Filed 10/24/13 P. v. Kuhn CA2/3

NOT TO BE PUBLISHED IN THE OFFICIAL REPORTS

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA

SECOND APPELLATE DISTRICT

DIVISION THREE

THE PEOPLE, Plaintiff and Respondent, v. MICHAEL ERIC KUHN, Defendant and Appellant.	B243792 (Los Angeles County Super. Ct. No. BA385064)

APPEAL from a judgment of the Superior Court of Los Angeles County, Patricia M. Schnegg, Judge. Affirmed.

Law Offices of Joseph Shemaria and Joseph Shemaria for Defendant and Appellant.

Kamala D. Harris, Attorney General, Dane R. Gillette, Chief Assistant Attorney General, Lance E. Winters, Assistant Attorney General, Scott A. Taryle and Stacy S. Schwartz, Deputy Attorneys General, for Plaintiff and Respondent.

Defendant and appellant Michael Eric Kuhn appeals from the judgment entered following his no contest plea to possession of child pornography, entered after the trial court denied his motion to quash and traverse a search warrant and suppress evidence. Kuhn contends the trial court erred by denying his motion. We affirm.

FACTUAL AND PROCEDURAL BACKGROUND

1. *Facts.*

a. *Issuance of search warrant for Kuhn's apartment.*

On August 31, 2010, Los Angeles Police Department (L.A.P.D.) Officer Eric Good sought and obtained a warrant to search Kuhn's Culver City apartment, vehicle, computer systems, and electronic equipment for child pornography and related materials. As pertinent here, the 19-page affidavit in support of the warrant stated the following.

Officer Good had been employed by the City of Los Angeles since 2002, began working for the L.A.P.D.'s Juvenile Division in December 2008, and, when the affidavit was prepared, was assigned to the Juvenile Division's Internet Crimes Against Children Unit (ICACU). One of the ICACU's tasks was investigation of "child sexual predators who use computers and the Internet to pursue their sexual interest in children." The affidavit described Good's formal training and experience in the investigation of child abuse and exploitation, which included over 120 hours of training on crimes related to sexual exploitation of children on the Internet.

Officer Good provided background information about users of child pornography. His affidavit stated: "I am aware that the following characteristics are generally found in varying combinations in people who produce, trade, distribute or possess images of child pornography: These people view children as sexual objects. They receive gratification from sexually explicit images of minors. They collect sexually explicit images of minors, which they use for their own sexual gratification and fantasy. They use these images as a means of reliving fantasies or actual sexual encounters. They rarely, if ever, dispose of sexually explicit images of minors because the images are treated as prized possessions. [¶] They store such images in many different formats including photographs, printouts, magazines, videotapes, and many other forms of digital media such as hard drives,

diskettes, CDs and/or DVDs and other storing devices," and store them "in many different locations such as their home, their vehicle, their work areas, and other areas under their control." Collectors of child pornography generally prefer to store images in electronic format as computer files. Officer Good had "personally witnessed collectors going to great lengths to protect their collection from discovery."

Such persons maintain images of minors with whom they had sexual contact; use the Internet to gain access to children for the purposes of sexual exploitation; and chat online with other suspects to share information on the sexual exploitation of children. Predators "will often exchange or purchase child pornography on the Internet or will entice children to meet with them for sexual purposes."

The affidavit described, in considerable detail, the technical process whereby investigators are able to identify persons who possess child pornography. Briefly summarized, that information included the following. The "Secure Hash Algorithm Version 1," or "SHA1," is a mathematical encryption method used to produce a unique digital signature of a computer file. No two files produce the same SHA1 value unless their contents are identical. Various government and private agencies cooperate to maintain a list of "verified positive child pornography SHA1 values." Thus, the contents of computer files can be positively established without viewing the content, "once a known file with a certain SHA1 value has been identified."

Persons with an interest in child pornography frequently use peer-to-peer networks to trade and share such files. One such network is Gnutella, an "open-source," publicly available network. Gnutella uses SHA1 values in its operation.

On July 26, 2009, Detective Schlund identified a computer with the Internet Protocol, or IP, address of 76.171.169.96 as distributing images of child pornography via file sharing. Schlund observed that the computer was sharing a folder with 20 video files, all of which had titles that were indicative of child pornography. Schlund was unable to download files at that time due to a slow Internet connection. On July 28, 2009, by comparing the contents of the shared file with the library of known child pornography,

Schlund confirmed that at least one of the files in the shared folder depicted minors engaged in sexually explicit conduct, as defined by Penal Code section 311.

Also on July 28, 2010, Schlund determined the Internet Service Provider for the computer was Time Warner Roadrunner. Schlund prepared a federal customs subpoena to obtain subscriber information.

On September 8, 2009, Time Warner notified Schlund that Michael Kuhn, residing at an apartment located at 7777 West 91st Street in Playa Del Rey, was the subscriber assigned to the IP address of 76.171.169.96.

On March 9, 2010, Officer Good matched the SHA1 signatures of known child pornography files with the files identified in the shared folder and confirmed that at least one of the files appeared to depict minors engaged in sexually explicit conduct. The file in question was a video entitled " '14 kids teens women (porno-lolitas-preteens-reelkiddymov-r@ygold-hussyfans-underage-girls-children-pedofilia-pthc-ptsc-xxx-sexy).avi' " (hereinafter "14 kids"). (Bold in original omitted.) It was approximately 30 minutes long and showed a montage of young girls between the ages of 3 to 11 years, orally copulating and "being vaginally penetrated by unknown adult male penises."

On May 4, 2010, an investigator checked to see if there was any further activity on IP address 76.171.169.96. By comparing SHA1 values, the investigator learned that the IP address "76.171.169.96 was identified 3 times on January 7, 2010, as flagged for having SHA1 values of known child pornography."

On July 22, 2010, Officer Good learned from a homeowners' association representative at the Playa Del Rey apartment complex that Kuhn was not living at the apartment.

On August 24, 2010, Good contacted Postal Inspector Harjala and asked if any change of address records existed for Kuhn. Harjala advised that Kuhn had filed a form on March 16, 2010, changing his address from the West 91st Street apartment to an apartment on Culver Boulevard, in Culver City. Harjala stated that Kuhn had not subsequently filed any additional change of address forms. Additionally, Harjala advised that three other persons—Felipe Serrano, Jeffrey Pederson, and Douglas Nicholas—had

also filed changes of address forms from the same Playa Del Rey apartment to the Culver Boulevard apartment.

