

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

UNITED STATES OF AMERICA,

Plaintiff,

vs.

Case No. 16-10107-01-EFM

ANTHONY SHULTZ,

Defendant.

MEMORANDUM AND ORDER

This matter comes before the Court on Defendant Anthony Shultz' Motion to Suppress and for Return of Property (Doc. 67) and Motion to Suppress Evidence for Violation of Fed. R. Crim. P. 41 (Doc. 69). For the reasons stated below, the Court denies both motions.

I. Factual and Procedural Background

According to Shultz, between April 21, 2016, and June 12, 2016, the FBI issued 13 administrative subpoenas in its attempt to identify a person reportedly producing and distributing child pornography in the Philippines. In the subpoenas, the FBI sought information concerning specific phone numbers, email addresses, IP addresses, the name "Dean Hendrickson," the name "Anthony Schwartzendruber," the username "Maxwell Makati," and the Skype ID "MaxMakati49." The recipients of these subpoenas included Yahoo! Inc., Skype, Cox Communications, Dropbox.com, Google Inc., PayPal, AT&T, and Verizon Wireless.

On June 16, 2016, U.S. Magistrate Judge Gale for the District of Kansas issued two search warrants related to the investigation of Shultz—one to Yahoo!, Inc. and one to Dropbox, Inc. Both warrants identified the subject property as located in the Northern District of California. On July 18, 2016, U.S. Magistrate Judge Birzer issued a warrant to search Shultz' residence based on an affidavit prepared by FBI Special Agent Michael Daniels ("SA Daniels"). The FBI executed the search warrant on Shultz' residence and interviewed Shultz on July 20, 2016.

On July 21, 2016, the Government filed a four-count complaint against Shultz alleging violations of laws regarding illicit sexual conduct in a foreign place, production of child pornography, distribution of child pornography, and identity theft. Shultz was indicted on August 16, 2016, for the same alleged offenses. On April 12, 2017, a superseding indictment charged Shultz with the following: two counts of engaging in illicit sexual conduct in a foreign place, in violation of 18 U.S.C. § 2423; three counts of production of child pornography in violation of 18 U.S.C. § 2251; two counts of sex trafficking of children in violation of 18 U.S.C. §§ 1591, 1594, and 1596; one count of selling or buying of children in violation of 18 U.S.C. § 2251A; one count of distribution of child pornography in violation of 18 U.S.C. § 2252A; one count of possession of child pornography in violation of 18 U.S.C. § 2252A; and one count of identity theft in violation of 18 U.S.C. § 1028.

Shultz filed the motions currently before the Court on December 18, 2017. The Court held a hearing on the motions on January 12, 2018.

II. Analysis

In his motions to suppress, Shultz asserts that the Government utilized administrative subpoenas to obtain information from third parties in violation of the Fourth Amendment and the Video Privacy Protection Act (“VPPA”), that the affidavit in support of the search warrant for his residence lacked probable cause, and that Magistrate Judge Gale exceeded his authority when he issued search warrants to be executed in California. Shultz seeks an order suppressing all evidence derived from the administrative subpoenas and search warrants, and requests the return of property seized from him. The Court will address each motion in turn.

A. **Motion to suppress evidence derived from administrative subpoenas and from the search of Shultz’ residence (Doc. 67)**

Shultz argues that the Government’s use of administrative subpoenas to obtain information from third parties violated his Fourth Amendment rights, that the Government’s use of administrative subpoenas to obtain information from third parties violated the VPPA, and that the affidavit in support of the warrant to search Shultz’ home lacked probable cause. Shultz’ arguments lack merit.

