

NOT TO BE PUBLISHED IN OFFICIAL REPORTS

California Rules of Court, rule 8.1115(a), prohibits courts and parties from citing or relying on opinions not certified for publication or ordered published, except as specified by rule 8.1115(b). This opinion has not been certified for publication or ordered published for purposes of rule 8.1115.

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA
SIXTH APPELLATE DISTRICT

THE PEOPLE,

Plaintiff and Respondent,

v.

JEREMY ROCHA BERNAL,

Defendant and Appellant.

H040437

(Santa Clara County

Super. Ct. No. C1242138)

I. INTRODUCTION

After the trial court denied his motion to suppress evidence, defendant Jeremy Rocha Bernal pleaded no contest to possession of child pornography. (Pen. Code, § 311.11, subd. (a).¹) Defendant was placed on probation and ordered to serve four months in county jail plus 60 days of hard labor.

On appeal, defendant contends the trial court erred by denying his motion to suppress. He argues that there was no probable cause to support issuance of a search warrant for his residence, which was associated with an internet protocol address from which child pornography was being transmitted. We disagree and will affirm the judgment.

¹ All further statutory references are to the Penal Code unless otherwise indicated.

II. BACKGROUND

A. Factual Background

On August 2, 2011, while working with the Silicon Valley Internet Crimes Against Children Task Force, San Jose Police Officer Russell Chubon applied for and obtained a search warrant for the premises of 752 Wedgewood Drive.

In his probable cause statement, Officer Chubon described his training and expertise in investigating sexual assaults, child pornography, child sexual exploitation, and child molestation. His training included a 40-hour course on child pornography investigative techniques, a 28-hour course on child pornography peer-to-peer investigations, and a 21-hour course on commercial sexual exploitation of children.

Officer Chubon explained that peer-to-peer networks are frequently used by persons trading in child pornography. A person can install peer-to-peer software in order to search for and download pornography that is located on other users' computers. Officer Chubon further explained that Internet Protocol (IP) addresses are used to identify the location of computers on the internet. With an IP address, police can identify a user's internet service provider, and the service provider can identify the account holder.

On separate occasions, Officer Chubon and another officer had both used peer-to-peer software to locate a computer that was sharing files containing child pornography. The computer had an IP address of 98.248.73.18. That IP address was assigned to Comcast Cable Communications, Inc., which informed the officers that the account was associated with a residence at 752 Wedgewood Drive. The account was in defendant's uncle's name.

On August 4, 2011, officers served the search warrant at 752 Wedgewood Drive, a three or four bedroom single family residence where five or six people lived, including defendant. In a hall closet, officers found compact discs and DVD's containing child pornography. Defendant was present during the search and acknowledged the items in the closet belonged to him. Defendant's sister confirmed that defendant had been

sleeping on the couch and keeping his belongings in the hall closet. Defendant's sister also stated that defendant was in charge of maintaining the family computer.

B. Procedural Background

Defendant was charged with possession of child pornography. (§ 311.11, subd. (a).) He subsequently filed a motion to quash the search warrant and suppress evidence. In the motion, defendant argued that the search warrant was issued without probable cause and that the good faith exception to the exclusionary rule did not apply because a reasonable and well-trained officer would have known that the affidavit failed to establish probable cause. Specifically, defendant argued that because his residence was equipped with an "open wireless router," another person could have been linked into the IP address from which the child pornography had been shared. Defendant attached a declaration from an expert who asserted that "anyone in range of the wireless router could connect to the network in the Bernal residence without a password" and that activities performed by such a person could be traced back to the IP address associated with that residence.

The prosecution filed a memorandum in opposition to defendant's motion to suppress. The prosecution argued that probable cause to search existed despite the possibility that someone else had accessed the network at defendant's residence, and that in any event, the officers executing the search relied in good faith on the issuance of the warrant.

At the hearing on defendant's motion to suppress, trial counsel asserted that an IP address is not associated with a particular computer, but with a signal. Since the signal came from a wireless network, it could have been accessed by someone outside the residence. He argued that because there was no "corroboration that this computer actually rested inside that house," there was not a "fair probability" that the child pornography would be found in the house.

