UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA,	)	
v.	)	**Criminal No. 09-30042-DJC**
ROBERT ROSENBECK,	)	
Defendant.	)	

MEMORANDUM AND ORDER

CASPER, J. June 24, 2011

I. Introduction

Defendant Robert Rosenbeck ("Rosenbeck") has been charged in a three-count indictment, filed on December 10, 2009, with receipt of child pornography in violation of 18 U.S.C. §§ 2552(a)(2) and (b)(1) (Count I) and two counts of possession of child pornography in violation of 18 U.S.C. § 2252(a)(4)(B) (Counts II and III). The first two counts arise out of the seizure of a computer and other materials seized during a search of Rosenbeck's residence executed pursuant to a search warrant on August 3, 2007. Rosenbeck claims that the evidence was seized in violation of the Fourth Amendment and has now moved to suppress that evidence on the grounds that: i) probable cause did not exist to support the issuance of the search warrant; and ii) the evidence relied upon in the affidavit supporting the application for the search warrant was stale. For the reasons set forth below, Rosenbeck's motion to suppress evidence obtained in the August 3, 2007 search of his residence is DENIED.

II. Standard of Review and Burden of Proof

Where a defendant challenges the legality of a search conducted pursuant to a search warrant, as Rosenbeck does here, the defendant bears the burden to show by a preponderance of the evidence that the search was unlawful. United States. v. Legault, 323 F. Supp. 2d 217, 220 (D. Mass. 2004); see United States v. Burdulis, No. 10-40003, 2011 WL 1898941, at *3 (D. Mass. May 19, 2011) (citing cases); see also United States v. Longmire, 761 F.2d 411, 417 (7th Cir. 1985) (noting that "[t]he general federal rule on who bears the burden of proof with respect to an allegedly illegal search or seizure is based upon the warrant-no warrant dichotomy: If the search or seizure was effected pursuant to a warrant, the defendant bears the burden of proving its illegality; if the police acted without a warrant, the prosecution bears the burden of establishing legality"). A reviewing court "must examine the affidavit in a practical, commonsense fashion" and "accord considerable deference to a magistrate's determination that information in a particular affidavit establishes probable cause." United States v. Feliz, 182 F.3d 82, 86 (1st Cir. 1999) (internal quotation marks and citation omitted); see Illinois v. Gates, 462 U.S. 213, 236 (1983). The Court will affirm the magistrate judge's determination as long as the magistrate "had a substantial basis for concluding that probable cause existed." New York v. P.J. Video. Inc., 475 U.S. 868, 876 (1986) (internal quotations and citations omitted); Feliz, 182 F.3d at 86.

III. Factual Background

The following facts are based upon the affidavit of Federal Bureau of Investigation ("FBI") Special Agent ("SA") Andrew Litowitz filed on July 30, 2007 in support of the application for a warrant to search Rosenbeck's residence.[1]

[1]References to the Affidavit of SA Litowitz are abbreviated as "(Aff. ¶_)."

A. FBI Investigation of Child Pornography Leads to Rosenbeck

At the time of the application for the search warrant, SA Litowitz had been a FBI agent for over three years and his duties included investigating individuals involved in the "on-line sexual exploitation of children" and suspected of violating the federal child pornography laws. (Aff. ¶¶ 1, 4). He had also participated in various training programs for the investigation and enforcement of federal child pornography laws. (Aff. ¶ 4). Based upon his training and experience and the experience of other agents investigating child exploitation matters, SA Litowitz noted, in relevant part, that collectors of child pornography often maintain hard copies of such pornographic materials (e.g., pictures, films, videotapes) and "often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area." (Aff. ¶ 5c, d). "These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the collector to view the collection, which is valued highly." (Aff. ¶ 5d). Collectors of child pornography use computers for production of such pornography, communication with others for obtaining, viewing and trading such images and distribution and storage of same. (Aff. ¶¶ 7-12).

