

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

UNITED STATES OF AMERICA,

Plaintiff,

vs.

JASON WAYNE IRVING,

Defendant.

Case No. 18-10019-EFM

MEMORANDUM AND ORDER

This matter comes before the Court on Defendant Jason Wayne Irving’s Motion to Suppress (Doc. 18). Defendant seeks suppression of all evidence obtained against him pursuant to two search warrants. The second search warrant was based on the findings of the first search warrant. The Court finds that Defendant has standing to object to the search, the search warrant was overbroad, and the good faith exception cannot save the illegal search. Because the first search warrant is invalid, the second search warrant is also invalid. Accordingly, the Court grants Defendant’s Motion to Suppress.

I. Factual and Procedural Background

On March 20, 2017, Officer Jordon Garrison with the Pittsburg, Kansas police department, requested a search warrant for items related to a Facebook account in the name of “jasson.irving.” In Officer Garrison’s affidavit, he alleged that he had probable cause to believe that Defendant

was in violation of the Kansas Offender Registry Act. He stated that he had received a report on March 14, 2017, that Defendant (a registered sex offender) was walking with a young juvenile at odd hours of the night.

On March 15, Officer Garrison conducted a registered offender search and learned that Defendant lived within Crawford County. He also located a Facebook page with the user ID of jasson.iring. Officer Garrison believed that account belonged to Defendant because (1) the name was similar to Defendant's name, (2) the owner of the account had Facebook "friends" associated with Defendant's address, (3) the profile picture looked like Defendant's registered offender pictures, and (4) the profile listed an association to Arkansas City, Kansas for which Defendant had ties.

Officer Garrison averred that he knew that registered sex offenders were required, pursuant to K.S.A. § 22-4907(a)(19), to provide any online identities used by the offender. Officer Garrison confirmed that Defendant had not provided any information related to this Facebook account. Thus, Officer Garrison sought a search warrant for Defendant's Facebook account.

Officer Garrison stated in his affidavit that the information and records maintained by Facebook for the user ID jasson.iring had "the potential to provide identifying information for the account's user, identify investigative leads, and corroborate other information obtained during the investigation." He sought a detailed list of seven categories of evidence. This included (1) all contact and personal identifying information, (2) all activity logs showing his posts, (3) all photoprints, (4) all Neoprints (which included profile and news feed information, status updates, wall posting, friend lists, future and past event posting, comments, tags, and more), (5) all chat and private messages, (6) all IP logs, and (7) all past and present lists of friends.

The Crawford County, Kansas, district judge approved and issued the search warrant (“the first search warrant”) the same day. Two days later, Defendant went to the police station to speak with Officer Garrison after Facebook notified him of the search warrant. Officer Garrison was not there, and they never spoke.

On April 17, 2017, Officer Garrison received the requested information from Facebook. After reviewing the records, he noted communications with suspected minors involving nude photographs. The following week, Officer La’Mour Romine reviewed the account and observed suspected child pornography. Based on this suspected child pornography, Officer Romine sought and obtained a search warrant (“the second search warrant”) to search Defendant’s house for child pornography.

In January 2018, the government filed a four-count indictment against Defendant charging him with production of child pornography, production of child pornography while required to register as a sex offender, distribution of child pornography, and possession of child pornography. The first two counts were subsequently dismissed, and only the latter two remain.

Defendant filed a Motion to Suppress. He asserts that the government’s affidavit for the first search warrant lacks particularity and is overbroad. He contends that because the first search warrant was defective, all evidence (including the evidence obtained from the second search warrant as it was based on the information received from the defective first search warrant) must be suppressed. The Court held a hearing on August 1, 2018.

II. Analysis

Defendant argues that the Fourth Amendment requires suppression of all evidence found against him because the first search warrant lacks particularity and is overbroad. The government

contends that (1) Defendant lacks standing to object to the search, (2) the warrant is sufficiently particular, and (3) even if the warrant lacks particularity, the good faith exception is applicable.

A. Defendant has standing to object to the Facebook search

“The Fourth Amendment protects the ‘right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.’”¹ This right is personal, and “a defendant may only claim the benefits of the exclusionary rule if his own Fourth Amendment rights have in fact been violated.”² The burden is on Defendant to establish this standing.³

Under the reasonable expectation of privacy approach, “[a] search only violates an individual’s Fourth Amendment rights if he or she has a legitimate expectation of privacy in the area searched.”⁴ There is a two-part test in determining whether a reasonable expectation of privacy exists.⁵ First, the defendant must demonstrate that he “manifested a subjective expectation

¹ *United States v. Johnson*, 584 F.3d 995, 999 (10th Cir. 2009) (citing U.S. Const. amend. IV).

