Filed 7/31/12 P. v. Aflleje CA2/7

NOT TO BE PUBLISHED IN THE OFFICIAL REPORTS

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA

SECOND APPELLATE DISTRICT

DIVISION SEVEN

THE PEOPLE, Plaintiff and Respondent, v. JOHNNY MARTINEZ AFLLEJE, Defendant and Appellant.	B231304 (Los Angeles County Super. Ct. No. BA365823)

APPEAL from a judgment of the Superior Court of Los Angeles County, Leslie A. Swain, Judge. Affirmed.

Alan Stern, under appointment by the Court of Appeal, for Defendant and Appellant.

Kamala D. Harris, Attorney General, Dane R. Gillette, Chief Assistant Attorney General, Lance E. Winters, Senior Assistant Attorney General, Steven D. Matthews and Shawn McGahey Webb, Deputy Attorneys General, for Plaintiff and Respondent.

_____

INTRODUCTION

Defendant Johnny Martinez Aflleje appeals from a judgment of conviction entered after he pled no contest to a charge of possession of child pornography (Pen. Code, § 311.11, subd. (a)).[1] He entered into a plea agreement following the denial of his motion to quash a search warrant and suppress evidence. Pursuant to the plea agreement, defendant received three years of formal probation, with the first 365 days to be served in county jail. As part of the plea disposition, a charge of committing a lewd act upon a child (§ 288, subd. (a)) was dismissed.

On appeal, defendant contends that the trial court erred in denying his suppression motion. We affirm.

FACTS[2]

On December 9, 2009, Officer Michael Solis of the Los Angeles Police Department (LAPD) and other members of a search team executed a warrant at defendant's home, which he shared with his parents, three brothers and the girlfriend of one of his brothers. Defendant was not home at the time, and he kept his bedroom door locked. The officers made a forced entry into his locked bedroom.

During the search, the police seized three computers, hard drives, zip drives, thumb drives, DVDs, a digital camera, and a pair of panties for a young female. Child pornography was found on one or more of the DVDs, on a computer, and on a memory card in the digital camera.

---

1 All future statutory references are to the Penal Code.

2 The facts are drawn from testimony presented at the preliminary hearing.

When defendant returned home, he was interviewed after waiving his *Miranda*[3] rights. Defendant admitted to Officer Solis that he possessed over one hundred digital images and videos of child pornography. He explained that he fantasized about children and was sexually aroused by images.

When asked about his six-year-old niece, K.V., defendant acknowledged that he gave her a kiss on the lips and took a picture of it. He admitted the picture aroused him in a sexual manner. When K.V. and her mother were later interviewed, they both denied that the panties belonged to K.V.

DISCUSSION

A. *Applicable Law*

Section 1525 provides that a search warrant cannot be issued but upon probable cause, supported by an affidavit. A defendant seeking to quash a search warrant bears the burden of establishing its invalidity. (*Theodor v. Superior Court* (1972) 8 Cal.3d 77, 101.) Most California appellate courts have adopted the federal standard of review, under which a magistrate's determination is given "'great deference'" and will not be overturned unless the affidavit fails as a matter of law to establish probable cause. (*Fenwick & West v. Superior Court* (1996) 43 Cal.App.4th 1272, 1277-1278.)

Probable cause to issue a search warrant exists when, based on the totality of circumstances described in the affidavit, "there is a fair probability that contraband or evidence of a crime will be found in a particular place." (*Illinois v. Gates* (1983) 462 U.S. 213, 238 [103 S.Ct. 2317, 76 L.Ed.2d 527].) Because of the law's preference for warrants, doubtful or marginal cases should be resolved in favor of upholding the warrant. (*People v. Superior Court (Corona)* (1981) 30 Cal.3d 193, 203.)

---

3 *Miranda v. Arizona* (1966) 384 U.S. 436 [86 S.Ct. 1602, 16 L.Ed.2d 694].

B. ***Suppression Motion and Hearing Held Over Four Days***

1. August 3, 2010

In 2009, Officer Solis investigated Internet crimes against children. He was also designated as a federal agent and worked with the Federal Bureau of Investigation and Immigration Customs Enforcement (ICE) on the federal Internet Crimes Against Children (ICAC) task force. The task force monitored activity on the Internet and determined that child pornography had been downloaded by a customer of Time Warner Road Runner. Officer Solis signed a federal summons directed to Time Warner to identify the customer. The summons was signed by a customs commissioner and sent to Time Warner.

Time Warner responded by faxing a letter to Officer Solis disclosing defendant's name, address, phone number, user name, and the length of time Road Runner had provided his Internet service. Officer Solis used the information provided by Time Warner to obtain a search warrant for defendant's address.

2. August 27, 2010

Defendant argued that he retained a right of privacy in the information he had disclosed to Time Warner. He also claimed that the federal summons was invalid because the stated purpose of its issuance was not an investigation into Internet child pornography, but an investigation or inquiry to ascertain the correctness of any entry, to determine the liability for duties, taxes, fines, penalties, or forfeitures, and/or to insure compliance with the laws or regulations administered by the United States Customs Service under the Tariff Act of 1930 (19 U.S.C. § 1509(a)).