Based upon the foregoing, Officer Good opined that probable cause existed to show the crime of possession of child pornography in violation of Penal Code section 311.11, subdivision (a), had been committed by a person residing at the Culver Boulevard address. Good then set forth, in considerable detail, information regarding the special circumstances related to searches of digital devices, explaining why they generally must be seized and examined by experts in a police laboratory, rather than at the scene of the search. Good also explained that "[e]lectronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet."

b. *Search of Kuhn's Culver City Apartment and discovery of child pornography.*

On September 1, 2010, Officer Good, along with other officers, executed the search warrant at Kuhn's apartment in Culver City. Good seized two laptop computers, five hard drives, batteries and adaptors, memory cards, compact discs, a camera, a Time Warner bill, and a receipt, all found in Kuhn's bedroom. A forensic examination of those items disclosed images of child pornography on one or more of the seized devices. When Good executed the search, he conducted a recorded interview of Kuhn. Kuhn admitted to Good that he had downloaded child pornography.[1] Kuhn was arrested and charged with violating Penal Code section 311.11, subdivision (a)[2] (possession of matter depicting a minor engaged in sexual conduct).

c. *Motion to quash and traverse the warrant and suppress evidence.*

Kuhn thereafter filed a motion pursuant to section 1538.5 to quash and traverse the search warrant and suppress the seized evidence and his statements. He alleged, inter alia, that the warrant affidavit was insufficient to establish probable cause because: (1) it

---

[1] Because Kuhn pleaded no contest before trial, we glean these facts from the transcript of the preliminary hearing.

[2] All further undesignated statutory references are to the Penal Code.

was based upon stale information and the "images in question were located at a different residence"; (2) the warrant affidavit contained intentionally misleading and/or false statements; (3) the warrant was a "prohibited general warrant" in that it was overbroad; and (4) the warrant was obtained without a good faith belief the affidavit provided sufficient probable cause to justify the search.

On April 20, 2012, the trial court heard and denied Kuhn's motion. The court credited Officer Good's opinion that persons who possess child pornography rarely delete such files. It therefore rejected the argument that the information was too stale to establish probable cause, observing that child pornography was detected on Kuhn's computer initially in July 2009 and again in January 2010. The court discounted Kuhn's argument that the term "collector," as used by Good in the warrant affidavit, was misleading, explaining the defense contention was "a linguistic argument that I do not find persuasive. [¶] . . . [¶] People who collect illegal material, I think it is reasonable to infer that they are going to be disinclined to delete such material and therefore there was nothing misleading provided to the issuing magistrate in that regard." Furthermore, one week before issuance of the warrant, Good learned from Harjala that Kuhn had filed a change of address form. The court reasoned: "So this is a situation where law enforcement is not simply relying on information learned months before they enter the property in question but, in fact, take a very significant step to try and make sure that Mr. Kuhn has not moved to any new location and that investigation was done one week prior to the search." The court expressed the view that people do not normally distance themselves from their personal computers, which are both highly portable and valuable. Common sense dictated that a computer owner would take his computer to his new residence. The court also rejected the argument that the warrant was overbroad: given the fact child pornography was discovered in July and again in January, "the investigation would suggest that there is a sufficient scope or breadth of material that needs to allow the investigating officer some degree of latitude to make sure that they're not missing something. To suggest that they can only look for one particular title strikes this court as simply absurd."

2. *Procedure.*

After the trial court denied his suppression motion, Kuhn pleaded no contest to possession of child pornography (§ 311.11, subd. (a)). The court placed Kuhn on probation for three years, on the condition he serve two days in jail, with credit for two days served. It ordered that Kuhn register as a sex offender, and imposed a restitution fine, a suspended probation revocation restitution fine, a criminal conviction assessment, a court operations assessment, and a sex offender fine. Kuhn appeals.

DISCUSSION

Kuhn contends the trial court erred by denying his motions to quash and traverse the warrant and suppress evidence seized in the search, as well as his statements. He argues the affidavit in support of the search warrant failed to state facts sufficient to establish probable cause because it was based on stale information and contained unsupported conclusions and recklessly misleading misstatements; and the warrant was an overbroad "general warrant." We disagree.

1. *Applicable legal principles.*

A search warrant may only be issued upon a showing of probable cause. (U.S. Const., 4th Amend.; § 1525.) Probable cause exists where there is a fair probability that contraband or evidence of a crime will be found in a particular place, at the time of the search. (*Illinois v. Gates* (1983) 462 U.S. 213, 238; *People v. Carrington* (2009) 47 Cal.4th 145, 161; *People v. Kraft* (2000) 23 Cal.4th 978, 1040-1041; *People v. Gibson* (2001) 90 Cal.App.4th 371, 380.) The probable cause showing must appear in the affidavit offered in support of the warrant. (*Carrington*, at p. 161.) " '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 before him [or her], 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.' " (*Ibid.*; *Illinois v. Gates*, *supra*, at p. 238; *People v. Scott* (2011) 52 Cal.4th 452, 483.) Probable cause may be shown by evidence that would not be competent at trial,

and a magistrate may reasonably rely on the special experience and expertise of the affiant officer. (*People v. Varghese* (2008) 162 Cal.App.4th 1084, 1103.)

On review, we defer to the trial court's express and implied factual findings if supported by substantial evidence, but independently determine the legality of the search under the Fourth Amendment. (*People v. Eubanks* (2011) 53 Cal.4th 110, 133; *People v. Lenart* (2004) 32 Cal.4th 1107, 1119; *People v. Hirata* (2009) 175 Cal.App.4th 1499, 1504.) "Because courts accord a preference to searches and seizures conducted pursuant to a search warrant, 'in a doubtful or marginal case a search under a warrant may be sustainable where without one it would fall.' " (*Eubanks*, at p. 133.) Any challenge to the admissibility of a search or seizure must be evaluated solely under the Fourth Amendment. (*People v. Carter* (2005) 36 Cal.4th 1114, 1141; *People v. Stipo* (2011) 195 Cal.App.4th 664, 668.)

2. *The search warrant affidavit supported the probable cause finding.*

a. *Purportedly stale information.*

Kuhn contends the information in the affidavit did not supply probable cause because (1) there was a lengthy delay between the date investigators first identified files containing child pornography on his computer and sought issuance of the warrant; and (2) he moved during that period, but Officer Good failed to take sufficient steps to determine that he was living at the Culver City address and had taken the computer with him. These contentions lack merit.