² *Id.* (quotation marks and citation omitted).

³ *Id.* at 998. As the United States Supreme Court made clear in a recent opinion, standing in the Fourth Amendment context is not a jurisdictional question. *Byrd v. United States*, --- U.S. ---, 138 S. Ct. 1518, 1530 (2018). Instead, “[t]he concept of standing in Fourth Amendment cases can be a useful shorthand for capturing the idea that a person must have a cognizable Fourth Amendment interest in the place searched before seeking relief for an unconstitutional search.” *Id.* Should a court determine that another justification exists for the search, it is not required to assess whether an individual possesses a reasonable expectation of privacy in the place searched. *See id.* at 1530-31.

⁴ *United States v. Ruiz*, 664 F.3d 833, 838 (10th Cir. 2012) (quotation marks and citation omitted). Defendant also argues that under a property-rights approach, he has a property interest in his Facebook account and the Court could find that this ownership gives him standing to object to the search. The Court will only consider Defendant’s standing under the privacy-rights approach.

⁵ *See Smith v. Maryland*, 442 U.S. 735, 740 (1979).

of privacy in the area searched.”⁶ Next, there is the question of “whether society is prepared to recognize that expectation as objectively reasonable.”⁷

The government contends that Defendant does not sufficiently demonstrate that he had a legitimate expectation of privacy to object to the search because (1) he was an unauthorized user of Facebook, (2) much of his account was public, and (3) any expectation of privacy was thwarted by Facebook’s Terms of Service (“TOS”) and notification of its intention to provide information to law enforcement. Defendant disagrees and asserts that he does have standing.

1. Unauthorized User

The government argues that Defendant does not have a legitimate expectation of privacy in his Facebook account because he was an unauthorized user of Facebook. Defendant was an unauthorized user of Facebook because he was a convicted sex offender and Facebook’s TOS prohibits convicted sex offenders from using Facebook. Facebook, however, allowed Defendant to have an account on Facebook and he remained on Facebook at the time of the search (and after the search). Thus, it appears that Facebook viewed Defendant as an authorized user who had privacy rights in his account. This conclusion is bolstered because Facebook sent a notice to Defendant that the government sought a search warrant for his account. Furthermore, it is unclear why an unauthorized user loses a reasonable expectation of privacy.⁸ In the same way that an individual who is a smoker may falsely represent to a landlord that he is not a smoker to obtain an

⁶ *Johnson*, 584 F.3d at 999 (citation omitted).

⁷ *Id.* (quotation marks and citation omitted).

⁸ Facebook’s TOS also prohibits individuals under the age of 13 from using Facebook, so the government’s argument would necessarily mean that any individual under the age of 13 does not have any legitimate expectation of privacy in a Facebook account even though Facebook allowed that individual to set up an account. This proposition does not appear tenable.

apartment lease, that individual does not lose all expectation of privacy in the rented apartment. Accordingly, the Court finds the government's argument without merit.

2. *Public Account*

Next, the government argues that much of Defendant's Facebook account was public. Facebook, however, has privacy settings as well and allows its users to set posts to private or public. In addition, Facebook has a "messenger" component which is always private because it is not available for the public to view. Indeed, the government states that an area in which Defendant could ostensibly assert a privacy interest would be his Facebook messages.⁹ The fact that the majority of an individual's information may be found on a "public" portion of Facebook does not mean that one gives up any expectation of privacy. "A person does not surrender all Fourth Amendment protection by venturing into the public sphere."¹⁰ Furthermore, the fact that there is a line between public and private access would further demonstrate a reasonable expectation of privacy in the information shared privately. Thus, the government's argument fails on this point.

3. *Facebook's TOS*

Finally, the government contends that any expectation of privacy was thwarted by Facebook's TOS and its notification to Defendant of its intention to provide information to law enforcement. Facebook's TOS has several provisions relating to collecting information and the content posted on Facebook. The TOS generally informs users that Facebook collects a user's content and information. The TOS also provides that the user, by accessing Facebook, agrees that Facebook can collect and use content and information in accordance with its Data Policy. At the

⁹ It appears that the information Defendant seeks to suppress comes from being found in the "messenger" component.