A 2006 child pornography investigation originating with the San Francisco Division of the FBI led the agents to investigate Rosenbeck. (Aff. ¶¶ 18-22). On May 1, 2006, FBI SA Luders of San Francisco received an e-mail to an undercover e-mail account advertising a child pornography website. (Aff. ¶ 18). When the agent accessed the link in the e-mail, he was connected to a website containing multiple images of child pornography. (Aff. ¶ 18). SA Luders clicked on a link to join the website and provided undercover credit card information to do so. (Aff. ¶ 19). Shortly thereafter, he received an e-mail confirmation directing him to make a payment of $89.04 to a

PayPal account in the name of a merchant using an e-mail address at yahoo.co.uk. (Aff. ¶ 19). He made the payment as directed and, the following day, he received an e-mail containing a login and password for a website. (Aff. ¶¶ 19, 20). Logging into the website, he viewed multiple images and videos of child pornography. (Aff. ¶ 20). Paypal, pursuant to a May 5, 2006 administrative subpoena, provided account information and transaction information regarding this yahoo e-mail account including over 250 names and addresses of PayPal customers who paid this account approximately $89.00 since November 2005 to the FBI. (Aff. ¶ 21). One of the PayPal accounts that made such a payment to the e-mail address was in Rosenbeck's name and his Springfield address and was listed with his e-mail address. (Aff. ¶ 22). This account made a payment of $89.04, the same amount that the FBI agent had made in May 2006, to the e-mail address on April 29, 2006. (Aff. ¶ 22).

B. Examination of Rosenbeck's Computer Reveals Images of Child Pornography

SA Litowitz and another FBI agent interviewed Rosenbeck at his Springfield residence on January 3, 2007. (Aff. ¶ 23). At the time of the interview, he was living alone, but informed the agents that he had a roommate in the past. (Aff. ¶ 23). Rosenbeck confirmed that he had a computer at his residence. (Aff. ¶ 23). He claimed using the internet for very limited purchases, including but not limited to trial memberships to adult pornography websites, but he denied accessing child pornography sites. (Aff. ¶ 23).

Rosenbeck produced a Compaq Presario 6000 computer ("Computer 1") from his office and gave the agents oral and written consent to search it. (Aff. ¶ 23). A preliminary review, conducted on January 5, 2007, identified approximately 778 files on Computer 1 as potential child pornography. (Aff. ¶ 24). These files contained, but were not limited to, images of minors posing

in sexually explicit manners and engaged in sexually explicitly contact with adults and other minors. (Aff. ¶ 24). In April 2007, SA James Scripture, a FBI certified forensic examiner conducted a review of Computer 1 and recovered approximately 800 images of child pornography and approximately 60 child pornography videos. (Aff. ¶ 25). SA Scripture determined that Computer 1 had been last used on April 30, 2006. (Aff. ¶ 25). The images from these files from Computer 1 were compared to a database maintained at the National Center for Missing and Exploited Children ("NCMEC") and over 150 of the 778 files matched images in the database. (Aff. ¶ 26). A match to the NCMEC database "indicates that the child depicted in the image has been identified by a law enforcement agency and that the child was under the age of 18 when the sexually explicit was created." (Aff. ¶ 26).

The FBI interviewed Rosenbeck again at his residence on January 11, 2007 to inquire about the child pornography that was found as a result of the preliminary examination of Computer 1. (Aff. ¶ 27). Rosenbeck denied involvement in downloading child pornography to the computer and offered to have the agents review his bank statement from April 2006. (Aff. ¶ 27). He retrieved and gave the agents TD BankNorth bank statements from April 22 to May 21, 2006. (Aff. ¶ 27). They did not reflect any transactions in the amount of $89.00. (Aff. ¶ 27).