To justify issuance of a warrant, "[t]here must be probable cause to believe that the material sought to be seized will be on the premises to be searched when the warrant is served." (*People v. Gibson, supra,* 90 Cal.App.4th at p. 380; *People v. Hirata, supra,* 175 Cal.App.4th at p. 1504.) Information in a warrant affidavit that is remote in time, or "stale," does not establish present probable cause for a search. (*People v. Jones* (2013) 217 Cal.App.4th 735, 741-742; *People v. Hulland* (2003) 110 Cal.App.4th 1646, 1652; *Gibson*, at p. 380.) There is no bright line rule indicating when information becomes stale. (*People v. Carrington*, *supra*, 47 Cal.4th at p. 163; *Jones*, at pp. 741-742; *Hirata*, at p. 1504.) However, delays of more than four weeks are generally considered

insufficient to demonstrate present probable cause. (*Jones*, at pp. 741-742; *Hirata*, at p. 1504.) Longer delays are nonetheless justified where there is evidence of an activity continuing over a long period of time, or the nature of the activity is such as to justify the inference that it will continue until the time of the search. (*Carrington*, at p. 164, and cases cited therein; *Jones*, at p. 742; *People v. Stipo*, *supra*, 195 Cal.App.4th at p. 672; *Hulland*, at p. 1652.) The question of staleness turns on the facts of each particular case. (*Carrington*, at p. 163; *Gibson*, at p. 380; *Jones*, at p. 741.)

"In the context of child pornography cases, courts have largely concluded that a delay—even a substantial delay—between distribution and the issuance of a search warrant does not render the underlying information stale." (*U.S. v. Richardson* (4th Cir. 2010) 607 F.3d 357, 370 [2010 U.S. App. LEXIS 11928]; see, e.g., *U.S. v. Lacy* (9th Cir. 1997) 119 F.3d 742, 745-746 [affidavit provided non-stale information despite 10-month lapse between computer download and issuance of the warrant]; *U.S. v. Morales-Aldahondo* (1st Cir. 2008) 524 F.3d 115, 119 [three-year delay between acquisition of child pornography and application for warrant did not render supporting information stale]; *U.S. v. Irving* (2d Cir. 2006) 452 F.3d 110, 125 ["When a defendant is suspected of possessing child pornography, the staleness determination is unique because it is well known that 'images of child pornography are likely to be hoarded by persons interested in those materials in the privacy of their homes' "]; *U.S. v. Allen* (5th Cir. 2010) 625 F.3d 830, 842 [2010 U.S. App. LEXIS 22920] [18-month-old information was not stale]; *U.S. v. Newsom* (7th Cir. 2005) 402 F.3d 780, 783 [one year not stale]; *U.S. v. Lemon* (8th Cir. 2010) 590 F.3d 612, 614-615 [18-month-old information was not stale].) Computers and computer equipment are "not the type of evidence that rapidly dissipates or degrades." (*U.S. v. Vosburgh* (3d Cir. 2010) 602 F.3d 512, 529 [2010 U.S. App. LEXIS 8140] (*Vosburgh*).) Therefore, "the passage of weeks or months here is less important than it might be in a case involving more fungible or ephemeral evidence, such as small quantities of drugs or stolen music." (*Vosburgh*, at p. 529.) "[I]nformation concerning [child pornography] crimes has a relatively long shelf life. It has not been, and should not be, quickly deemed stale." (*Ibid.*)

Here, investigators determined that Kuhn's computer contained child pornography files on July 26, 2009, and again on January 7, 2010. Officer Good sought issuance of the search warrant on August 31, 2010. Thus, there was a seven-and-a-half month delay between the last identification of contraband files on Kuhn's computer and issuance of the warrant. On the facts of this case, the delay did not render the information stale for several reasons. First, from the information in the affidavit, the magistrate could reasonably believe Kuhn continued downloading child pornography several months after the initial download in July. From this, it was reasonable to infer Kuhn's interest in Internet child pornography, and his downloading activity, was ongoing.

Second, Officer Good—who had considerable experience in the investigation of child pornography—averred that persons who possess child pornography "rarely, if ever, dispose of sexually explicit images of minors because the images are treated as prized possessions." Law enforcement officers may draw upon their expertise to interpret the facts in a search warrant application, and such expertise may be considered by the magistrate as a factor supporting probable cause. (*People v. Nicholls* (2008) 159 Cal.App.4th 703, 711.) Here, Good had the necessary experience and training to describe the predilections and proclivities of persons who download child pornography. Good's statement, which was credited by the trial court, demonstrated the likelihood that the pornographic files likely remained on Kuhn's computer or other electronic media at the time the warrant was issued. (See, e.g., *U.S. v. Lacy, supra,* 119 F.3d at pp. 745-746 [upholding warrant based on information that defendant downloaded child pornography 10 months earlier, and on affiant's assertion that collectors of child pornography generally retain the images]; *U.S. v. Gourde* (9th Cir. 2006) 440 F.3d 1065, 1072, and cases cited therein; *United States v. Murray* (D.Az. 2010) 696 F.Supp.2d 1044, 1049 [2010 U.S. Dist. LEXIS 26696] (*Murray*); cf. *People v. Stipo, supra,* 195 Cal.App.4th at p. 672 [in computer hacking case, staleness argument rejected where the hacked information could be used for identity theft, was therefore valuable, and would likely have been retained by defendant]; *People v. Jones, supra,* 217 Cal.App.4th at p. 742.)

"Substantial delays do not render warrants stale where the defendant is not likely to dispose of the items police seek to seize." (*Stipo*, at p. 672.)

Third, Good averred that electronic files or remnants of such files could be recovered months or even years after their original download using "readily-available forensics tools," even if the user had deleted the files. This fact suggested the pornographic files would be found on the computer regardless of the delay. (See *Murray, supra,* 696 F.Supp.2d at p. 1049 ["Thanks to the long memory of computers, any evidence of [child pornography] was almost certainly still on [defendant's] computer, even if he had tried to delete the images"]; *U.S. v. Gourde, supra,* 440 F.3d at p. 1071; *Vosburgh, supra,* 602 F.3d at p. 529; *People v. Stipo, supra,* 195 Cal.App.4th at p. 673 [staleness argument rejected where traces of network intrusion likely remained on the defendant's computer because they were automatically entered and difficult to remove].)