¹⁰ *Carpenter v. United States*, --- U.S. ---, 138 S. Ct. 2206, 2217 (2018).

same time, however, Facebook informs the user that the user owns all of the content and information and can control how it is shared through the user's settings. In requesting a user to "help to keep Facebook safe," the TOS provides that the user not post content that is pornographic or contains nudity. In a provision entitled "protecting other people's rights," Facebook states that it can remove content or information that it believes violates the TOS or its policies. The government contends that these provisions in Facebook's TOS inform its users that using Facebook means a user uses it at one's peril. The Court disagrees, but the Court must discuss two District of Kansas cases first.

Two cases from the District of Kansas, *United States v. Stratton*¹¹ and *United States v. Ackerman*,¹² have found that a TOS diminishes a user's objectively reasonable expectation of privacy. The circumstances and the TOS's, however, are different from this case. In *Stratton*, the defendant had an account through electronic service provider Sony's PlayStation Network ("PSN").¹³ Users can communicate with other users online in a manner similar to email communication, and users must agree to Sony's TOS.¹⁴ The defendant sent messages about child pornography and downloaded images that included child pornography.¹⁵

In *Stratton*, the Court noted that users of Sony's PSN had to agree to the TOS when signing up for an account.¹⁶ The TOS included such terms that Sony reserved the right to monitor online

¹¹ 229 F. Supp. 3d 1230 (D. Kan. 2017).

¹² 296 F. Supp. 3d 1267 (D. Kan. 2017). This case was decided by the undersigned, and it is currently on appeal to the Tenth Circuit Court of Appeals.

¹³ *Stratton*, 229 F. Supp. 3d at 1233.

¹⁴ *Id.*

¹⁵ *Id.* at 1235.

¹⁶ *Id.* at 1233.

activity and that users must not violate any laws.¹⁷ The TOS also provided that Sony, in its sole discretion, could make a determination on what was offensive, hateful, or vulgar.¹⁸ In addition, Sony monitored misuses of its PSN through PSN reports and actively viewed and monitored the content to determine if it violated its TOS.¹⁹ Indeed, Sony turned over the information it received regarding the defendant's account to the National Center for Missing and Exploited Children ("NCMEC").²⁰ Thus, the Court found that the TOS "explicitly nullified its users reasonable expectation of privacy" because Sony informed its users that it reserved the right to monitor activity and any violations of laws may be turned over to law enforcement authorities.²¹

In *Ackerman*, the defendant agreed to AOL's TOS by using his email account.²² The TOS expressly alerted the defendant that he was not to participate or engage in illegal activity.²³ In addition, the TOS provided that a user must not post explicit sexual acts.²⁴ Furthermore, AOL's TOS informed the defendant that if he did not comply with the TOS, it could take technical, legal or other actions (in its sole discretion) without notice to him to enforce the TOS.²⁵ And in fact, AOL did just that.²⁶ When AOL flagged an email containing previously identified child

¹⁷ *Id.*

¹⁸ *Id.*

¹⁹ *Id.* at 1234.

²⁰ *Id.* at 1235.

²¹ *Id.* at 1242.

²² 296 F. Supp. 3d at 1271.

²³ *Id.*

²⁴ *Id.* at 1271-72.

²⁵ *Id.* at 1272.

²⁶ *Id.* at 1270.

pornography, AOL shut down the defendant's email account and forwarded the email to NCMEC.²⁷ NCMEC then reviewed the email and the attached images.²⁸

In *Ackerman*, the government took a narrow position and asserted that the defendant did not have a reasonable expectation of privacy in his email and the attachments (the one email that contained the contraband) *after* AOL terminated the account for violating its TOS.²⁹ This Court found that AOL's TOS limited the defendant's reasonable expectation of privacy because AOL explicitly informed him that he must comply with applicable laws and that AOL may take technical and legal action against him if he failed to do so.³⁰ And in fact, AOL did take action against him (terminated the defendant's account) after he failed to comply with the TOS. Accordingly, the Court found that he lacked a reasonable expectation of privacy in that email.³¹

Here, the factual circumstances and the TOS are different. Facebook's TOS does not have explicit terms about monitoring user's accounts for illegal activities and reporting those activities to law enforcement. Instead, Facebook's TOS generally states that Facebook can collect data and information. It also states, however, that the user owns all of the content and information and can control how to share it. Although Facebook's TOS does state that a user should not post content that is pornographic or unlawful, it makes these statements in the context of safety and in asking for the user's help "to keep Facebook safe."

