IN THE DISTRICT COURT OF APPEAL OF THE STATE OF FLORIDA FIFTH DISTRICT JULY TERM 2011

STATE OF FLORIDA,

Appellant,

٧.

Case No. 5D09-4197

RAMON LUIS OLIVERAS,

Appellee.

Opinion filed July 22, 2011

Appeal from the Circuit Court for Orange County, F. Rand Wallis, Judge.

Pamela Jo Bondi, Attorney General, Tallahassee, and Ann M. Phillips, Assistant Attorney General, Daytona Beach, for Appellant.

James S. Purdy, Public Defender, and Kathryn Rollison Radtke, Assistant Public Defender, Daytona Beach, for Appellee.

SAWAYA, J.

The State appeals the order suppressing evidence seized from the home of Ramon Oliveras upon execution of a search warrant. We reverse.

The victim owned two computers, which she brought with her in her luggage on a trip from Houston to Orlando. One of the computers had tracing software from Absolute Software Corporation (Absolute) that allowed Absolute to trace the location of the computer via the internet. The victim discovered that her computers had been stolen from her luggage at some point during their transport from Houston to an Orlando hotel. She notified Absolute of the theft and requested that it provide information to the police regarding the location of the computer and the identifying information of the person using it. Pursuant to that request, Absolute began monitoring the location of the computer and provided information to the police that the computer was being used by Oliveras at a location that was later discovered to be his residence. Once the police received that information, they determined that Oliveras was working for a baggage delivery service at the Orlando airport at the time pertinent to the theft of the victim's computers. A warrant was obtained and executed, leading to the recovery of the victim's computers from Oliveras' residence. Oliveras was arrested and charged with third-degree grand theft.

Oliveras moved to suppress this evidence, arguing that the police had not obtained a court order or subpoena to retrieve information from the computer tracing company, pursuant to the provisions of the Florida Security of Communications Act, chapter 934, Florida Statutes (2009). Specifically, he argued that failure to comply with the requirements of section 934.23, Florida Statutes (2009), rendered the information used in the affidavit "defective" and the evidence seized pursuant to the warrant inadmissible. The trial court suppressed the evidence, but it did so for a different reason. The trial court ruled that probable cause had not been established for issuance of the warrant because the affidavit did not contain sufficient facts to show how the software worked and how Absolute had been able to trace the stolen computers to

2

Oliveras' home. We will address the trial court's reasoning and the argument advanced

by Oliveras, which is the argument he makes in this appeal.

The basis of the trial court's ruling is lack of probable cause established by the

affidavit. The affidavit recites the pertinent facts:

Victim Billie White stated that on 02/14/2009 at 0735 hours, she flew on Continental Flight 586 from Houston, Texas to Orlando International Airport. She stated that, prior to checking her luggage in at Houston airport, she saw her two laptops, in their cases, inside her luggage. On 02/14/2009 at 1600 hours, White arrived at the Disney Pop Century resort, where her luggage had been delivered from Orlando International Airport. White opened her luggage and discovered that her Dell Inspiron 1525 laptop, S/N 6QVHYG1, and her HP Pavilion DV7 laptop had been removed from their cases and four compact disc boxes were also missing. White contacted the Houston Police Department and filed a report. White also contacted Absolute Software Corporation, which has tracking software on her Dell laptop. The total theft is estimated at \$3100. White was later informed that the Dell Inspiron laptop was being used in Florida.

On 02/21/2009, White came to the Orlando International Airport Police Office and provided a sworn statement. The Dell Inspiron was entered into Teletype. White stated that she would call back with the model and serial number for the HP Pavilion laptop. Victim White stated that she did not give anyone permission to remove her property and she desires prosecution.

On 02/20/2009, I Detective Chris Hall was assigned to investigate this case.