1. The government properly utilized administrative subpoenas to obtain information

Shultz’ arguments regarding the Government’s use of administrative subpoenas fail. First, the government did not engage in a warrantless search in violation of the Fourth Amendment because Shultz did not have a reasonable expectation of privacy with regard to the information subpoenaed from third parties. Second, Shultz cannot establish a violation of the VPPA as he cannot show that the Government obtained personally identifiable information (“PII”) as defined by the VPPA, and regardless, the Government acted pursuant to explicit statutory authorization when it issued the subpoenas.

a. Reasonable expectation of privacy

The Fourth Amendment protects citizens from “unreasonable searches and seizures” conducted by state or federal government officials.¹ “A search only violates an individual’s Fourth Amendment rights if he or she has a ‘legitimate expectation of privacy in the area searched.’ ”² Courts employ a two-part test in determining whether a reasonable expectation of privacy exists. First, the defendant must demonstrate that he “manifested a subjective expectation of privacy in the area searched.”³ Second, the Court asks “whether society is prepared to recognize that expectation as objectively reasonable.”⁴ As the party seeking suppression, Shultz “has the burden of adducing facts” at the suppression hearing indicating that his rights were violated.⁵

Without citation, Shultz asserts that “customers of service providers such as the recipients of the administrative subpoenas issued in this case have a reasonable expectation of privacy in their personally identifiable and other account information.” Citing Tenth Circuit precedent, the Government argues that it merely sought subscriber information provided by Shultz to third parties, and that this information is not protected by the Fourth Amendment.⁶

¹ U.S. Const. amend. IV; *Mapp v. Ohio*, 367 U.S. 643, 654 (1961); *United States v. White*, 584 F.3d 935, 944 (10th Cir. 2009).

² *United States v. Ruiz*, 664 F.3d 833, 838 (10th Cir. 2012) (quoting *United States v. Anderson*, 154 F.3d 1225, 1229 (10th Cir. 1998)).

³ *Id.* (quoting *United States v. Allen*, 235 F.3d 482, 489 (10th Cir. 2000)). Shultz does not explicitly allege that he maintained a subjective expectation of privacy in the information subpoenaed by the Government.

⁴ *Id.* (quoting *Allen*, 235 F.3d at 489).

⁵ *United States v. Eckhart*, 569 F.3d 1263, 1274 (10th Cir. 2009) (quoting *Allen*, 235 F.3d at 489).

⁶ According to the Government, the subpoenas sought “the account holder’s name, address, length of service, subscriber number or identity, means and source of payment, registration IP address, and records of session times and durations.” Doc. 84, p. 16.

In *United States v. Perrine*,⁷ the Tenth Circuit recognized that “[e]very federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment’s privacy expectation.”⁸ Shultz has not identified any authority contradicting the Tenth Circuit’s holding and has not sought to distinguish the information obtained here from the subscriber information addressed in *Perrine*.⁹ Indeed, Shultz does not challenge the Government’s characterization of the information requested as subscriber information. Accordingly, Shultz has failed to identify facts indicating that he had a reasonable expectation of privacy in the records obtained via administrative subpoena.

b. VPPA

The VPPA prohibits “video tape service providers” from knowingly disclosing PII except as authorized by law.¹⁰ PII “obtained in any manner other than as provided in [the VPPA] shall not be received in evidence” in a subsequent legal proceeding.¹¹ The VPPA broadly defines a video tape service provider to mean “any person, engaged in the business, . . . of rental, sale or delivery of prerecorded video cassette tapes or similar audio visual materials.”¹² PII is defined as

⁷ 518 F.3d 1196 (10th Cir. 2008).

⁸ *Id.* at 1204. In *Perrine*, the Government obtained information from Yahoo! and Cox Communications regarding the IP address, name, physical address, and logon records for a username. *Id.* at 1199-1200. *See also Doe v. Shurtleff*, 628 F.3d 1217, 1226 (10th Cir. 2010); *United States v. Swenson*, 335 F. App’x 751, 754 n.1 (10th Cir. 2009).

⁹ Shultz criticizes the Government’s citation to *Smith v. Maryland*, for the proposition that the Supreme Court has made clear that an individual does not retain a reasonable expectation of privacy in information given to third parties, even if the individual subjectively expected the information to remain confidential. 442 U.S. 735 (1979). He argues that the Supreme Court may overturn *Smith* when it decides a case currently pending before the Supreme Court. Even if the Supreme Court overturns *Smith* and the other cases relied upon by the Government, however, the Government nevertheless acted in good faith based on the law as it existed at the time. *See United States v. Leon*, 468 U.S. 897 (1984).