Kuhn's arguments that Officer Good failed to reliably determine he and his computer had actually moved to the Culver City address fare no better. The affidavit stated that on July 22, 2010, Good learned from a homeowner's association representative at the Playa Del Ray apartments that there was no record of Kuhn living in the apartment. On August 24—just a week before seeking the warrant—Good spoke to Postal Inspector Harjala and learned that Kuhn had filed a form on March 16, 2010, changing his address from West 91st Street in Playa Del Rey to the Culver Boulevard apartment. Inspector Harjala told Good that Kuhn had not subsequently filed a change of address form. The most logical and reasonable inference from this information was that Kuhn moved from the Playa Del Rey apartment to the Culver City apartment in March 2010. The absence of a subsequent change of address form made it reasonably probable that Kuhn was still living at the Culver City address when the warrant was sought. It was a reasonable inference that, having once filed a change of address when moving to a new residence, Kuhn would have done so again had he moved from the Culver City location. (See generally *People v. Gibson, supra,* 90 Cal.App.4th at pp. 380-381 [where there was no reason to believe appellant had moved in the five to six months preceding issuance of

the warrant, affidavit was not defective for failure to provide information she was still living there when the warrant was sought].)[3]

It was eminently reasonable for the trial court to believe Kuhn took his computer with him when he moved. Computers are highly portable and usually quite valuable. Common sense and common experience teach that, in today's society, computers are an oft-used and indispensible tool, and are generally used to store personal and financial data. They are not the type of item likely to be discarded or left behind when the owner moves. Kuhn's move from Playa Del Rey to Culver City was not a transatlantic or cross-country move, making it even less likely he would have neglected to take the computer with him. (See *People v. Miller* (1978) 85 Cal.App.3d 194, 200 [affidavits must be interpreted in a common sense fashion rather than a hypertechnical one; "[r]easonable and logical inferences may be drawn and the magistrate may consider matters of common knowledge concerning human behavior"]; *Vosburgh, supra,* 602 F.3d at p. 529 [computers and computer equipment are not the type of property "that is usually[,] quickly or continuously discarded"]; *People v. Stipo, supra,* 195 Cal.App.4th at p. 672 [because defendant was unaware he was a suspect, he was unlikely to dispose of his computer equipment during the six months between the crime and issuance of the warrant]; *People v. Ulloa* (2002) 101 Cal.App.4th 1000, 1007 [it was reasonable to assume defendant's computer would be located at his home].)

Kuhn argues Officer Good could have taken additional steps to verify he was living at the Culver City address, still owned the computer, and had the computer with him, such as conducting surveillance or checking utility, rent, Internet provider, and

---

[3] *U.S. v. Rowland* (10th Cir. 1998) 145 F.3d 1194, 1205, cited by Kuhn, is factually distinguishable. That case involved an "anticipatory warrant" (that is, a warrant contingent on the occurrence of an anticipated future event), where government agents mailed child pornography to the defendant's post office box as part of a sting operation. Because the delivery was made to the post office box, rather than the house to be searched, and the affidavit failed to establish a nexus between the contraband or criminal activity and the house, the warrant was invalid. (*Id.* at p. 1206.) The instant case does not involve similar facts.

Department of Motor Vehicles records. He also complains that Good failed to establish the computer was not accessed by other persons, or via an unsecured Internet connection. Such further investigation and information might have bolstered the probable cause showing, but was not required to establish it. " '[T]he term "probable cause" . . . means less than evidence which would justify condemnation.' " (*United States v. Ventresca* (1965) 380 U.S. 102, 107.) Kuhn's arguments attempt to "sidestep the 'fair probability' standard and elevate probable cause to a test of near certainty," in contravention of the teachings of the Supreme Court. (*U.S. v. Gourde, supra,* 440 F.3d at p. 1072; *Illinois v. Gates, supra,* 462 U.S. at p. 235.) Kuhn's citation to cases in which a more extensive investigation was completed and additional evidence was presented in support of a warrant is unavailing. Each case must be considered on its own facts (*People v. Carrington, supra,* 47 Cal.4th at p. 163), and the circumstance that more, or stronger, evidence was present in another case does not demonstrate the probable cause showing was insufficient here.

b. *The warrant affidavit was not based upon unsupported conclusions.*

Kuhn next contends the warrant affidavit failed to establish probable cause because it was based on unsupported conclusions. We disagree.

An affidavit based on mere suspicion or belief, or stating a mere conclusion without supporting facts, is insufficient to establish probable cause. (*Illinois v. Gates, supra,* 462 U.S. at p. 239; *People v. Garcia* (2003) 111 Cal.App.4th 715, 721.)

Kuhn first attacks the portion of the affidavit in which Officer Good described the typical characteristics of persons who possess child pornography. Kuhn points to Good's statements that: (1) certain characteristics were "generally found in varying combinations in people who produce, trade, distribute or possess images of child pornography"; (2) such persons "rarely, if ever, dispose of sexually explicit images of minors because the images are treated as prized possessions"; (3) "collectors of child pornography generally prefer to store images in electronic format as computer files"; and (4) collectors will go to great lengths to protect their pornography from discovery. According to Kuhn, Good failed to provide facts to support these statements, explain

"what he mean[t] by a 'collector' of child pornography," or state facts showing Kuhn met the definition of a collector.

These contentions are meritless. As noted, the opinions of an experienced officer may be considered in the probable cause determination. (*People v. Nicholls, supra,* 159 Cal.App.4th at p. 711; *People v. Garcia, supra,* 111 Cal.App.4th at p. 721; *People v. Deutsch* (1996) 44 Cal.App.4th 1224, 1232.) The affidavit here detailed Good's training in the area of investigating child pornography crimes, which included, in addition to training at the police academy and through Peace Officer Standards and Training courses, over 120 hours of training on Internet crimes involving children.[4] He had personally examined digital videos, videotapes, and computer files depicting child pornography during the course of his work. It is not a stretch to believe Good's training and experience encompassed the challenged aspects of the affidavit.