In opposition to the motion to suppress, the People argued that defendant lacked standing to challenge the summons because he had no expectation of privacy under state or federal law in any information he had willingly provided to Time Warner Road Runner. Time Warner Road Runner's Subscriber Privacy Notice clearly stated that it would disclose subscriber information to third parties such as advertisers and direct mail companies for purposes such as direct marketing, and to governmental entities pursuant

to laws, including the Electronic Communications Privacy Act (ECPA), which allow personally identifiable information to be obtained through a subpoena, warrant, or court order. The People also argued that the ECPA allows the government to subpoena a third party service provider for information such as a subscriber's name and address.

The court noted that defendant was asking whether the administrative summons was authorized by federal statute to be used in the investigation of child pornography. The People responded that, along with the language indicating that the requested information was required in connection with an investigation to ascertain liability for duties, taxes, etc., the summons states "and/or to insure compliance with the laws or regulations administered by the U.S. Customs Service."

3. October 8, 2010

Prior to the hearing, the People provided the court with the Privacy Impact Assessment for the Immigration and Customs Enforcement Child Exploitation Tracking System (ICE-CETS). Section 1.6 deals with the legal authorities applicable to the collection of information. The section states that the ECPA "authorizes the release of certain basic subscriber information upon service of an authorized administrative subpoena by a government entity" and the Tariff Act of 1930 "allows for collection of this type of information by Customs Summons when there is probable cause to believe an importation into the United States has been made. Crimes involving exploitation of children often involve international distribution; as a result investigations of these crimes are part of ICE's enforcement mission."

Defendant claimed that the ECPA authorized the issuance of a summons seeking the release of subscriber information only "where there is probable cause to believe an importation into the United States" had occurred, and there was no probable cause to believe that importation had occurred in this case. All that had been established was that an LAPD officer was investigating a purely state crime in California without a showing of any international distribution on the record.

The trial court identified the issues as whether the summons issued could properly be used in the investigation of child pornography and whether there had been a showing that the material had an international origin or connection.

4. October 22, 2010

The People referred the court to the Customs Border Act of 2001 and the Homeland Security Act of 2002, which created ICE by merging several federal agencies and gave ICE jurisdiction to investigate and prevent child pornography and sexual exploitation. The People also cited the Effective Child Pornography Prosecution Act of 2007, which gives federal law enforcement agencies jurisdiction over any person who "knowingly mails, or transports or ships using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any child pornography; . . . ." (18 U.S.C. § 2252A(a)(1).)

The People also asserted that even if there was error in issuing the summons without amending the boilerplate language (regarding liability for duties, taxes, and fines, etc.), suppression was not warranted because Officer Solis had acted in good faith.

Defendant responded that the People were not addressing the question whether or not the three files at issue came under the jurisdiction of ICE, because the People had not shown any importation of these materials into the United States.

The court indicated the question had been narrowed to specifically determine "whether there is evidence of at least reasonable probable cause to believe that this material has some foreign nexus . . . ." The court noted it believed the summons used by the Customs Department in seeking information about pornography was appropriate because on the face of the Tariff Act there are provisions for obscene material.

After considering the parties' written and oral arguments, the trial court issued a five-part ruling: (1) Defendant had no expectation of privacy in his subscriber information given Time Warner's Subscriber Privacy Notice; (2) ICE had jurisdiction to investigate child pornography; (3) there was probable cause to believe the child pornography possessed by defendant had an international nexus; (4) the summons used

by Officer Solis was an appropriate means by which to obtain defendant's subscriber information; and (5) Officer Solis had a good faith belief in the validity of the summons.

C. *Analysis*

Defendant contends that he retained the right to privacy in the information he had disclosed to Time Warner. He also contends that the federal summons was invalid because the stated purpose of its issuance was not an investigation into Internet child pornography, but "an investigation or inquiry to ascertain the correctness of entries, to determine the liability for duties, taxes, fines, penalties or forfeitures, and/or to insure compliance with the laws or regulations administered by the U.S. Customs Service."

Both parties note that neither the California nor the United States Supreme Court has addressed the treatment of Internet addresses under the Fourth Amendment. Division Six of this district and all lower federal courts that have addressed this issue have concluded that a person does not retain a reasonable expectation of privacy in his personal identifying information that was openly disclosed to his Internet service provider (ISP).

