

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF KANSAS

UNITED STATES OF AMERICA,)	
)	
Plaintiff,)	CRIMINAL ACTION
)	
v.)	No. 11-10086-MLB
)	
JOHN D. ROACH,)	
)	
Defendant.)	
)	

MEMORANDUM AND ORDER

This case comes before the court on defendant's motion to suppress items seized pursuant to a search warrant. (Doc. 15). The motion has been fully briefed and is ripe for decision.¹ (Docs. 15, 19). Defendant's motion to suppress is denied for the reasons herein.

I. Facts²

On July 9, 2009, Special Agent James Kanatzar applied for a search warrant for 3012 SE Downing Drive in Topeka, Kansas. In his affidavit, Kanatzar described how law enforcement learned of and identified various websites advertising child pornography operated by CP Company, a pay-for-access commercial website that offers the sale of hardcore child pornography in a variety of formats. Kanatzar described the child pornography images that were visible at those

¹ The court gave defendant an opportunity for an evidentiary hearing but defendant declined, informing the court that he could rule on the motion based on the written submissions. (Doc. 20).

² The facts are largely taken from the government's response and the affidavit. (Doc. 19). Defendant does not dispute the facts in the affidavit but instead asserts that the affidavit was not sufficient to establish probable cause and that the information in the affidavit was stale.

advertising websites. The affidavit details how law enforcement collected both child pornography images and the associated point-of-contact email addresses from the CP Company's child pornography advertising websites. Kanatzar then described how law enforcement identified the names of certain individuals in Russia who were receiving payments for CP Company.

Agents then obtained corroboration from Russian officials who were also investigating CP Company. Some of that corroboration came from interviews of individuals who were acting as recipients of the Western Union transactions for CP Company as well as a website operator of CP Company. The Russian authorities also confirmed some of the identities of the payment recipients already identified by US investigators.

Kanatzar then provided examples of how CP company would orchestrate transactions through Western Union payments sent to Russia recipients. Agents contacted the individuals listed on the websites and sent payments through Western Union, attempting to purchase the child pornography. The agents, however, were not provided with the child pornography that they ordered.

The agents subsequently learned of the pricing structure for CP Company from the individuals serving as a point-of-contact for CP Company, such that the agents could identify "unique dollar amounts," i.e., \$130, \$190, \$350, \$490, for the child pornography products offered. Using the "unique dollar amounts" in combination with the specific identified Russian recipients, the agents were able to obtain a list of transactions from Western Union that met those combined parameters. Using this approach, the agents were able to obtain the

names, addresses, and credit card information of U.S. purchasers who had sent the "unique dollar amounts" to a CP Company recipient in Russia via Western Union. Defendant, and his residence at 3012 SE Downing Drive, were identified through this methodology. Defendant wired \$490.00 to Ilya Oboriyn in Perm, Russia.

Kanatzar acknowledged that a prior search of a home in a different investigation yielded no child pornography when the individual who submitted payment to a Russian payee sent an amount that was not unique.³ Using the refined methodology of only identifying unique payments, agents accurately identified nine other individuals who possessed child pornography.

In the affidavit, Kanatzar listed the information received from Western Union on March 18, 2009. That information included both a unique dollar amount previously identified and one of the previously identified Russian recipients for CP Company. The transaction information also identified the sending date as January 9, 2009, and included John Roach's name, phone number, address, and credit card number. Kanatzar corroborated that John Roach's address was actually 3012 SE Downing Drive by using Roach's KS driver's license, credit record checks, and U.S. Postal records. Kanatzar noted that John Roach was previously identified as a potential lead in an earlier 2006 child pornography investigation and that the credit card used in that earlier investigation was the same card as used in this case.

³ It was discovered that one of the CP Company's Russian wire recipients, Tatyana Brayer, was also involved in receiving Western Union transactions related to purported mail-order-bride type services. Brayer received money wires in the amounts of \$1500, \$600 and \$500 related to the search which did not uncover child pornography.

Finally, Kanatzar explained certain characteristics common to child pornographers, based upon his 20 years of experience. His affidavit states that child pornographers keep the materials secure, or in the privacy of their homes, and they typically maintain their collections for years.