Good provided an explanation of why possessors of child pornography prefer to store it on computers as electronic files: "The computer's ability to store images in digital format makes a computer an ideal repository for child pornography. Portable disks can contain thousands . . . of child pornography images. The portable digital media are particularly well suited to conceal images of child pornography." The statement that collectors attempt to conceal pornography was based on Good's personal experience; as he explained in the affidavit, "I have personally witnessed collectors going to great lengths to protect their collection from discovery." Thus, none of these statements lacked a sufficient factual foundation.

Nor are we persuaded by Kuhn's argument that Good failed to adequately define "collector." The term, as used in the affidavit, is readily understandable by reference to

---

[4] Good had attended a 36-hour Internet Crimes Against Children Investigative Techniques course through the Office of Juvenile Justice and Delinquency Prevention; a 36-hour Internet Crimes Against Children Undercover Chat Class taught by experts in the field, which included instruction on the preservation of digital evidence; 20 hours of training by experts at the 2009 Silicon Valley Internet Crimes Against Children Conference; and 36 hours of training at the 2010 Internet Crimes Against Children National Conference, where experts instructed regarding the investigation of crimes related to the sexual exploitation of children on the Internet.

its plain meaning, that is, a person who downloads or otherwise obtains, and keeps, child pornography. There was a factual basis for a conclusion Kuhn was a collector who would retain his child pornography. The affidavit stated that on July 26, 2006, an IP address later connected to Kuhn was sharing 20 files with titles indicating child pornography. On January 7, 2010, Kuhn's IP address was "identified 3 times" as "flagged for having SHA1 values of known child pornography." A person who has over 20 child pornography files can reasonably be considered a collector.

Kuhn also complains that Officer Good failed to describe the contents of the SHA1 files identified on January 7, 2010. From this he reasons that there was insufficient information the January 7 files "really [did] involve child pornography." Not so. Good explained at length that a SHA1 value is essentially a digital signature, and no two files will have the same SHA1 value unless they are identical. By matching SHA1 values with files already identified as containing child pornography, an investigator could reliably determine that a file contained such material, without actually viewing its contents. The affidavit stated that a detective "discovered that IP address 76.171.169.96 was identified 3 times on January 7, 2010, as flagged for having SHA1 values of known child pornography." Because the files, identified by their unique digital signatures, had already been determined to contain child pornography, Good did not need to further describe the files' contents in order for the trial court to reasonably conclude they involved child pornography.

Kuhn next avers that Good's statement that possessors of child pornography always keep it is an impermissible " 'profile' allegation that does not provide probable cause." In support, he cites *Richards v. Wisconsin* (1997) 520 U.S. 385, 394. In *Richards,* the United States Supreme Court held that the Fourth Amendment does not permit a blanket exception to the knock-and-announce requirement in felony drug investigations. (*Id.* at pp. 387-388.) Although felony drug investigations frequently involve both danger to police officers and the likelihood evidence will be destroyed if advance notice is given, this did not justify dispensing with a case-by-case evaluation of the manner in which a search is executed. (*Id.* at pp. 391, 394.) Kuhn attempts to

analogize *Richards* and similar cases (e.g., *U.S. v. Granville* (9th Cir. 2000) 222 F.3d 1214, 1219; *People v. Gastelo* (1967) 67 Cal.2d 586, 588), arguing that "there is no such thing as 'profile probable cause' to allow the search of the residence for items of a crime without individual specific information that evidence of a crime would be at that location at that time."

But this case does not involve a proposed blanket exception to the knock-and-announce rule; Good's statements about the proclivities of possessors of child pornography were not used to justify a per se exception to Fourth Amendment requirements. The warrant affidavit here *did* contain specific information regarding Kuhn that provided probable cause for the search. Indeed, numerous federal courts have found similar statements by affiant officers supported a probable cause finding. (See, e.g., *U.S. v. Lacy*, *supra*, 119 F.3d at p. 746; *U.S. v. Gourde*, *supra*, 440 F.3d at p. 1072 ["[t]he details provided on the use of computers by child pornographers and the collector profile" provided support for a finding of probable cause]; *U.S. v. Riccardi* (10th Cir. 2005) 405 F.3d 852, 860-861 [probable cause finding based in part on "the observation that possessors often keep electronic copies of child pornography"]; *Vosburgh*, *supra*, 602 F.3d at p. 528; *U.S. v. Lemon*, *supra*, 590 F.3d at p. 615 ["Many courts, including our own, have given substantial weight to testimony from qualified law enforcement agents about the extent to which pedophiles retain child pornography"]; *U.S. v. Richardson*, *supra*, 607 F.3d at p. 370, and cases cited therein].) *U.S. v. Weber* (9th Cir. 1990) 923 F.2d 1338, and *U.S. v. Zimmerman* (3d Cir. 2002) 277 F.3d 426, cited by Kuhn, are distinguishable on their facts.[5]

---

[5] In *Weber*, the Ninth Circuit rejected information regarding the practices of child molesters because there was "not a whit of evidence" in the affidavit indicating the defendant was a child molester. (*U.S. v. Weber*, *supra*, 923 F.2d at p. 1345.) In *Zimmerman*, the warrant application contained no information suggesting the defendant ever possessed child pornography in his home, and only minimal, stale evidence suggested adult pornography would be found there; on these facts, there was no probable cause to search for either. (*U.S. v. Zimmerman*, *supra*, 277 F.3d at pp. 433-435.) In contrast, here the affidavit contained sufficient evidence Kuhn had downloaded and collected files containing child pornography on his computer, which could reasonably be

c. *The warrant affidavit did not contain recklessly misleading statements.*

Kuhn next contends his motions should have been granted because the affidavit contained recklessly misleading statements. He is incorrect.

A defendant has a limited right to challenge the veracity of statements contained in an affidavit of probable cause made in support of the issuance of a search warrant. (*Franks v. Delaware* (1978) 438 U.S. 154, 155-156; *People v. Scott, supra,* 52 Cal.4th at p. 484; *People v. Lewis and Oliver* (2006) 39 Cal.4th 970, 988.) When presented with such a challenge, a trial court must conduct an evidentiary hearing on the question if the defendant makes a substantial showing that (1) the affidavit contains statements that are deliberately false or were made in reckless disregard of the truth, and (2) the affidavit's remaining contents, after the false statements are excised, are insufficient to support a finding of probable cause. (*People v. Bradford* (1997) 15 Cal.4th 1229, 1297; *Scott*, at p. 484; *Lewis and Oliver*, at p. 989; *People v. Luera* (2001) 86 Cal.App.4th 513, 524-525.) If the statements are proved false or reckless at the hearing, they must be excised. If the remaining contents of the affidavit are insufficient to establish probable cause, the warrant must be voided and any evidence seized pursuant to the warrant suppressed. (*Franks v. Delaware, supra,* at pp. 155-156; *Bradford*, at p. 1297.) "Innocent or negligent misrepresentations will not support a motion to traverse." (*Scott*, at p. 484; *Lewis and Oliver*, at pp. 988-989.) The defendant must make his or her showing by a preponderance of the evidence, and the affidavit is presumed valid. (*Scott*, at p. 484.)

