court now issues the following findings of fact and conclusions of law.

**Findings of Fact**

FBI Special Agent Daniel O'Donnell was investigating email addresses identified as trading in and discussing child pornography. One of the emails Special Agent O'Donnell investigated was jesusweptone@gmail.com. In November 2012, Special Agent O'Donnell requested and obtained a search warrant from a magistrate judge in the District of Maryland. The warrant was addressed to Google Inc., located in the Northern District of California, for the contents of jesusweptone@gmail.com. The face of the warrant stated that the information was stored in Maryland, but the affidavit in support indicated that the information was stored in Mountain View, California.

The jesusweptone@gmail.com search warrant execution revealed that six emails were sent or received by bigw1991@gmail.com to or from jesusweptone@gmail.com, with a total of forty-two images attached to the emails. The images contained child pornography involving prepubescent females and toddlers.

Using the results from the November 2012 warrant, Special Agent O'Donnell then obtained a second search warrant in the District of Maryland for information in possession of Google Inc., for the contents of bigw1991@gmail.com. Again, the face of the warrant stated that the information was stored in Maryland, but the supporting affidavit indicated that the information was stored in Mountain View, California. Special Agent O'Donnell then determined that this email address was associated with defendant William Barber, at an address in Kansas City, Kansas. The execution of the warrant also revealed that between June 2011 and December 2012, approximately fifty-one of the emails sent or received by bigw1991@gmail.com contained child pornography or text indicative of an interest in child pornography. Over ninety images or videos of child pornography were sent or received in the emails.

Based on this information, FBI Special Agent Michael Daniels submitted an affidavit in support of a search warrant on the residence of defendant. Judge James P. O'Hara in the District of Kansas authorized the warrant for the search of defendant's home.

Special Agent O'Donnell testified in court that he believed he was able to ask any court with jurisdiction over a particular violation to issue a warrant when he was investigating email accounts without knowing where the account users were located. When Special Agent O'Donnell obtained the first warrant from the Maryland magistrate judge, he did not know whether any potential violators resided in the District of Maryland. He did, however, consult with a Department of Justice attorney before requesting the warrants. Also, a Department of Justice attorney reviewed Special Agent O'Donnell's affidavits.

## Conclusions of Law

### Standing

The first question before the court is whether defendant has standing to challenge the warrant for the contents of the email account belonging to jesusweptone@gmail.com. The court determines that defendant does not have a reasonable expectation of privacy in his sent emails once they were received by the recipient. *See United States v. Lifshitz*, 369 F.3d 127, 190 (2d Cir. 2004) (noting that individuals may not "enjoy such an expectation of privacy in transmissions over the Internet or e-mail that have already arrived at the recipient"); *see also United States v. Lustyik*, 57 F. Supp. 3d 213, 223 (S.D.N.Y. 2014) ("A person has no expectation of privacy in another person's email account."). *But see United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) ("[W]e hold 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 ISP.'" ). "Emails are comparable to letters sent using the United States mail. Letters are protected by the Fourth Amendment, but the sender's reasonable expectation of privacy

ends upon delivery of the letter. *United States v. King*, 55 F.3d 1193, 1195–96 (6th Cir. 1995). Likewise, a legitimate expectation of privacy in an email is lost once the email reaches the recipient. *Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001) ("Users would logically lack a legitimate expectation of privacy in the materials intended for publication or public posting. They would lose a legitimate expectation of privacy in an e-mail that had already reached its recipient; at this moment, the e-mailer would be analogous to a letter-writer, whose expectation of privacy ordinarily terminates upon delivery of the letter."). For these reasons, defendant lacks a legitimate expectation of privacy in his sent emails that law enforcement found in the jesusweptone@gmail.com account. This decision does not end the inquiry, however, as defendant may still challenge the warrant targeted at his own email account—bigw1991@gmail.com.

Rule 41(b) v. The Stored Communications Act

Next, the court considers which standards to apply to the second warrant: those of Rule 41(b) or those of the Stored Communications Act ("SCA"). Defendant is correct that if Fed. R. Crim. P. 41(b) were the only authority governing the issuance of the warrant, then this motion would be fairly easily resolved: The magistrate judge would have exceeded his authority by issuing a warrant for a search outside his district. Rule 41(b) gives a magistrate judge authority to issue a warrant for a search and seizure of property located within the district. The Maryland judge's act in issuing a warrant for execution in California would exceed that authority. But here, the SCA may apply to extend the jurisdiction of the issuing judge. 18 U.S.C. § 2703(a) provides:

> A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction.