Based upon these facts, United States Magistrate Judge Gary Sebelius determined probable cause existed for the search of 3012 SE Downing Drive in Topeka, Kansas, for "evidence of Western Union transactions, including images of child pornography" and other items pertaining to the purchase of child pornography. The search warrant was executed on July 10, 2009, and evidence of the Western Union transaction and images of child pornography were discovered.

Defendant moves to suppress the items seized pursuant to the search warrant on the basis that the agents failed to identify the IP address used in obtaining the child pornography and, additionally, that the information in the affidavit was stale.

II. Analysis

The Fourth Amendment to the United States Constitution provides that:

[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and 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.

U.S. Const. amend. IV. The validity of a warrant is not determined by "nit-picking" discreet portions of the application. Rather, the test is whether, under the totality of the circumstances presented in the affidavit, the issuing judge had a "substantial basis" for

determining that probable cause existed. Illinois v. Gates, 462 U.S. 213, 238-39 (1983); United States v. Harris, 369 F.3d 1157, 1165 (10th Cir. 2004) ("In determining whether a search warrant was supported by probable cause, we review "the sufficiency of the affidavit upon which a warrant [wa]s issued by looking at the totality of the circumstances and simply ensuring 'that the [issuing] magistrate had a substantial basis for concluding that probable cause existed.'" (internal citation omitted)).

Probable cause exists when "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." Harris, 369 F.3d at 1165 (quoting United States v. Hernandez-Rodriguez, 352 F.3d 1325, 1330 (10th Cir. 2003)). The Tenth Circuit has adopted the general rule that probable cause requires a "nexus between [the contraband to be seized] or suspected criminal activity and the place to be searched." United States v. Rowland, 145 F.3d 1194, 1203-04 (10th Cir. 1998)(quoting United States v. Corral-Corral, 899 F.2d 927, 937 (10th Cir. 1990)).

The Supreme Court has observed that "a magistrate's 'determination of probable cause should be paid great deference by reviewing courts.'" Gates, 462 U.S. at 236 (quoting Spinelli v. United States, 393 U.S. 410, 419 (1969)). In doing so, reviewing courts must apply the totality of the circumstances test:

The task of the issuing magistrate judge is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the veracity and basis of knowledge of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a

particular place. And the duty of a reviewing court is simply to ensure that the magistrate had a substantial basis for. . . conclud[ing] that probable cause existed.

Gates, 462 U.S. at 238-39 (internal citation omitted).

A. Probable Cause

Defendant argues that probable cause was lacking to support the search warrant because the affidavit does not verify that the IP address listed on the Western Union money order belonged to a computer located in defendant's home. Therefore, defendant asserts that the affidavit did not provide an adequate nexus between the crime and defendant's residence. Defendant cites United States v. Renigar, 613 F.3d 990 (10th Cir. 2010), to support his contention that an IP address, in connection with other evidence of child pornography downloads, is sufficient evidence to establish probable cause. Defendant thus concludes that an IP address identification is necessary for probable cause to justify a warrant search in an internet child pornography case. (Doc. 15 at 20-21). The Renigar opinion, however, does not support this conclusion.

In Renigar, agents determined that the defendant was downloading child pornography from a certain IP address. The agents discovered who the IP address was registered to. That information, however, did not detail the exact physical address of the computer but it did detail to whom the IP address is registered, at least, in some cases. The agents sought a search warrant at the residence of the individual listed as the name on the IP address. The defendant challenged the search warrant as not providing sufficient probable cause to conclude that the computer was located at his residence. The Tenth Circuit,

and other circuit courts, have determined that an IP address and evidence of file downloading, along with the agent's statement that individuals usually access child pornography from their home computers, is sufficient to establish probable cause. The Circuit did not express any opinion on the necessity of identifying the IP address.