The trial court noted there was a “possibility” that someone outside the home had accessed the network, but that there was “still a fair probability” that the child pornography was actually located in the home. The trial court denied defendant’s motion to suppress.

III. DISCUSSION

Defendant contends the trial court erred by denying his motion to suppress. He claims the search warrant affidavit was based on speculation that child pornography would be located at 752 Wedgewood Drive, since the IP address could have been accessed by someone else over the open wireless network.

A. *Standard of Review*

“In ruling on a motion to suppress, the trial court must find the historical facts, select the rule of law, and apply it to the facts in order to determine whether the law as applied has been violated. [Citation.] We review the court’s resolution of the factual inquiry under the deferential substantial evidence standard. The ruling on whether the applicable law applies to the facts is a mixed question of law and fact that is subject to independent review. [Citation.]” (*People v. Ramos* (2004) 34 Cal.4th 494, 505.)

B. *Probable Cause Standard*

“Probable cause to search exists when, based upon the totality of the circumstances described in the affidavit, ‘there is a fair probability that contraband or evidence of a crime will be found in a particular place.’ [Citations.]” (*People v. Farley* (2009) 46 Cal.4th 1053, 1098, quoting *Illinois v. Gates* (1983) 462 U.S. 213, 238.) “A ‘practical, nontechnical’ probability that incriminating evidence is involved is all that is required.” (*Texas v. Brown* (1983) 460 U.S. 730, 742.) “ ‘The process does not deal with hard certainties, but with probabilities.’ ” (*Ibid.*)

C. *Analysis*

Defendant has not cited, and we have not found, any published California case supporting his argument.² Federal cases have uniformly rejected the claim that the use of an unsecured wireless network vitiates the probable cause that would otherwise exist to search the home of an Internet subscriber whose IP address is used to access child pornography. (See, e.g., *United States v. Vosburgh* (3d Cir. 2010) 602 F.3d 512, 526 & fn. 13 [listing cases]; *United States v. Perez* (5th Cir. 2007) 484 F.3d 735, 740 (*Perez*); *United States v. Hay* (9th Cir. 2000) 231 F.3d 630, 634-635; *U.S. v. Carter* (D. Nev. 2008) 549 F.Supp.2d 1257, 1267 [affidavit was not misleading insofar as it represented that there was probable cause to believe child pornography was located at premises associated with a particular IP address].)

In *Perez*, the defendant claimed “that the association of an IP address with a physical address does not give rise to probable cause to search that address,” since neighbors could have accessed an unsecure wireless connection to make the illicit transmissions. (*Perez, supra*, 484 F.3d at p. 740.) The Fifth Circuit rejected the claim: “[T]hough it was *possible* that the transmissions originated outside of the residence to which the IP address was assigned, it remained *likely* that the source of the transmissions was inside that residence. [Citation.] ‘[P]robable cause does not require proof beyond a reasonable doubt.’ [Citation.]” (*Ibid.*, italics added, fn. omitted.)

We agree with the federal cases cited above. Here, it was *possible* that the child pornography originated outside of the residence to which the IP address was assigned, but

² Defendant cites several unpublished federal district court opinions that recognize it is possible for neighbors and passersby to access an unsecured wireless network, but he does not claim that any cases have held that this possibility vitiates probable cause for a search warrant. Defendant also asserts that “[r]ecognized experts in the area of cyber crimes have long agreed that the identification of an IP address alone is insufficient to support . . . the issuance of a search warrant,” and he quotes from a journal article, but provides an insufficient citation for the journal.

“it remained *likely* that the source of the transmissions was inside that residence.” (See *Perez, supra*, 484 F.3d at p. 740.) In other words, although it may not have been certain that the child pornography came from the residence associated with the IP address, there remained at least “a fair probability that contraband or evidence of a crime” would be found there. (*Illinois v. Gates, supra*, 462 U.S. at p. 238.) The trial court did not err by denying defendant’s motion to suppress.

IV. DISPOSITION

The judgment is affirmed.

BAMATTRE-MANOUKIAN, ACTING P.J.

WE CONCUR:

MÁRQUEZ, J.

GROVER, J.