"A court of competent jurisdiction" is defined as "any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). This means that when the SCA applies, a magistrate judge with jurisdiction over the offense being investigated can issue a warrant to be executed outside of that judge's ordinary jurisdiction, using the procedures of Rule 41, but not constrained by the jurisdictional limitation of Rule 41(b).

The problem with utilizing the SCA to provide the jurisdiction the Maryland magistrate judge needed to issue the second warrant is this: The government presented no evidence that the offense being investigated occurred in Maryland. Courts that have interpreted the language "jurisdiction over the offense being investigated" have held that Congress intended it to mean territorial jurisdiction over the offense—not general jurisdiction over all federal criminal offenses. *See, e.g., United States v. Lopez-Acosta*, No. 13-CR-275, 2014 WL 3828225, at *3 (D. Neb. Aug. 4, 2014); *In re Search of Yahoo, Inc.*, No. 07-3194-MB, 2007 WL 1530071, at *5 (D. Ariz. May 21, 2007); *In re Search Warrant*, No. 05-MC-168-Orl-31-JGG, 2005 WL 3844032, at *5 (M.D. Fla. Feb. 13, 2006). The court has reviewed the rationale of these cases and agrees that the statute refers to territorial jurisdiction. The Maryland magistrate judge therefore lacked jurisdiction to issue the second warrant because the offense being investigated did not take place in Maryland.

Impact of the Lack of Jurisdiction

The government argues that any violation of the SCA does not require suppression because the SCA does not provide for a remedy of exclusion of evidence. The SCA provides that fines are the only remedies for nonconstitutional violations. 18 U.S.C. § 2708. But it does not address constitutional violations. The court must therefore determine whether a constitutional violation was involved.

Courts have found that warrants issued without jurisdiction are void from their inception. *See, e.g., United States v. Baker*, 894 F.2d 1144, 1147–48 (10th Cir. 1990). A warrant that is void from its inception is no warrant at all. *See United States v. Krueger*, 809 F.3d 1109, 1124–25 (10th Cir. 2015) (Gorsuch, J., concurring); *see also Groh v. Ramirez*, 540 U.S. 551, 559 (2004) ("[T]he warrant was so obviously deficient that we must regard the search as 'warrantless' within the meaning of our case law."). Using this logic, the search of defendant's email account was the equivalent of a warrantless search. Although all warrantless searches do not violate the Fourth Amendment, the government has not argued that it was reasonable to engage in a warrantless search in this instance. The Fourth Amendment prohibits unreasonable searches. The court therefore finds that the search of defendant's email account was a constitutional violation. *See Warshak*, 631 F.3d at 288 ("The government may not compel a commercial ISP to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause."). Suppression is a potential remedy for the violation.

Good Faith Exception

Having decided that the search of defendant's email account was essentially a warrantless search that could result in suppression of the evidence, the court now turns to whether the good faith exception applies in this instance. The first question is whether the good faith exception applies at all to warrants that are invalid from their inception.

The Tenth Circuit has not directly answered this question. *See Baker*, 894 F.2d at 1147 ("[T]he case at bar, involving a warrant but one that was essentially void ab initio, appears to fall somewhere between the two poles occupied by the defective-warrant and absent-warrant cases."). The court finds persuasive those cases that suggest the good faith exception does not apply to warrants that are invalid from their inception. *See, e.g., United States v. Scott*, 260 F.3d 512, 515 (6th Cir. 2001) ("[W]e are confident that *Leon* did not contemplate a situation where a warrant is issued by a person lacking the

requisite legal authority."), *overruled by United States v. Master*, 614 F.3d 236 (6th Cir. 2010)[1]; *United States v. Evans*, 469 F. Supp. 2d 893, 900 (D. Mont. 2007) ("The *Leon* good faith exception may possibly excuse a deficiency in the language of a warrant, but it does not apply to excuse the absence of a warrant.") (criticized by the Tenth Circuit on other grounds in *United States v. Cruz*, 774 F.3d 1278, 1288–90 (10th Cir. 2014)); *United States v. Neering*, 194 F. Supp. 2d 620, 627 (E.D. Mich. 2002).