In this case, while the agents had an IP address listed on the Western Union money order, they did not obtain the name of the owner of that IP address. This supposed failure, however, does not automatically lead to the conclusion that there was not a nexus between the alleged criminal activity and defendant's home. Rather, there was sufficient information in the affidavit to establish that there was probable cause to believe that a search would result in the seizure of child pornography. The agents in this case have been investigating the CP Company for an extended period of time. The CP Company has numerous websites -- all of which contain illegal material. The CP Company also employs numerous contacts which cash the Western Union money orders in return for a percentage of the money. These contacts have been identified by both United States and Russian government agents. Defendant sent a money order to one of the contacts who has been identified as a person who receives funds for CP Company. Furthermore, the agents established certain price points for the illegal products sold by CP Company and defendant's money order was in an amount that would provide him with 30-day access to videos on the CP Company's websites. The money order sent by defendant identified his name, address and credit card. The credit card used by defendant had also been previously flagged in an earlier

child pornography investigation. Finally, SA Kanatzar stated that individuals keep child pornography in their homes and they frequently access it on their home computers. The court finds that the magistrate judge had a "substantial basis" for determining that there was probable cause to search defendant's residence.⁴ See United States v. Fisk, 255 F. Supp.2d 694, 698 (E.D. Mich. 2003)(probable cause established when the defendant wired a certain dollar amount to an individual previously identified by the agents in a foreign country as the contact person for a web site offering child pornography).

2. Good Faith Exception

Even if the affidavit were legally insufficient, the court would uphold the search because the officers executing the search warrant acted with an objective good-faith belief that the warrant was properly issued by a neutral magistrate. See United States v. Leon, 468 U.S. 897 (1984).

The Supreme Court recognizes four situations in which an officer would not have reasonable grounds for believing a warrant was properly

⁴ Defendant alternatively appears to argue that the evidence was stale because there was a six-month delay from the point of purchase and the search. Defendant, however, concedes that the Tenth Circuit has "repeatedly endorsed" that possessors of child pornography hoard their materials. United States v. Perrine, 518 F.3d 1196 (10th Cir. 2008). Defendant further avers that the lapse of time in conjunction with a lack of knowledge that defendant received child pornography "does not support a finding of probable cause." (Doc. 15 at 25). Defendant does not cite any authority to support this position. As defendant has recognized, the Tenth Circuit would not conclude that the information was stale based on a six-month delay. Moreover, the evidence concerning the transaction, the websites, and the contact information in Russia was sufficient to support a finding that there was probable cause to believe that child pornography would be located at defendant's residence without requiring the agents to establish that defendant had received child pornography after the money order was cashed.

issued. In these situations, the good-faith exception to the exclusionary rule would not apply.

First, evidence should be suppressed if the issuing magistrate was misled by an affidavit containing false information or information that the affiant would have known was false if not for his "reckless disregard of the truth." Second, the exception does not apply when the "issuing magistrate wholly abandon[s her] judicial role." Third, the good-faith exception does not apply when the affidavit in support of the warrant is "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable." Fourth, the exception does not apply when a warrant is so facially deficient that the executing officer could not reasonably believe it was valid.

United States v. Danhauer, 229 F.3d 1002, 1007 (10th Cir. 2000) (citing throughout United States v. Leon, 468 U.S. 897 (1984)).

Defendant argues that reliance on the affidavit by officers in executing the search warrant was unreasonable, in violation of Leon. When reviewing the reasonableness of an officer's reliance upon a search warrant, a court "must examine the underlying documents to determine whether they are 'devoid of factual support.'" United States v. Danhauer, 229 F.3d 1002, 1006 (10th Cir. 2000) (quoting United States v. McKneely, 6 F.3d 1447, 1454 (10th Cir. 1993)).

The affidavit supporting the search warrant was not so lacking in indicia of probable cause that the executing officer should have known that the search may have been illegal despite the magistrate's authorization. See Leon, 468 U.S. at 922 n.23. Nor was the warrant so facially deficient that the executing officer could not believe it was valid. The executing officer could reasonably have believed that the evidence of submitted in the affidavit sufficiently linked criminal activity with defendant's residence. See United States v.

Nolan, 199 F.3d 1180, 1185 (10th Cir. 1999).

Defendant's motion to suppress is denied. (Doc. 15). The case is set for trial or other disposition on November 15, 2011. If the case is to be tried, the parties shall submit proposed voir dire questions and jury instructions no later than November 9, 2011.

IT IS SO ORDERED.

Dated this 18th day of October 2011, at Wichita, Kansas.

s/ Monti Belot

Monti L. Belot

UNITED STATES DISTRICT JUDGE