¹⁰ 18 U.S.C. § 2710. The VPPA does not address disclosure of PII in response to administrative subpoenas.

¹¹ 18 U.S.C. § 2710(d).

¹² 18 U.S.C. § 2710(a)(4).

including “information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider.”¹³

Shultz argues that the information obtained pursuant to the administrative subpoenas should be suppressed under § 2710(d) because the recipients of the subpoenas are video service providers and they provided PII to the Government. Notably lacking from Shultz’ motion, perhaps by design, is any discussion of the definition of PII as that term is defined by the VPPA. During oral argument, Shultz advocated for an exceptionally broad definition of PII. He argued that the term “services” in the phrase “specific video materials or services” is completely divorced from and not modified by “video” or “specific video.” Thus, according to Shultz, the VPPA may be violated (1) by identifying a person as having requested or obtained specific video materials from a video tape service provider, or (2) by identifying a person as having requested or obtained *any* service¹⁴ from a video tape service provider. Further, Shultz claims that if not done in accordance with the VPPA’s disclosure provisions, the simple identification of a person as a consumer of the provider violates the VPPA, regardless of whether the provider also identifies specific goods or services the consumer sought, and regardless of whether the consumer requested or obtained audio visual materials or audio visual services.

Shultz requests the Court to adopt a broadly sweeping definition of PII because without it, his argument fails. He does not allege that the Government sought or received any information relating to video services or video materials obtained or requested by Shultz, let

¹³ 18 U.S.C. § 2710(a)(3).

¹⁴ As recognized during the hearing, many video tape service providers also offer numerous goods and services unrelated to audio video services or audio video materials. Shultz argued for an interpretation of the VPPA that would prohibit a provider from disclosing the fact that a consumer purchased a Coke or received an oil change from a business qualifying as a video tape service provider.

alone specific video materials or services.¹⁵ Nor does he allege that the government has relied upon or intends to introduce any such evidence. Rather, Shultz admits that the subpoenas requested information including names, addresses, IP addresses, telephone numbers, credit cards, and internet usage information such as log-in times and duration.

Shultz points to no authority to support his proposed interpretation of the term PII; nor has the Court located any. Although the Tenth Circuit has not addressed the definition of PII for purposes of the VPPA, courts that have addressed the meaning of PII have uniformly applied an interpretation linked to the disclosure of *video* materials or *video* services obtained by a specific individual. For example, the Third Circuit defines PII as information “that identifies a specific person *and* ties that person to particular videos that the person watched.”¹⁶ Courts have also rejected Shultz’ argument that merely identifying an individual as a consumer violates the VPPA.¹⁷

¹⁵ When asked what video material or service Shultz requested or obtained that is relevant to the subpoenas, Shultz responded, “The service, just the fact that he uses Cox, you know, he uses the service of Cox for Internet or that he uses Gmail.” Doc. 112, p. 83.

¹⁶ *In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 285 (3d Cir. 2016) (quoting *In re Hulu Privacy Litig.*, 2014 WL 1724344, at *8 (N.D. Cal. 2014); citing *Eichenberger v. ESPN, Inc.*, 2015 WL 7252985, at *4) (W.D. Wash. 2015)) (emphasis added). See also *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 985 (9th Cir. 2017) (recognizing that the VPPA prohibited a video rental store from disclosing “the name and address of a customer—along with a list of the videos that the customer had viewed”); *Yershov v. Gannett Satellite Info. Network, Inc.*, 820 F.3d 482, 486 (1st Cir. 2016) (holding that complaint adequately alleged a claim where defendant disclosed information reasonably and foreseeably likely to reveal which videos a specific subscriber had obtained); *Lewert v. P.F. Chang’s China Bistro, Inc.*, 819 F.3d 963, 968 (7th Cir. 2016) (recognizing that the VPPA “does not recognize a legal interest in personally identifiable information beyond the video-rental context”); *In re Vizio, Inc., Consumer Privacy Litig.*, 238 F. Supp. 3d 1204, 1225 (C.D. Cal. 2017) (finding that to state a claim, plaintiffs must demonstrate that the disclosures “are ‘reasonably and foreseeably likely to reveal’ what video content Plaintiffs have watched”); *Robinson v. Disney Online*, 152 F. Supp. 3d 176, 179 (S.D.N.Y. 2015) (recognizing that information disclosed must identify a particular person “and connect this particular person with his or her viewing history”); *Hulu*, 2014 WL 1724344, at *7 (discussing disclosures of unique numeric identifiers “tied to video watching”).

