"THE FEDERAL CORNER"

Tim (The Magician) Henry Gets an Unbelievable Result In a Child Pornography Case – You Won't Believe It!

Buck Files

Jason Wayne Irving was a Kansas registered sex offender who had child pornography on his Facebook account. Kansas law enforcement officers, acting under the authority of search warrants issued by a Kansas state judge, discovered this pornography. Because of the exceptional work of Assistant Federal Defender Timothy J. Henry of the Federal Public Defenders Office for the District of Kansas, United States DistrictJudgeEric F. Melgren suppressed the evidence obtained during these two searches, holding that: (1) Irving had standing to object to the searches; (2) the first search warrant had been invalid as overbroad; and, (3) the good faith exception to the exclusion of evidence did not apply.*United States v. Irving*, ___F.Supp.3d____, 2018 WL 4681631 (D.Kan. September 28, 2018)

[Note: Although this case is more than three months old, it just came up in WestLaw's WTH-CJ database.]

[The Facts]

Officer Jordan Garrison of the Pittsburg, Kansas, Police Department became interested in Irving when he received information that Irving had been seen walking with a young juvenile at odd hours of the night. Garrison learned that Irving had a Facebook page with the user ID of jasson.irving. The profile picture on Irving's Facebook account looked like his registered sex offender pictures.

Garrison was aware that registered sex offenders were required under Kansas law to provide online identities used by the offenders. He found that Irving had not provided any such information as to the Facebook account. Garrison went to a Kansas state judge and requested and received a search warrant that permitted him to obtain from Facebook seven categories of evidence:

> (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.

When Garrison received the requested information from Facebook, he reviewed the records and observed that there were communications between Irving and suspected minors that involved nude photographs. Another officer, Le'MourRomine, reviewed the information obtained by Garrison and obtained a second warrant that permitted him to search Irving's home for child pornography. Romine found and seized this child pornography.

Irving was indicted on a four-count indictment. Two of the counts were dismissed, but counts alleging possession and distribution of child pornography remained.Irving's lawyer filed a motion to suppress all evidence obtained as a result of the two searches. He contended that the first warrant lacked particularity and was overbroad; further, because the first warrant was overbroad, all evidence from the two searches should be suppressed.

Judge Melgren's opinion reads, in part, as follows:

[An Overview]

> 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.

[The Reasonable Expectation of Privacy Approach]

> 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.' There is 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.' Next, there is the question of 'whether society is prepared to recognize that expectation as objectively reasonable.'

[The Government's Position]

> 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.
>
> * * *
>
> 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.
>
> * * *
>
> Next, the government argues that much of Defendant's Facebook account was public.
>
> * * *

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.

[The Court's Response]

Facebook…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. 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 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.

* * *

Facebook… 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.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.' 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.

* * *

[Facebook's Terms of Service]

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 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's Contention and the Court's Response]

* * *

.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…

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.'

* * *

…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. Accordingly, the Court finds that Defendant has standing because he had a reasonable expectation of privacy in his Facebook account.

[Warrants and the Fourth Amendment]

'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."' With regard to the particularity requirement, it 'prevents general searches and strictly limits the discretion of the officer executing the warrant.' '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.'

* * *

[The Warrant in this Case]

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. The warrant lists 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's Position]

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. In sum, the warrant encompassed everything in Defendant's Facebook account and there were no set limits.

[An Eleventh Circuit Case]

As noted by the Eleventh Circuit, Facebook searches can be limited to specific information. In *United States v. Blake*, 868 F.3d 960 (11th Cir. 2017), 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.' 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."'

[The First Warrant Was Overly Broad and General]

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.

* * *

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 Good Faith Doctrine]

'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*.'

[The Government's Burden]

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.' 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.' 'It is the government's burden to prove its agents' reliance upon the warrant was objectively reasonable.'

* * *

[The Affidavit Was Insufficient for a Finding of Good Faith]

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.

* * *

[The Good Faith Exception is Not Applicable]

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.' Thus, the Court finds the good faith exception inapplicable.

[Conclusion]

> 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.

[My Thoughts]

- Once again, we have great work by an assistant federal defender. When I talked with Mr. Henry, he was as laid back as a prevailing lawyer could ever be. You would have thought that his win in *Irving* was just a common occurrence – and maybe it was.
- We have all heard Racehorse Haynes say that he never had a win without some help from the other side. Mr. Henry explained that he was helped by Garrison's seeking information for further investigation when he applied for the first search warrant.
- If you had asked me whether a defendant could ever prevail on a reasonable expectation of privacy issue like the one that we see in *Irving*, I would have bet the farm against it.
- Congratulations to Mr. Henry!

Buck Files is a member of TDCLA's Hall of Fame and a former President of the State Bar of Texas. In May, 2016, TDCLA's Board of Directors named Buck as the *author transcendent* of the Texas Criminal Defense Lawyers Association. This is his 227th column or article. He practices in Tyler with the law firm of Bain, Files, Jarrett and Harrison, P.C., and can be reached at bfiles@bainfiles.com.