²⁷ *Id.*

²⁸ *Id.*

²⁹ *Id.* at 1271. The government did not rely on the third-party doctrine and agreed that the defendant had an expectation of privacy in his email account *before* AOL terminated the account. *Id.*

³⁰ *Id.* at 1272.

³¹ *Id.*

Furthermore, unlike the service providers in *Stratton* (Sony PSN) and *Ackerman* (AOL), Facebook did not terminate Defendant's account due to a violation of its TOS. Here, Defendant's account was active and viable at the time the government sought a search warrant. Indeed, at the time the government sought the search warrant, there was no indication that Defendant had violated Facebook's TOS.³² Accordingly, the Court finds that Defendant has standing because he had a reasonable expectation of privacy in his Facebook account.

B. The warrant was overbroad

“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.’ ”³³ With regard to the particularity requirement, it “prevents general searches and strictly limits the discretion of the officer executing the warrant.”³⁴ “It is not enough that the warrant makes reference to a particular offense; the warrant must ensure that the search is confined in scope to particularly described evidence relating to a specific crime for which there is demonstrated probable cause.”³⁵

Here, the warrant at issue (the first search warrant) states that the crime being investigated is a violation of the Kansas Offender Registry Act. This act requires a convicted sex offender to register any and all email addresses and online identities used on the internet.³⁶ The warrant lists

³² The search warrant, along with the evidence from that search, is the very evidence demonstrating Defendant's violation of Facebook's TOS.

³³ *Cassady v. Goering*, 567 F.3d 628, 634 (10th Cir. 2009) (citing U.S. Const. amend. IV).

³⁴ *Id.* at 635 (citations omitted).

³⁵ *Id.* at 636 (internal quotation marks and citation omitted).

³⁶ *See* K.S.A. § 22-4907(a)(19).

seven categories of items to be seized. These include (1) all contact and personal identifying information, including name, user identification number, birth date, gender, contact email addresses, Facebook passwords, Facebook security questions and answers, physical address, telephone numbers, screen names, and other personal identifiers; (2) all activity logs and all other documents showing the user's posts; (3) all photoprints, including all photos uploaded by the user or photos tagging the user; (4) all Neoprints, including profile contact information, status updates, photographs, wall postings, friend lists, groups and networks, rejected friend requests, comments; (5) all other records of communications and messages made or received by the user including all private messages, chat history, video calling history, and pending friend requests; (6) all IP logs; and (7) all past and present lists of friends created by the account.

The government argues that the warrant was limited to the specific Facebook account and identified areas associated with user attribution information. This warrant, however, allowed the officer to search virtually every aspect of Defendant's Facebook account. It required disclosure of all data and information that was contained in his account. It included all contact and personal identifying information, all private messages and chat histories, all video history, all activity logs, all IP logs, all friend requests, all rejected friend requests, all photoprints, all Neoprints, and all past and present lists of friends. In addition, there was no specified time frame so the warrant covered the entire timeframe that Defendant operated and had the Facebook account.³⁷ In sum, the warrant encompassed everything in Defendant's Facebook account and there were no set limits.

³⁷ The government argues that the operation of the Facebook account reflected a new violation each time Defendant did not report the account, and thus, the investigation included the entire account to determine the full extent of Defendant's use.

As noted by the Eleventh Circuit, Facebook searches can be limited to specific information. In *United States v. Blake*,³⁸ the Eleventh Circuit found the government's Facebook search to be overbroad because it "required disclosure to the government of virtually every kind of data that could be found in a social media account."³⁹ The Eleventh Circuit noted that the warrant could have been more limited in time and limited to the crime at issue. Had the request been more limited, the Eleventh Circuit stated that it "would have undermined any claim that the Facebook warrants were the internet-era version of a 'general warrant.'"⁴⁰

Similarly, in this case, the warrant could have been more limited in scope and time. The only crime specified was the registration violation. This crime is simply that Defendant, as a registered sex offender, failed to register that he had Facebook account. The information that the officer sought was user attribution information and that Defendant was on Facebook and failed to register his account. The scope of the warrant should have been defined and limited by that crime. Instead, the warrant allowed for the search and seizure of Defendant's entire Facebook account. It appears to be more akin to a general warrant rummaging through any and all of Defendant's electronic belongings in Facebook. Thus, the warrant here was overly broad and general. Accordingly, it was an improper search warrant.⁴¹

³⁸ 868 F.3d 960 (11th Cir. 2017).