¹⁷ *FTC v. Amazon.com, Inc.*, 2015 WL 11256312, at *2-3 (W.D. Wash. 2015) (rejecting argument that identifying customers denied a refund for in-app purchases violates the VPPA because no specific video information had been requested); *Amazon.com LLC v. Lay*, 758 F. Supp. 2d 1154, 1170-72 (W.D. Wash. 2010) (holding that request for records of “all information for all sales” from Amazon clearly requested the sales of specific video titles, and that the government could not obtain names, addresses or other personal information of customers as long as it

In accordance with every other court to address the issue, as well as the legislative history surrounding the enactment of the VPPA,¹⁸ this Court finds that the term “specific video” in the definition of PII modifies not only the word “material,” but also the word “services.” Since Shultz has not identified any information relating to video material or video services revealed in response to the administrative subpoenas, he cannot establish that the Government obtained, introduced, or intends to introduce PII as defined for purposes of the VPPA. Accordingly, it is unnecessary to address the Government’s argument regarding the scope of the term “video tape service provider.”¹⁹ Shultz’ request to suppress information obtained in response to the administrative subpoenas is denied.

c. Title, 18 U.S.C. § 3486 and the Stored Communications Act

Though Shultz’ motion is properly denied on the grounds discussed above, the Court also notes that the Government acted pursuant to explicit statutory authorization when it issued the administrative subpoenas in question. Congress has broadly authorized the Government “[i]n any investigation of . . . a Federal offense involving the sexual exploitation or abuse of children,”

continued to have access to or possession of Amazon’s detailed purchase records); *Gonzalez v. Cent. Elec. Cooperative, Inc.*, 2009 WL 3415235, at *9-11 (D. Or. 2009) (holding that evidence indicating a plaintiff purchased one of 15 movies, but not identifying which movie, does not constitute PII for purposes of the VPPA).

¹⁸ Congress enacted the VPPA in response to the disclosure and publication of 146 films that then-Supreme Court nominee Judge Robert H. Bork and his family had rented from a video store. *Yershov*, 820 F.3d at 485. The stated purpose of the VPPA is “[t]o preserve personal privacy with respect to the rental, purchase or delivery of video tapes or similar audio visual materials.” *Id.* As recognized in the legislative history, the definition of PII “includes the term ‘video’ to make clear that simply because a business is engaged in the sale or rental of video materials or services does not mean that all of its products or services are within the scope of the bill.” S. Rep. No. 100-599, at 12 (1988), *reprinted in* 1988 U.S.C.C.A.N. 4342-1. It states, for example, that “a department store that sells video tapes would be required to extend privacy protection to only those transactions involving the purchase of video tapes and not other products.” *Id.* The legislative history also states that “a video tape service provider is not prohibited from responding to a law enforcement agent’s inquiry as to whether a person patronized a video tape service provider at a particular time or on a particular date.” *Id.*

¹⁹ The Government also argues that simply because subsidiaries of the recipients of the subpoenas qualify as video tape service providers does not mean that the separate branches of those companies also qualify as video tape service providers.

to issue administrative subpoenas for “the production of *any* records or other things relevant to the investigation.”²⁰ The lone limitation in § 3486 applies to providers of electronic communication services and remote computing services under the Stored Communication Act (“SCA”).²¹ This limitation, however, does not prohibit the use of administrative subpoenas. Rather, it merely restricts the scope of information the Government may subpoena from these service providers to include the following information for a subscriber or customer:

- (A) name;
- (B) address;
- (C) local and long distance telephone connection records, or records of session times and durations;
- (D) length of service (including start date) and types of service utilized;
- (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
- (F) means and source of payment for such service (including any credit card or bank account number).²²

Shultz wholly fails to present any argument or offer any rationale as to why the Court should ignore the explicit statutory authorization of the Government’s use of the administrative subpoenas in its investigation. Indeed, he ignores these statutes even though each subpoena conspicuously states that it was issued under the authority of § 3486 and attaches a copy of its language, and despite the fact that the Government discussed §§ 3486 and 2703 in its response brief and noted during oral argument that the information obtained pursuant to the subpoenas falls under the SCA. Shultz’ total failure to address this issue is as telling as the statutes are

²⁰ 18 U.S.C. § 3486(a) (emphases added).

²¹ 18 U.S.C. § 3486(a)(1)(C).

²² *Id.*; 18 U.S.C. 2703(c)(2) (recognizing that these providers “shall disclose” such information “when the governmental entity uses an administrative subpoena authorized by a Federal or State statute”).

clear. The Government properly issued administrative subpoenas under 18 U.S.C. §§ 3486 and 2703, and only requested information within the scope of § 2703(c)(2).

2. *The affidavit in support of the warrant to search Shultz' residence adequately establishes probable cause*²³

The Fourth Amendment provides 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 “[T]he physical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed.”²⁵ “To search a suspect’s residence, ‘[a] search warrant must be supported by probable cause, requiring more than mere suspicion but less evidence than is necessary to convict.’”²⁶ “The task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place.”²⁷ The court asks “whether the facts presented in the affidavit would ‘warrant a man of reasonable caution’ to believe that evidence of a crime will be found at the place to be searched.”²⁸ In reviewing a determination of probable cause, the Court affords “great deference” to the issuing judge’s determination.²⁹ The Court’s duty is to ensure that the issuing judge had a

²³ Unless otherwise noted, the facts listed in this section appear in the warrant affidavit submitted as Defendant’s Exhibit 1.

²⁴ U.S. Const. amend IV.

²⁵ *United States v. Edwards*, 813 F.3d 953, 960 (10th Cir. 2015).

²⁶ *Id.* (quoting *United States v. Danhauer*, 229 F.3d 1002, 1005 (10th Cir. 2000)) (alteration in original).

²⁷ *United States v. Nolan*, 199 F.3d 1180, 1182 (10th Cir.1999) (citing *Illinois v. Gates*, 462 U.S. 213, 238 (1983)).

²⁸ *Id.* (citing *Texas v. Brown*, 460 U.S. 730, 742 (1983)).

²⁹ *United States v. Finnigin*, 113 F.3d 1182, 1185 (10th Cir. 1997).

“substantial basis” for concluding that the affidavit in support of the search warrant established probable cause.³⁰

Shultz disputes Judge Birzer’s probable cause finding for two reasons. First, he claims that the affidavit relies on information obtained in violation of the VPPA, and that without this information, the affidavit lacks probable cause. As stated above, the Government did not obtain PII in violation of the VPPA or use PII in the affidavit, accordingly, this argument fails.³¹ Second, Shultz argues that even with the information obtained via administrative subpoena, the probable cause affidavit fails to link the alleged criminal activity to Shultz’ home. He asserts that the affidavit’s general allegation that most people who collect child pornography keep it at home or in another secure location is insufficient to meet the nexus element of probable cause.

After examining the warrant affidavit, the Court concludes that ample evidence supports the probability that evidence of violations of 18 U.S.C. §§ 2251, 2252, 2252A, and 2423 would be found in Shultz’ home. The affidavit provides a detailed account of the investigation completed at the time of the search warrant request and clearly establishes probable cause.³² Highly summarized, the affidavit states that in investigating reports of a U.S. citizen sexually abusing minors in the Philippines, the FBI obtained information that someone operating under the name “Max Makati” was sexually abusing minors, live-streaming the sexual abuse of minors,

³⁰ *Nolan*, 199 F.3d at 1182 (citing *Gates*, 462 U.S. at 236).