During a third interview at the FBI's office in Springfield on January 19, 2007, Rosenbeck again denied involvement with child pornography, stated that he only used his computer for limited purposes (including checking his e-mail account) and indicated that Computer 1 had not been working for several months and that he believed it had been inoperable since the summer 2006. (Aff. ¶ 28). He denied having a PayPal account or knowing anything about the child pornography website, but he indicated that he had memberships to various adult pornography websites and had

downloaded adult pornography to Computer 1 from those websites. (Aff. ¶ 29). During this interview, he provided the agents with more information about his former roommate, Dan Devillez. (Aff. ¶ 30). According to Rosenbeck, Devillez had moved in around 2004 and resided with him for approximately two years. (Aff. ¶ 30). He claimed that Devillez had used Computer 1 and he believed that he bought and sold items on e-Bay. (Aff. ¶ 30). Rosenbeck said that he had set up an E-GOLD account for Devillez at his request and had used his own credit card information for the account. (Aff. ¶ 30). Rosenbeck stated that his roommate gave him $200 on two occasions to cover the cost of his purchases through the E-GOLD account. (Aff. ¶ 30). He said that he did not know what purchases Devillez made and never noticed any unusual charges on his credit card statement that exceeded the $400 Devillez had given him. (Aff. ¶ 30).

C. ICE Investigation of Child Pornography Leads to Rosenbeck

On February 1, 2007, SA Francischelli of the Immigration and Customs Enforcement Agency ("ICE") informed SA Litowitz that Rosenbeck had been identified by his agency as the purchaser of child pornography in an ICE investigation. (Aff. ¶ 31). On March 14, 2006, a Visa credit card issued by Applied Card Bank, ending in 7204 ("7204 Visa card"), identified as Rosenbeck's, was used to purchase a subscription to a known child pornography website. (Aff. ¶¶ 31, 33). On May 7, 2006, another Visa credit card issued by Capital One, ending in 2688 ("2688 Visa card"), also identified as Rosenbeck's, was used to purchase a subscription to a known child pornography website. (Aff. ¶¶ 31, 32). The ICE agent obtained the preliminary credit card information through AdSoft, a credit card processing company. (Aff. ¶ 31).

Subpoenaed credit card statements for the 2688 Visa card later revealed, among other things, that Rosenbeck had made between three and twelve online purchases each month between June 2005

and December 2006. (Aff. ¶ 32a). They also revealed that a May 7, 2006 charge of $79.99 appeared in the name of AdSoft, consistent with the information provided by ICE, and Rosenbeck did not protest this charge to his account and a credit to the account in the amount of $500 was made to the account prior to the next statement generation. (Aff. ¶ 32b). In addition, many charges appeared to have been made to third party payment processors, including but not limited to PayPal. (Aff. ¶ 32c). Four charges of $79.00 each appeared on the credit card statements in the same merchant name that would appear for a website known to the FBI as a child pornography website. (Aff. ¶ 32e). It was not until January 14, 2007, between Rosenbeck's second and third FBI interviews, that he filed a fraudulent activity report with Capital One protesting two charges on his January 2007 statement despite the fact that a charge to at least one of these merchants had appeared on an earlier statement and he had not disputed it. (Aff. ¶ 32f, g).

Subpoenaed credit card statements for the 7204 Visa credit card revealed that Rosenbeck had made between one and twelve online purchases every month between June 2005 and December 2006. (Aff. ¶ 33a). There was a March 14, 2006 charge of $79.99 in the name of AdSoft, consistent with the information provided by ICE, and Rosenbeck also had not protested this charge to his account and a credit of $250 was made to the account prior to the next statement generation. (Aff. ¶ 33b). Many charges to third party payment processors, including but not limited to PayPal, also appeared on the statements for the 7204 Visa credit card. (Aff. ¶ 33c). A PayPal charge of $89.04 was posted to the account on April 30, 2006 and appeared on the statement which was consistent in the amount and merchant name with the undercover purchase the FBI agent had made to enter the child pornography site in the same time period. (Aff. ¶ 33e). This charge was also not disputed by Rosenbeck. (Aff. ¶ 33e). There were also four charges on these 7204 Visa card statements for

$79.00 each in the same merchant name that appeared on the 2688 Visa card and that was the merchant name that would appear for the website known to the FBI as a child pornography website. (Aff. ¶¶ 33f, 32e). On or about January 23, 2007, again after Rosenbeck had been interviewed by the FBI, Rosenbeck disputed thirteen charges on his most recent statement despite the fact that charges to some of these same entities had appeared on prior statements and he had not disputed them. (Aff. ¶ 33g).