³⁹ *Id.* at 974.

⁴⁰ *Id.* (citation omitted).

⁴¹ The parties do not discuss severability of the warrant, but it does not appear applicable in this case. Generally, if a warrant is found to be overbroad, the Court suppresses evidence seized from the improper part of the warrant, but it does not suppress evidence seized from the valid portion of the warrant. *United States v. Sells*, 463 F.3d 1148, 1150 (10th Cir. 2006). To determine whether severability is applicable, a court divides the warrant into individual parts to determine whether that portion satisfies the requirement of probable cause and particularity. *Id.* at 1151. As noted, the parties do not discuss this doctrine or its applicability. Thus, it is not prudent for the Court to undertake this analysis.

C. Good Faith

“Even if the warrant was not sufficiently particularized to comply with the Fourth Amendment, the evidence need not be excluded if the search qualified under the good faith doctrine of *United States v. Leon*.”⁴² There are several circumstances, however, in which the *Leon* good faith exceptions may not be applicable. Relevant to this case, an officer may not rely on a warrant when it “is so facially deficient that the executing officer could not reasonably believe it was valid.”⁴³ In making this determination, “the good-faith inquiry is confined to the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal despite the magistrate’s authorization.”⁴⁴ “It is the government’s burden to prove its agents’ reliance upon the warrant was objectively reasonable.”⁴⁵

As noted above, the warrant in this case was overbroad and amounted to a general rummaging of Defendant’s effects, albeit electronically through his Facebook account. The Court, however, must review the text of the warrant as well as the circumstances of the search to determine whether the officer reasonably presumed it to be valid.⁴⁶ “Although a warrant application or affidavit cannot save a warrant from facial invalidity, it can support a finding of good faith, particularly where . . . the officer who prepared the application or affidavit also executed the search.”⁴⁷ The converse may also be true.

⁴² *United States v. Burgess*, 576 F.3d 1078, 1095 (10th Cir. 2009) (citing *United States v. Leon*, 468 U.S. 897 (1984)).

⁴³ *United States v. Danhauer*, 229 F.3d 1002, 1007 (10th Cir. 2000) (citation omitted).

⁴⁴ *United States v. Leary*, 846 F.2d 592, 607 (10th Cir. 1988) (internal quotation marks and citation omitted).

⁴⁵ *Burgess*, 576 F.3d at 1096 (internal quotation marks and citation omitted).

⁴⁶ *United States v. Russian*, 848 F.3d 1239, 1246 (10th Cir. 2017)

⁴⁷ *Id.*

In this case, the officer who executed the search warrant is the same one who prepared the affidavit for the search warrant. And the affidavit in support of the search warrant does not support a finding of good faith. In his affidavit to the court, the officer noted the facts for the warrant. When identifying the description of the items seized, he stated that the Facebook records had the “potential to provide identifying information for the account’s user, *identify investigative leads, and corroborate other information obtained during the investigation.*” In this case, the officer’s affidavit did not limit the search to Defendant’s user attribution information. Instead, the affidavit appeared to expand the officer’s search of Defendant’s belongings as he averred that the information from Facebook could identify investigative leads and corroborate other information obtained during the search. Although these words do not appear in the search warrant, the fact that they are included in the affidavit indicates the broad view that the officer took of the search warrant. There does not appear to be an objective reason that the officer should have believed that this general rummaging would be permitted. “A reasonably well-trained officer should know that a warrant must provide guidelines for determining what evidence may be seized.”⁴⁸ Thus, the Court finds the good faith exception inapplicable.

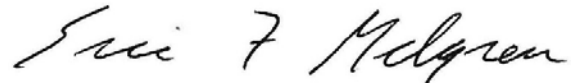
In sum, the Court finds that Defendant has standing to object to the search. Further, the first search warrant was overbroad and thus an invalid search warrant. In addition, the good faith doctrine does not save the execution of the first search warrant. Finally, because the first search warrant was invalid, the second search warrant was also invalid as the probable cause for the second warrant was based on the evidence obtained from the first search warrant.

⁴⁸ *Leary*, 846 F.2d at 609.

IT IS THEREFORE ORDERED that Defendant's Motion to Suppress (Doc. 18) is hereby **GRANTED**.

IT IS SO ORDERED.

Dated this 28th day of September, 2018.

A handwritten signature in black ink that reads "Eric F. Melgren". The signature is written in a cursive, flowing style.

ERIC F. MELGREN
UNITED STATES DISTRICT JUDGE