³¹ Additionally, although Shultz has failed to assert a colorable argument that the VPPA was violated, even if a violation had occurred, the Government acted in good faith in relying on the search warrant based on the law as it existed at the time. *See Leon*, 468 U.S. 897. *See also* 18 U.S.C. § 3486(a); 18 U.S.C. § 2703(c)(2).

³² Further, it is not necessary that the affidavit “contain personal knowledge of illegal activity at the residence.” *United States v. \$149,442.43*, 965 F.2d 868, 874 (10th Cir. 1992). *See also United States v. Deppish*, 994 F. Supp. 2d 1211, 1218 (D. Kan. 2014) (noting that “[t]he affidavit need not aver that criminal activity actually occurred in” the location to be searched as long as “‘a person of reasonable caution’ would ‘believe that the articles sought would be found’ ” in the place to be searched).

producing videos depicting the sexual abuse of minors, and distributing child pornography, that “Max Makati” accepted money via PayPal under the name “Dean Hendrickson” in return for distributing child pornography, and that “Max Makati” told an undercover journalist that a girl being sexually assaulted by “Max Makati” was 13 years old. The FBI also obtained videos received by the journalist from “Max Makati,” two of which contained “Max Makati’s” face. In its investigation, the FBI connected the aliases “Max Makati” and “Dean Hendrickson,” as well as numerous e-mail addresses and other account information associated with the aliases used in the alleged sexual exploitation of children, to Shultz’ address in Lindsborg, Kansas. Additionally, records received from PayPal pertaining to the user name “Dean Hendrickson” indicated that the user’s address matched Shultz’ address in Lindsborg. The FBI accessed Shultz’ Kansas driver’s license photograph, Shultz’ U.S. passport records, and a Facebook page for Anthony Michael Shultz, and determined that the photographs of Shultz matched the individual in the videos sexually abusing minors and identified as “Max Makati.” State Department records also indicated that Shultz traveled from the United States to the Philippines.

SA Daniels stated that based on his training and experience, the majority of child pornography offenders share certain traits, including collecting sexually explicit materials; seeking other like-minded individuals, often through Internet-based mediums; collecting materials on the subject of sexual activities with children as a way of understanding their own feelings; and maintaining information relating to other individuals that have similar sexual interests. SA Daniels also stated that:

The majority of individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials. They almost always maintain their collections in the privacy and security of their homes or other secure location, such as in password-protected online storage.

SA Daniels stated his belief that “Shultz evinces many of these characteristics common to child pornography offenders, particularly as it relates to the usage of computers and the internet for his child pornography or sexual abuse activity.”

A person of reasonable caution considering the facts identified in the affidavit would accept the probability that evidence of the crimes alleged would be found at Shultz’ home. Accordingly, when viewing the totality of the circumstances presented in the affidavit, a substantial basis supports the Magistrate Judge’s decision that probable cause existed to authorize a warrant to search Shultz’ home and seize the property at issue. Shultz’ motion to suppress evidence obtained as a result of the warrant to search his residence is denied.³³

B. Motion to suppress evidence obtained in violation of Fed. R. Crim. P. 41

Shultz argues that U.S. Magistrate Judge Gale for the District of Kansas exceeded the bounds of his authority under Federal Rule of Criminal Procedure 41(b) by issuing search warrants to be executed in the Northern District of California. Accordingly, he argues, the search warrants were invalid and all information derived from the search warrants should be suppressed. The Government argues that the Stored Communications Act (“SCA”) explicitly authorizes U.S. Magistrate Judges to issue search warrants like those at issue here.³⁴

Despite the fact that the application for the search warrant to Yahoo! explicitly identifies 18 U.S.C. § 2703 as authority to issue a search warrant for property located in another district,³⁵

³³ Even if probable cause was lacking, denial of Shultz’ motion to suppress is proper under the good faith exception recognized in *Leon*.

³⁴ The Government represents that it does not intend to introduce information obtained from the Dropbox warrant in its case in chief, but rather, only evidence obtained from Dropbox pursuant to subpoena.