PayPal subpoenaed records revealed that Rosenbeck had three PayPal accounts in his name and Springfield address and that these accounts were used to conduct seventeen transactions between April 29, 2006 and December 19, 2006 for a total amount of $1485.42. (Aff. ¶ 35). Moreover, when compared against Rosenbeck's work time sheets from his employer, Tedeschi Food Shops, none of these transactions occurred when Rosenbeck was working. (Aff. ¶¶ 34-35).

The ICE investigation also revealed that Rosenbeck's PayPal account was used to make eleven purchases from child pornography sites between September 2, 2006 and December 19, 2006. (Aff. ¶ 36). Nine of these purchases, those between October 22, 2006 and December 19, 2006, occurred from an IP address later identified by Comcast Cable as being subscribed to by Rosenbeck at his Springfield address. (Aff. ¶¶ 36-37). Comcast also confirmed that Rosenbeck terminated his high speed internet connection in January 2007 after he was interviewed by the FBI. (Aff. ¶ 37). The FBI later learned that Rosenbeck reconnected his Comcast high speed internet connection on June 6, 2007. (Aff. ¶ 44).

Subpoenaed records from another credit card processing service, CCBill.com, revealed that 121 transactions for the account subscribed to in Rosenbeck's name and address were for subscriptions to websites with sexually suggestive names and, based upon comparison with

Rosenbeck's work time sheets, none of these transactions occurred when Rosenbeck was working. (Aff. ¶ 38). The analysis conducted by the FBI's Cyber Division, in conjunction with NCMEC, indicated that the merchant names and e-mail addresses regarding Rosenbeck's purchases included names and addresses known to be used for access to subscription-based child pornography sites. (Aff. ¶ 39).

D. Agents Conduct Search of Rosenbeck's Residence Pursuant to Search Warrant

Based upon the information in his affidavit, SA Litowitz concluded that "one or more computers" other than Computer 1 given by Rosenbeck to the FBI on January 3, 2007 was located at Rosenbeck's Springfield residence. (Aff. ¶¶ 40-45). Accordingly, the search warrant sought, in relevant part, "[a]ll visual depictions, including still images videos, films or other recordings of child pornography or minors engaged in sexually explicit conduct. . .and any mechanism used for the receipt or storage of the same, including but not limited to: [a]ny computer, computer system and related peripherals . . . . " (Attachment A to Search Warrant). Magistrate Judge Neiman issued the search warrant on July 30, 2007. Law enforcement agents executed a search of the Rosenbeck residence, pursuant to the search warrant, on August 3, 2007. As a result of that search, the agents seized a Gateway GT 5432 computer ("Computer 2") that contained images of child pornography. (Opp. at 7-8).

IV. Discussion

A. Probable Cause for the Search Warrant

A "warrant application must demonstrate probable cause to believe that (1) a crime has been committed–the 'commission' element, and (2) enumerated evidence of the offense will be found at the place to be searched–the so-called 'nexus' element." United States v. Ribeiro, 397 F.3d 43, 48 (1st Cir. 2005) (citation omitted). Accordingly, in determining whether probable cause for the search

warrant exists, the court must assess whether there is "a fair probability" that evidence of the offense will be found in the place to be searched. Gates, 462 U.S. at 238. "'Probability is the touchstone' of this inquiry." United States v. Baldyga, 233 F.3d 674, 683 (1st Cir. 2000) (quoting United States v. Khounsavanh, 113 F.3d 279, 283 (1st Cir. 1997)).