Relying on the rationale in these cases, the court determines that the good faith exception applies only to evidence seized under a once-valid warrant that was subsequently invalidated—not evidence seized pursuant to a warrant that was void at its inception. In this instance, there was no warrant at all. Suppressing the evidence under these circumstances serves the goal of deterring police from obtaining warrants from judges who lack jurisdiction to issue them. Special Agent O'Donnell should have sought a warrant where the information was stored—in the Northern District of California. *See* Fed. R. Crim. P. 41(b) ("[A] magistrate judge with authority in the district . . . has authority to issue a warrant to search for and seize a person or property located within the district[.]"). The court understands that when Special Agent O'Donnell sought the warrant, he did not know what court had territorial jurisdiction over the crime. But Special Agent O'Donnell did know where the information was stored. The proper procedure would have been to seek a warrant there.

Fruit of the Poisonous Tree

Finally, the court turns to the warrant for a search of defendant's home. This warrant was based both on the information obtained as a result of the search of defendant's email account, as well as the information obtained as a result of the search of the jesusweptone@gmail.com account. The

[1] The Sixth Circuit has since "clarified" or "modified" its precedent in *Scott*. *Master*, 614 F.3d at 143. It now requires courts to apply a balancing test when determining whether to suppress evidence following a Fourth Amendment violation. *Id*. Nevertheless, this court finds the reasoning in *Scott* to be logical, and cites the case for its reasoning only—acknowledging that it may no longer be followed in the Sixth Circuit.

question is then whether, based on one void warrant and one warrant that defendant lacks standing to challenge, the evidence found in defendant's home must be suppressed based on the "fruit of the poisonous tree" doctrine.

When a search warrant relies on unconstitutionally obtained information, the warrant is not automatically invalid. Where probable cause exists without the unconstitutionally obtained information, the court need not suppress the evidence from the "tainted" warrant. *United States v. Sims*, 428 F.3d 945, 954 (10th Cir. 2005) ("When a warrant is tainted by some unconstitutionally obtained information, we nonetheless uphold the warrant if there was probable cause absent that information."); *see also United States v. Martinez*, 696 F. Supp. 2d 1216, 1244–45 (D.N.M. 2010), *aff'd*, 643 F.3d 1292 (10th Cir. 2011). "An affidavit containing erroneous or unconstitutionally obtained information invalidates a warrant if that information was critical to establishing probable cause. If, however, the affidavit contained sufficient accurate or untainted evidence, the warrant is nevertheless valid." *Sims*, 428 F.3d at 954 (citation omitted).

The standards for a valid search warrant are well-established: "Probable cause to issue a search warrant exists . . . when the supporting affidavit sets forth facts that would lead a prudent person to believe there is a fair probability that contraband or evidence of a crime will be found in a particular place." *United States v. Basham*, 268 F.3d 1199, 1203 (10th Cir. 2001). Here, without the information obtained from the bigw1991@gmail.com warrant, the affidavit still included information about child pornography being transferred involving the email account bigw1991@gmail.com. But Special Agent O'Donnell did not learn of the home address or the IP address until after executing the search warrant on the bigw1991@gmail.com account. It appears that he may have been able to independently learn the home address, but it is unclear whether Special Agent O'Donnell could have independently learned the IP address without the information from the tainted warrant.

On the record before it, the court cannot conclude that the search warrant for defendant's home contained sufficient information to support probable cause to search his home (or to know which home to search). The evidence found in defendant's home under the March 27, 2013 search warrant must also be suppressed as the fruit of the poisonous tree.

**IT IS THEREFORE ORDERED** that defendant William Elam Barber's Motion to Suppress Fruits of Illegal Searches (Doc. 29) is granted in part and denied in part. Although defendant lacks standing to challenge the warrant for the email account jesusweptone@gmail.com, defendant has successfully challenged the warrant for his own email account. The evidence obtained as a result of that second warrant must be suppressed. So, too, must the evidence from the search of defendant's house be suppressed as the fruit of the poisonous tree.

Dated this 27th day of April, 2016, at Kansas City, Kansas.

s/ Carlos Murguia
**CARLOS MURGUIA**
**United States District Judge**