³⁵ See Defendant’s Exhibit 18.

Shultz' motion fails to address the applicability of § 2703. When questioned about the applicability of § 2703 during the hearing, Shultz advanced two arguments. First, he asserted that Rule 41 trumps § 2703. Second, he argued that if the Court is authorized to issue a warrant for property outside of the District of Kansas, then the Court should strike the information obtained in violation of the VPPA from the affidavit and then analyze the affidavit to determine if there is still evidence of jurisdiction in Kansas absent such information. As discussed above, the Government did not obtain information in violation of the VPPA. Accordingly, Shultz' second argument fails.

Shultz' argument that Rule 41 somehow vitiates the authorization provided by § 2703 also fails. The plain language of Rule 41(a) and § 2703, as well as caselaw analyzing the interplay between these rules, clearly establishes that the Magistrate Judge had authority to issue the warrants in question. Rule 41(a) explicitly states “[t]his rule does not modify any statute regulating search or seizure, or the issuance and execution of a search warrant in special circumstances.” The SCA authorizes a court of competent jurisdiction to issue a warrant for information identified in § 2703, and defines “a court of competent jurisdiction” as “*any* district court of the United States (including a magistrate judge of such a court)” that “has jurisdiction over the offense being investigated.”³⁶ Courts have recognized that this means “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).”³⁷ Thus, if a Court has

³⁶ 18 U.S.C. §§ 2703, 2711(3) (emphasis added).

³⁷ *United States v. Barber*, 184 F. Supp. 3d 1013, 1017 (D. Kan. 2016).

jurisdiction over the offense being investigated, it may issue a warrant to search property not located in its district under § 2703.

Several courts have grappled with whether the phrase “jurisdiction over the offense” refers to subject matter, personal, or territorial jurisdiction.³⁸ These courts appear in agreement that “territorial jurisdiction” is required. The Court need not decide this issue here, however, because there is no dispute that each type of jurisdiction is present. The Court clearly had subject matter jurisdiction over the federal offenses being investigated, as well as personal jurisdiction over Shultz. Likewise, the affidavit connected the various accounts and aliases Shultz allegedly utilized in the commission of the crimes charged to his residence in Lindsborg, Kansas, establishing territorial jurisdiction. Indeed, Shultz does not dispute the Government’s assertion that “the offense(s) being investigated . . . related to the sexual exploitation of children *from Lindsborg, Kansas* – specifically, importing sexual exploitation material produced in a foreign country, trafficking child pornography and traveling in foreign commerce to engage in sexually explicit conduct.”³⁹ Rather, he simply requests that the Court strike certain information in the affidavit and reevaluate the affidavit to “see whether or not there’s still evidence of jurisdiction in Kansas.”⁴⁰

The Magistrate Judge did not exceed his authority in issuing the search warrants in question here. Accordingly, Shultz’ motion to suppress is denied.

³⁸ See *id.*; *United States v. Alahmedalabdaloklah*, 2017 WL 2839645, at *4-5 (D. Ariz. 2017); *In re Search of Yahoo, Inc.*, 2007 WL 1539971, at *3 (D. Ariz. 2007); *In re Search Warrant*, 2005 WL 3844032, at *4-5 (M.D. Fla. 2006).

³⁹ Doc. 85, p. 6 (emphasis in original).

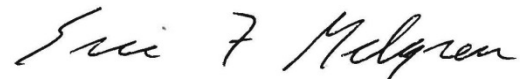
⁴⁰ Doc. 112, p. 90.

IT IS THEREFORE ORDERED that Defendant Anthony Shultz' Motion to Suppress and For Return of Property (Doc. 67) is **DENIED**.

IT IS FURTHER ORDERED that Defendant Anthony Shultz' Motion to Suppress Evidence for Violation of Fed. R. Crim. P. 41 (Doc. 69) is **DENIED**.

IT IS SO ORDERED.

Dated this 24th day of January, 2018.


ERIC F. MELGREN
UNITED STATES DISTRICT JUDGE