Rosenbeck argues that there was no probable cause for the search warrant since the agent's affidavit failed to satisfy the commission element–i.e., possession or receipt of child pornography. (Def. Memo at pp. 3-4). Specifically, he argues that there was no determination made that the internet purchases from the purported child pornography websites "did not also transmit other forms of legal pornography or other products" and even if the purchases were of child pornography, Deveillez, Rosenbeck's roommate in 2006, could have made these purchases. Id. Rosenbeck further argues that even if the Court were to conclude that the agent's affidavit provided probable cause that a crime had been committed, it still failed to show a sufficient nexus–i.e., that evidence of the child pornography offenses would be found in Rosenbeck's residence. (Def. Memo at 4). In this regard, Rosenbeck argues that it is not "probable" to believe that Rosenbeck would retain evidence of his child pornography crimes at his residence in the wake of three FBI interviews and numerous acts–namely, canceling his internet service and challenging internet-related charges on his credit cards–that the government alleged to be acts of concealment. Id.

Based upon the facts and information in SA Litowitz's affidavit, there was probable cause to believe that there would be evidence of a crime at Rosenbeck's Springfield residence. First, Computer 1, the computer that Rosenbeck gave agents on January 3, 2007 and agreed to have searched, contained approximately 800 images of child pornography and approximately 60 videos of child pornography. This substantial collection of child pornography existed on Rosenbeck's computer, in his residence and he had retained it despite the fact that it was later determined that

Computer 1 had not been used since April 30, 2006. Moreover, Rosenbeck's e-mail address, IP address subscribed to at his residence, internet pay accounts and credit cards had been identified in investigations by the FBI and separately by ICE as purchasing access to subscription-based websites that offered images of child pornography. These internet purchases included purchases after April 30, 2006, the last date on which Computer 1 was used. Accordingly, it is a "fair inference" based upon the analysis of Computer 1 and the account and credit card information that, after April 30, 2006 when use of Computer 1 ceased, Rosenbeck was using another computer at his Springfield residence to access child pornography. See, e.g., United States v. Wilder, 526 F.3d 1, 6 (1st Cir. 2008) (concluding that it was a fair inference from the defendant's subscription to a child pornography website that "downloading and preservation in his home of images of child pornography might very well follow"). This seems particularly likely when Rosenbeck reconnected his high speed internet service in June 2007, five months after he had cancelled it (in the wake of his January 2007 interviews with the FBI).

It was also a fair inference, based on the evidence in the affidavit, that Rosenbeck retained child pornography at his Springfield residence. The nexus requirement is satisfied if a person of "reasonable caution [has] reason to believe that evidence of a crime will be found at the place to be searched." United States v. Rodrigue, 560 F.3d 29, 33 (1st Cir. 2009) (internal quotation marks and citation omitted). SA Litowitz asserted in the affidavit that child pornography collectors maintain their collections and secure them in private places to which they may have close access. The existence of abundant images of child pornography on Computer 1, which Rosenbeck produced to agents on January 3, 2007 and the frequency with which accounts and credit cards in his name and address were used to subscribe to child pornography websites indicate that Rosenbeck was a collector of child pornography and he was likely to retain such a collection in his home. Defense

counsel has suggested that it is not a fair inference that Rosenbeck would have retained child pornography at his residence in the wake of three interviews by the FBI and his awareness that he was a target of the agents' investigation. (Transcript of June 1, 2011 motion hearing at 6). Although the retention of such materials may not seem rational in light of the FBI investigation, it remains a fair inference that a collector of child pornography, who had invested time and money in assembling a collection, would retain it and keep it close at hand in his residence for all of the reasons articulated in SA Litowitz's affidavit.