The Second District, Division Six case of *People v. Stipo* (2011) 195 Cal.App.4th 664 is quite instructive.[4] In *Stipo*, a computer hacker gained control of the Hacienda La Puente High School District computer network. This information gave him access to payroll and employee records, birthdates, social security numbers, and other confidential data. The school district's computer expert tracked the hacker to a Time Warner Road Runner Internet Protocol (IP) address. This information was given to the investigating officer, who issued a warrant to Time Warner. Time Warner responded to the warrant with the defendant's name, address, and account information. With this information, the officer obtained a warrant to search the defendant's home. As a result of the search, the officer recovered a diagram mapping the intrusion of the high school's network along

---

[4] While *Stipo* is not binding on this court, it is persuasive authority. (*Lauderdale Associates v. Department of Health Services* (1998) 67 Cal.App.4th 117, 122.)

with digital evidence connecting the defendant to the crime. The defendant moved to quash the warrants and suppress the evidence obtained from Time Warner and from the search of his home, based upon a lack of probable cause. The trial court denied the motions and the defendant appealed. (*Id*. at p. 667-668.)

Initially relying on the United States Supreme Court's decision in *Smith v. Maryland* (1979) 442 U.S. 735 [99 S.Ct. 2577, 61 L.Ed.2d 220], the court rejected defendant's argument that he had a reasonable expectation of privacy in the information he had provided to Time Warner. "[T]he Supreme Court held that 'a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.' Here [the defendant] gave subscriber information to a business. In *Smith*, the court concluded that such information falls outside the Fourth Amendment's privacy protections. It said, 'When he used his phone, [the defendant] voluntarily conveyed numerical information to the telephone company and "exposed" that information to its equipment in the ordinary course of business. In so doing, [the defendant] assumed the risk that the company would reveal to police the numbers he dialed.'" (*People v. Stipo*, *supra*, 195 Cal.App.4th at p. 668, quoting from *Smith*, *supra*, at p. 744.)

Division Six in the *Stipo* opinion stated with regard to information conveyed to ISPs, the Tenth Circuit Court of Appeals had found that "'[e]very federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation.'" (*People v. Stipo*, *supra*, 195 Cal.App.4th at pp. 668-669, quoting *U.S. v. Perrine* (10th Cir. 2008) 518 F.3d 1196, 1204.) Division Six also relied on the Ninth Circuit Court of Appeals' decision in *U.S. v. Forrester* (9th Cir. 2008) 512 F.3d 500, 510, which drew an analogy between the telephone users discussed in *Smith* and Internet users.

The *Forrester* court explained that Internet users, like telephone users, rely on third party equipment to engage in communications: *Smith* "'based its holding that telephone users have no expectation of privacy in the numbers they dial on the users' imputed knowledge that their calls are completed through telephone company switching equipment. [Citation.] Analogously, e-mail and Internet users have no expectation of

privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information. Like telephone numbers, which provide instructions to the "switching equipment that processed those numbers," e-mail to/from addresses and IP addresses are not merely passively conveyed through third party equipment, but rather are voluntarily turned over in order to direct the third party's servers.'" (*People v. Stipo*, *supra*, 195 Cal.App.4th at p. 669, quoting *U.S. v. Forrester*, *supra*, 512 F.3d at p. 510.) Division Six held that "[a] subscriber has no expectation of privacy in the subscriber information he supplies to his Internet provider. Therefore, [a] challenge to a warrant requiring [the] Internet provider to identify [a person] through [the] Internet Protocol (IP) address has no merit." (*Stipo, supra,* at p. 666.)

Even if we elect not to follow *Stipo* and the federal cases and find that defendant had a privacy interest in his subscriber information, his contention would still fail because there was probable cause for issuance of the federal summons. Probable cause to search exists when "there is a fair probability that contraband or evidence of a crime will be found in a particular place." (*Illinois v. Gates*, *supra*, 462 U.S. at p. 238.) In the course of an ICAC investigation into Internet child pornography, the federal task force learned that child pornography had been downloaded to a particular IP address. This provided a fair probability that child pornography would be found at that address, i.e., in the home of the owner of the IP address.

Moreover, as the trial court found, Officer Solis was entitled to rely on the warrant even if the affidavit was insufficient to establish probable cause. In *United States v. Leon* (1984) 468 U.S. 897 [104 S.Ct. 3405, 82 L.Ed.2d 677], the United States Supreme Court held that evidence should not be excluded when an officer objectively relies in good faith on a warrant issued by a neutral and detached magistrate. The relevant inquiry for the exception is whether a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization. (*Id*. at pp. 922-923.) The Fourth Amendment's exclusionary rule does not bar the use of evidence obtained by officers

who in good faith reasonably rely on a search warrant that is ultimately found to be unsupported by probable cause. (*People v. Camarella* (1991) 54 Cal.3d 592, 596.)

Defendant argues the good faith exception does not apply because Officer Solis used his status as a cross-designated federal agent to obtain a warrant he would not have been able to get as an LAPD officer and had no basis to believe that defendant's IP address was linked to a federal crime. However, Officer Solis was a member of a federal task force investigating child pornography on the Internet, which had information that child pornography had been downloaded from defendant's IP address. Officer Solis revealed his cross-designation as an LAPD officer on the summons, and in seeking issuance of the summons he conveyed the information that he was "conducting an investigation involving child pornography." The officer's statement of all relevant information supports a finding of good faith.

DISPOSITION

The judgment is affirmed.

JACKSON, J.

We concur:

PERLUSS, P. J.

ZELON, J.