Echoing his arguments in the preceding section, Kuhn urges that Officer Good's statements that collectors of child pornography typically store such materials as computer files and go to great lengths to protect them from discovery were "certainly reckless." He repeats his concerns that the affidavit did not sufficiently define "collector" or provide information showing he was a collector. We have already explained that the affidavit did contain information sufficient to show Kuhn was a collector of child pornography. It

---

expected to be at the Culver City address. (See *U.S. v. Lacy, supra,* 119 F.3d at p. 746, fn. 6 [distinguishing *Weber*]; *Vosburgh, supra,* 602 F.3d at pp. 530-531 [distinguishing *Zimmerman*]; *People v. Nicholls, supra,* 159 Cal.App.4th at pp. 713-714.)

could not have been "reckless" for Good to describe the habits of collectors of child pornography, as such information was relevant and based upon his training and expertise. Kuhn also complains that his child pornography was not hidden, but was available to the general public through Gnutella. Assuming this assertion is accurate, it does not demonstrate the falsity of Good's statement that collectors often attempt to hide their materials.

Kuhn further complains that the affidavit contained an inaccurate statement that all three of the co-occupants of the Playa Del Rey apartment filed change of address forms in March 2010. According to the affidavit, Postal Inspector Harjala told Good that Serrano, Pederson, and Nicholas also filled out change of address forms indicating a move from the Playa Del Rey apartment to the Culver City apartment. According to a declaration filed by Kuhn's counsel in support of the suppression motion below, when the warrant was executed, "Serrano denied ever living at 7777 W. 91st Street . . . and Michael Kuhn and Jeffrey Pederson also denied that Felipe Serrano lived there." Kuhn asserts that this inaccuracy "calls into question all the information from the Postal Inspector."

It does not. Assuming arguendo that counsel's averments were accurate, they do not demonstrate any deliberately false or recklessly misleading statements by Good. Even if Harjala was mistaken, there is no reason to assume Good knew or had any reason to doubt her statements. (See *People v. Lewis and Oliver, supra,* 39 Cal.4th at p. 989; *People v. Lieng* (2010) 190 Cal.App.4th 1213, 1229.) Moreover, excising this information from the warrant affidavit would have had no effect on the probable cause showing. The federal cases cited by Kuhn (*United States v. Stanert* (9th Cir. 1985) 762 F.2d 775; *United States v. Davis* (9th Cir. 1983) 714 F.2d 896; *United States v. Chesher* (9th Cir. 1982) 678 F.2d 1353; *U.S. v. DeLeon* (9th Cir. 1992) 979 F.2d 761), are not factually similar to the instant matter.

3. *The warrant was not an overbroad "general warrant," either as written or as executed* .

Appellant next avers that the search warrant was an impermissible "general warrant" that allowed a search for "essentially anything." He is incorrect.

The Fourth Amendment requires that a search warrant particularly describe the place to be searched and the things to be seized. (*People v. Eubanks, supra,* 53 Cal.4th at p. 133; U.S. Const., 4th Amend.; see also Cal. Const., art. I, § 13; § 1525.) The Constitution prohibits the issuance of " '[g]eneral warrants' " that allow for a " ' "general, exploratory rummaging in a person's belongings." ' " (*People v. Ulloa, supra,* 101 Cal.App.4th at p. 1004, citing *Andresen v. Maryland* (1976) 427 U.S. 463.) The particularized description requirement " ' " 'makes general searches . . . impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.' " [Citations.]' " (*Ulloa,* at p. 1004.) A warrant that fails to particularly describe the evidence sought is unconstitutional. (*People v. Superior Court (Nasmeh)* (2007) 151 Cal.App.4th 85, 95 (*Nasmeh*).) " 'Specificity has two aspects: particularity and breadth. [] Particularity is the requirement that the warrant must clearly state what is sought. [Citation.] Breadth deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based.' " (*Ulloa,* at p. 1005.)

Whether a warrant is sufficiently particular is a question of law subject to independent review by an appellate court. (*People v. Eubanks, supra,* 53 Cal.4th at p. 133; *People v. Kraft, supra,* 23 Cal.4th at p. 1041; *Nasmeh, supra,* 151 Cal.App.4th at p. 95.) In analyzing this question, we consider the purpose of the warrant, the nature of the items sought, and the totality of the circumstances surrounding the case. "A warrant that permits a search broad in scope may be appropriate under some circumstances, and the warrant's language must be read in context and with common sense." (*Eubanks*, at pp. 133-134.)

Here, the warrant specified that the areas to be searched were the Culver City apartment, including "any attics, basements, garages, storage lockers, safes, buildings

attached or unattached that are readily accessible to, under the control of or used by the occupants. It is also to include the vehicles parked on the property, adjacent to the property or in the street that are owned by or under the control of any occupants of" the Culver Boulevard apartment.

The "subject items" to be seized were described as: (1) "Any digital device capable of storing any 'writing' as defined by Evidence Code [s]ection 250 of child pornography as defined by California Penal Code [s]ection 311"; and (2) "Any 'writing' that constitutes evidence of child sexual exploitation as defined by California Penal Code [s]ection 311.3." The warrant further defined "writing" and "digital device."[6]

The warrant allowed any digital devices or writings seized to be removed and subsequently searched for: visual depictions of minors engaged in sexually explicit conduct as defined in section 311; writings pertaining to the possession, production, reproduction, receipt, or distribution of such depictions; writings sent with the intent to seduce a minor, or for purposes of arranging to meet with a minor for the purpose of sexually exploiting the minor; writings showing use of digital devices containing such evidence; credit card information, bills, and payment records for Internet services and receipt of child pornography; writings tending to identify the children depicted; items that would show an unusual interest in children or children's activities, including collections of photographs and magazines depicting children; and writings showing dominion and