Rosenbeck's argument that someone else, perhaps his roommate, Devillez, used his accounts and his computer, Computer 1, to obtain and retain child pornography, has not defeated a finding of probable cause in similar child pornography cases and does not do so here. For example, in United States v. Grant, 218 F.3d 72 (1st Cir. 2000), the defendant argued that the affidavit had failed to provide probable cause to search his residence for child pornography since someone else could have used his account to acquire child pornography. Id. at 75. The First Circuit rejected his argument concluding that "even discounting for the possibility that an individual other than [the defendant] may have been using his account, there was a *fair probability* that [the defendant] was the user and that evidence of the user's illegal activities would be found in [the defendant's] home." Id. (emphasis in original). Although there was some suggestion that Rosenbeck's roommate through sometime in 2006, not him, could have used Computer 1, there still was a fair probability that Rosenbeck was the user of that computer and other computers where access was made via the internet connection to his residence, via accounts in his name and address and paid for with his credit cards.

B. Staleness

Delay between the discovery of evidence and the issuance of a search warrant based upon

that evidence, in and of itself, does not render evidence relied upon in the affidavit stale. To address a staleness claim, the Court may not simply resort to "counting the number of days that have elapsed" between the discovery of the information and the issuance of the warrant. United States v. Morales-Aldahondo, 524 F.3d 115, 119 (1st Cir. 2008); see United States v. Ricciardelli, 998 F.2d 8, 12 n. 4 (1st Cir. 1993). "The court must also look at the nature of the information supporting the warrant, the nature and characteristics of the alleged crimes, and the likely endurance of the information." United States v. Ladeau, No. 09-40021, 2010 WL 1427523, *7 (D. Mass. April 7, 2010) (citing Morales-Aldahondo, 524 F.3d at 119).

"The Ricciardelli and Morales-Aldahondo cases establish that it is reasonable to infer that in cases involving child pornography collectors a significant amount of time may elapse before the evidence is considered stale." Ladeau, 2010 WL 1427523, *7 (rejecting argument that evidence relied upon in the search warrant was stale where child pornography had been downloaded from the defendant's computer in August 2008, eight months before the application for the search warrant of his residence). In Morales-Aldahondo, three years lapsed between the last downloads of child pornography and the search warrant application did not render the evidence stale and therefore, the defendant's motion to suppress was properly denied. 524 F.3d at 119. In Ricciardelli, 998 F.2d at 12 n. 4, the court suggested that exigent circumstances sufficient to justify a search without a search warrant "will rarely, if ever be present in child pornography cases, as history teaches that collectors prefer not to dispose of their dross, typically retaining obscene materials for years." As a general proposition, SA Litowitz noted that child pornography collectors retain their collections. (Aff. ¶ 5). That "customers of child pornography sites do not quickly dispose of their cache," in the words of the First Circuit, "is not a new revelation." Morales-Aldahondo, 524 F.3d at 119 (citing cases). Moreover, there was ample evidence in the affidavit to suggest that Rosenbeck was a collector of

child pornography. First, there were approximately 800 images and 60 videos of child pornography found on Computer 1. Despite the evidence that Computer 1 had not been operable since the end of April 2006, Rosenbeck had retained it, with its abundant child pornography, and still had it in his possession, approximately eight months later in January 2007 when he was first interviewed by the FBI. Moreover, the frequency of his subscriptions to child pornography websites also suggests that he was likely to retain child pornography in his residence. See, e.g., Ladeau, 2010 WL 1427523 at *8.

Under these circumstances, the passage of time from May 2006 when Rosenbeck was first identified as a purveyor of child pornography to July 30, 2007 when the agents sought the search warrant for his residence, does not render the evidence upon which SA Litowitz relied in his affidavit stale. This is particularly true given that the investigation of Rosenbeck did not end with the FBI investigation in May 2006, but continued with the ICE investigation in February 2007 and continued at least into June 2007 when the FBI learned that Rosenbeck, despite having turned over Computer 1 to the agency in January 2007, had the high-speed internet connection reconnected at his residence. Given these facts and circumstances, it cannot be said that the evidence upon which SA Litowitz relied in his affidavit in support of the search warrant was stale.

V. Conclusion

For the foregoing reasons, Rosenbeck's motion to suppress evidence is DENIED.

So ordered.

/s/ Denise J. Casper
United States District Judge