---

[6] The warrant defined "writing" as "handwriting, typewriting, printing, Photostatting, photographing, photocopying, transmitted by electronic mail or facsimile, and every other means of recording upon any tangible thing, any form of communication or representation, including letters, words, pictures, sounds, or symbols, or combinations thereof, and any record thereby created, regardless of the manner in which the record has been stored." " '[D]igital device' " included "any electronic system or device capable of storing and/or processing data in digital form, including: central processing units; laptop or notebook computers; personal digital assistants; wireless communication devices such as telephone paging devices, beepers, and mobile telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices such as modems, cables, and connections; storage media such as hard disk drives, floppy disks, compact disks, magnetic tapes, and memory chips; and security devices."

control of the property searched. The affidavit explained that searching digital devices is a highly technical process requiring expertise and specialized equipment. Digital data is vulnerable to inadvertent or intentional modification or destruction, and in order to recover hidden, deleted, compressed, encrypted, or password protected data, examination in a controlled environment such as a law enforcement laboratory is essential to a complete and accurate analysis. Moreover, the volume of data typically stored on digital devices is so large as to make it impractical to search them at the time the warrant is executed.

a. *Particularity.*

It is readily apparent from the foregoing that the warrant described the items to be seized with sufficient particularity. (See *People v. Ulloa*, *supra*, 101 Cal.App.4th at p. 1005.) It did not provide for a "wide open" search for "evidence of general offenses not mentioned in the affidavit," or seizure of "virtually all 'writing' in the apartment," as Kuhn contends. The affidavit specifically identified the alleged criminal activities at issue. It authorized officers to search only the apartment and areas under the occupants' control, only for writings and digital devices related to child pornography activities. Officers had no discretion to seize writings that did not pertain to child pornography, or search any items that could not contain such writings.

Kuhn argues the warrant was not sufficiently precise because it failed to name him or his roommates specifically; failed to describe the subject computer by its IP address; and failed to list the "14 kids" video by name. But the "14 kids" file and the computer's IP address were described elsewhere in the affidavit and obviously fell within the categories of items listed in the warrant. It was also clear from the affidavit that Kuhn was one of the occupants of the Culver City apartment, and the main focus of the search. Under these circumstances, we do not discern how the failure to include his name, the "14 kids" file name, or the computer's IP address in the listing of items to be seized rendered the warrant unconstitutionally imprecise. " '[T]he requirement that a search warrant describe its objects with particularity is a standard of "practical accuracy" rather

than a hypertechnical one.' [Citations.]" (*Nasmeh, supra,* 151 Cal.App.4th at p. 96; see also *People v. Smith* (1994) 21 Cal.App.4th 942, 948-949.)

b. *Overbreadth.*

Nor was the warrant's scope overbroad. To the contrary, "the breadth of the warrant . . . was commensurate with the scope of the investigation." (*People v. Kraft, supra,* 23 Cal.4th at p. 1043.) As described *ante*, there was probable cause to believe Kuhn downloaded, possessed, or shared child pornography on his computer at his apartment. Based on his training and experience, Officer Good averred that child pornography collectors "store the images in many different locations such as their home, their vehicle, their work areas, and other areas under their control" and sometimes go to great lengths to hide their pornography. Therefore, the search of Kuhn's entire apartment and other areas on the premises where he could have stored or concealed child pornography was reasonable and within the scope of the probable cause showing. "The connection between the items to be seized and the place to be searched need not rest on direct observation. It may be inferred from the type of crime involved, the nature of the item, and the normal inferences as to where a criminal might likely hide incriminating evidence." (*People v. Miller, supra,* 85 Cal.App.3d at p. 201.)

The warrant was not overbroad in regard to the categories of writings sought. Obviously, a search for writings containing actual child pornography was justified by the probable cause showing. Evidence showing ownership of seized digital devices, payment for internet services, and payment for pornography itself was relevant to the determination of who in the apartment had downloaded the pornography. (See *People v. Eubanks, supra,* 53 Cal.4th at pp. 133-134 [search for items showing "dominion and control" was not overly broad or nonparticular]; *People v. Nicolaus* (1991) 54 Cal.3d 551, 575 [officers acted properly in seeking independent evidence to establish defendant's occupancy of apartment and control over evidence seized therefrom].) Likewise, items showing an unusual interest in children potentially had relevance to prove possession of child pornography.

Kuhn nevertheless contends the scope of the warrant was overbroad in several respects. He avers the warrant improperly allowed for the seizure of all digital devices in the apartment, whereas Good only had information that the single computer with the IP address 76.171.169.96 contained child pornography files. But it is common knowledge that computer files can be moved, copied, or stored on more than one device. Therefore, the warrant provided probable cause to search digital devices in addition to the single computer previously identified.

In a similar vein, he contends that the warrant should not have authorized a search for anything beyond the "14 kids" video or "at most" the additional SHA1 files identified in January 2010. The trial court found this contention "absurd." We agree. We see no reason why the search had to be limited to the files already identified. (See *Andresen v. Maryland, supra,* 427 U.S. at p. 479, fn. 10 [warrant allowing for " 'fruits, instrumentalities and evidence of crime at this [time] unknown' " was lawful because in context, the phrase permitted officers to seize evidence of other fraudulent real estate transactions relevant to the defendant's methods and motives in the charged crime]; *People v. Eubanks, supra,* 53 Cal.4th at p. 134 [discussing *Andresen*].) *U.S. v. Rabe* (9th Cir. 1988) 848 F.2d 994, cited by Kuhn, does not suggest a contrary conclusion. In *Rabe,* the Ninth Circuit *rejected* an overbreadth challenge where the warrant for the most part limited the officer's search to materials depicting minors engaged in sexually explicit conduct, as well as documents evidencing the purchase, sale, or trade of such material. (*Id.* at pp. 997-998.) *Rabe* undercuts, rather than supports, Kuhn's contention. Contrary to Kuhn's argument, the instant case bears no resemblance to *People v. Frank* (1985) 38 Cal.3d 711, or the federal cases he cites.

Next, Kuhn complains the search was overbroad as to time, because there was no limit on the dates of materials to be seized and searched. While such an omission might be problematic in certain cases, here it was not. The fact a writing was not recent would not negate its relevance: if, for example, Kuhn possessed vintage magazines or photos showing child pornography, he would still have been in violation of section 311.11.

Nor was suppression required because the warrant allowed officers to search for writings showing attempts to seduce or arrange a meeting with a minor. Kuhn argues that because Officer Good had no information he had or would engage in such behavior, there was no probable cause to seize items related to such activities. We do not necessarily agree with this contention. "[T]here is no requirement that each item seized be supported by probable cause" and no requirement "that there must be a precise correlation between the items in the warrant and the probable cause declarations in the affidavit." (*People v. Ulloa, supra,* 101 Cal.App.4th at pp. 1005, 1007; *People v. Kraft, supra,* 23 Cal.4th at p. 1050.) But we need not reach this question because the record does not reflect that any evidence Kuhn attempted to meet with or seduce a minor was recovered in the search. Therefore, even if this aspect of the warrant was overbroad, he has no cause to complain. (See *People v. Carpenter* (1999) 21 Cal.4th 1016, 1043-1044 [defendant contended portions of warrant were overbroad; however, he "has not identified any item seized under any of [the assertedly overbroad] provisions that was admitted at trial. Accordingly, even if we assume some provision of the warrant was overbroad, defendant has not shown that any evidence should have been suppressed"]; *People v. Camarella* (1991) 54 Cal.3d 592, 607, fn. 7 [" 'Even when a warrant is overbroad *in part*, evidence will not be suppressed if it was seized pursuant to a portion of the warrant which was *not*' "]; *People v. Farley* (2009) 46 Cal.4th 1053, 1101-1102; *U.S. v. Rabe, supra,* 848 F.2d at p. 998 [even if sections of warrant were impermissibly overbroad, "no evidence was obtained in reliance upon them"].)

For the same reason, we reject Kuhn's contentions that the warrant was overbroad because it allowed a search of the entire apartment, as opposed to only his room and the common areas; of buildings or vehicles accessible to the all occupants of the apartment; and of computers and digital equipment that belonged to his roommates, rather than to him. Again, while we do not necessarily agree these categories were overbroad, the only items seized in the search were found in Kuhn's bedroom in the Culver City apartment. Because no items were seized pursuant to the portions of the warrant Kuhn contends were overbroad, he fails to show suppression of any of the evidence was required. (*People v.*

Carpenter, supra, 21 Cal.4th at pp. 1043-1044; *People v. Camarella, supra,* 54 Cal.3d at p. 607, fn. 7; *People v. Farley, supra,* 46 Cal.4th at pp. 1101-1102.)

Kuhn argues that as executed, the search actually conducted amounted to a general warrant search. (See *United States v. Rettig* (9th Cir. 1978) 589 F.2d 418, 423 [although warrant was not a general warrant on its face, agents did not confine their search in good faith to the objects of the warrant].) The only basis for Kuhn's assertion appears to be that the officers searched "all the digital devices in the apartment for essentially any writing or crime involving children." However, as we have explained, the warrant properly allowed for a search of all digital devices. Kuhn points to nothing in the record showing the officers searched for evidence of crimes other than those related to child pornography, or otherwise exceeded the parameters of the warrant.

Finally, Kuhn complains that "the search warrant did not set forth a protocol for a limited search of the digital storage devices" and "did not restrict its execution to a digital expert using a 'hashing' program." However, Kuhn cites no California or United States Supreme Court case requiring such a protocol. The Ninth Circuit cases he does cite—*U.S. v. Comprehensive Drug Testing, Inc.* (9th Cir. 2010) 621 F.3d 1162 [2010 U.S. App. LEXIS 19070] (*CDT*), and *United States v. Tamura* (9th Cir. 1982) 694 F.2d 591, do not impose such a requirement either. *Tamura* was decided in 1982, "just preceded the dawn of the information age," and concerned paper, not electronic, records. (*CDT*, at p. 1169; see also *U.S. v. Stabile* (3d Cir. 2011) 633 F.3d 219, 324 [2011 U.S. App. LEXIS 1945].) *CDT* involved a federal investigation into steroid use by professional baseball players. In *CDT,* the Ninth Circuit offered "[c]oncluding [t]houghts" about "the challenges faced by modern law enforcement in retrieving information it needs to pursue and prosecute wrongdoers, and the threat to the privacy of innocent parties from a vigorous criminal investigation." (*CDT*, at p. 1175.) The court opined that the "pressing need of law enforcement for broad authorization to examine electronic records . . . creates a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant." (*Id.* at p. 1176.) The court explained that electronic files are generally found on media containing "thousands or

millions of other files among which the sought-after data may be stored or concealed. By necessity, government efforts to locate particular files will require examining a great many other files to exclude the possibility that the sought-after data are concealed there." (*Ibid.*)

In a concurrence, Chief Judge Kozinski offered "guidance" about "how to deal with searches of electronically stored data in the future so that the public, the government and the courts of our circuit can be confident such searches and seizures are conducted lawfully." (*CDT, supra,* 621 F.3d at p. 1178.) Among other things, Judge Kozinski suggested the following: "The process of sorting, segregating, decoding and otherwise separating seizable data (as defined by the warrant) from all other data should . . . be designed to achieve that purpose and that purpose only. Thus, if the government is allowed to seize information pertaining to ten names, the search protocol should be designed to discover data pertaining to those names only, not to others, and not those pertaining to other illegality. *For example, the government has sophisticated hashing tools at its disposal that allow the identification of well-known illegal files (such as child pornography) without actually opening the files themselves. These and similar search tools should not be used without specific authorization in the warrant, and such permission should only be given if there is probable cause to believe that such files can be found on the electronic medium to be seized*." (*Id.* at p. 1179 (Kozinski, C.J., concurring), italics added.) Thus, apart from the facts that Chief Judge Kozinski's concurrence comprised guidance, rather than mandatory procedures, and *CDT* is not binding on this court (*People v. Williams* (1997) 16 Cal.4th 153, 190), *CDT* did not require that files in child pornography cases be examined only using a "hashing tool" as Kuhn appears to suggest.[7]

[7] Because we conclude that the information in the affidavit provided probable cause to support the search warrant, which met the particularity requirement, we need not consider the People's assertion that the good faith exception to the warrant requirement applies. (*People v. Jones*, *supra*, 217 Cal.App.4th at p. 742.)

DISPOSITION

The judgment is affirmed.

NOT TO BE PUBLISHED IN THE OFFICIAL REPORTS

ALDRICH, J.

We concur:

CROSKEY, Acting P. J.

KITCHING, J.