I received information from Jen Farrell, Theft Recovery Officer for Absolute Software Corporation. Farrell advised that the stolen Dell laptop has ComputracePlus software installed on it. The software instructs the laptop to contact the Absolute Monitoring Center, on a periodic basis, when connected to a phone line or any type of Internet connection. The Monitoring Center captures the caller ID of the phone line to which the laptop is connected and/or the originating Internet Protocol (IP) address of the laptop. ComputracePlus software was first activated on the Dell laptop on Saturday, February 07, 2009. Prior to the theft, this laptop has contacted the Monitoring Center on at least six occasions. The Monitoring Center recorded the correct data on all of the calls. After the theft of the laptop, Farrell stated that the company began monitoring the laptop and learned that Ramon Luis Oliveras at 5773 Five Flags Blvd. Apartment 2268, Orlando, Florida, was using the computer. Ferrell [sic] also provided the IP address 74.244.140.244 to which the stolen laptop is connected. After obtaining this information, it was learned that Ramon Luis Oliveras is employed by ASIG, as a bag runner. This company is responsible for transferring luggage from airplanes at Orlando International Airport (OIA), which are then delivered to Disney hotels. Ramon Oliveras was working on the date and time when Victim Billie White arrived at OIA. Jen Farrell provided documentation, which showed Ramon Oliveras, surfing the Internet and typing his address into the stolen computer.

A State of Florida Driver License check reveals that Ramon Luis Oliveras and Dafne Rodriguez both are tenants at 5773 Five Flags Blvd., apartment 2268.

Since the beginning of 2009, the OPD Airport Division has received multiple police reports of laptop computers being stolen from passengers, traveling between OIA and Disney resorts.

Based upon the totality of the evidence, your affiant has probable cause to believe, and does believe, that certain stolen property, including: a Dell Inspiron laptop computer, S/N 6QVHYG1, and HP Pavilion DV7 laptop computer, six compact discs, and other stolen property, is being kept inside the residence, located at 5773 Five Flags Blvd, apartment 2268, Orlando, Florida.

The law is well-settled that before a search warrant may be issued, the issuing

judge must examine the affidavit to see if sufficient facts are alleged to establish probable cause. <u>Burnett v. State</u>, 848 So. 2d 1170, 1174 (Fla. 2d DCA 2003). The issuing judge fulfills this responsibility by making "a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, there is a fair probability that contraband or evidence of a crime will be found in a particular place." <u>Illinois v. Gates</u>, 462 U.S. 213, 238 (1983); <u>see also Willacy v. State</u>, 967 So. 2d 131 (Fla. 2007); <u>State v. Carreno</u>, 35 So. 3d 125 (Fla. 3d DCA 2010); <u>State v. Irizarry</u>, 948 So. 2d 39 (Fla. 5th DCA 2006); <u>State v. Siegel</u>, 679 So. 2d 1201 (Fla. 5th DCA 1996); State v. Price, 564 So. 2d 1239 (Fla. 5th DCA 1990). Hence, probable cause requires

the probability of criminal activity; it does not require absolute certainty or proof beyond a reasonable doubt. <u>See Doorbal v. State</u>, 837 So. 2d 940 (Fla. 2003); <u>Irizarry</u>. In other words, the standard for probable cause "requir[es] 'more than mere suspicion but less evidence than is necessary to convict." <u>United States v. Danhauer</u>, 229 F.3d 1002, 1005 (10th Cir. 2000) (quoting <u>United States v. Burns</u>, 624 F.2d 95, 99 (10th Cir. 1980)).

When reviewing a prior determination of probable cause and the issuance of a search warrant, the reviewing circuit judge must accord deference to the issuing judge's determination, presume it to be correct, and not disturb that determination unless there is a clear showing that the issuing judge abused his or her discretion in relying on the information in the affidavit. <u>Willacy</u>, 967 So. 2d at 147; <u>Carreno</u>, 35 So. 3d at 128; <u>Price</u>, 564 So. 2d at 1241. "A trial court's duty upon reviewing the magistrate's decision to issue the search warrant is not to conduct a de novo determination of probable cause but to determine whether substantial evidence supported the magistrate's finding that, based on the totality of the circumstances, probable cause existed to issue the warrant." <u>Willacy</u>, 967 So. 2d at 147.

We believe the affidavit sufficiently established probable cause for issuance of the search warrant. At the request of the victim, Absolute, a privately-hired company, voluntarily gave information to Officer Hall regarding the location of the stolen computer with the tracing software.¹ Upon conducting independent research into the identity of

¹This is not a case where law enforcement installed a tracking device in order to pursue a suspect. Rather, the computer's owner contracted with the private corporation, Absolute Software Corporation, to have the monitoring software installed on the computer at the time of purchase, and it was the owner who contacted the monitoring company and initiated the search for her property once it was stolen. Law enforcement was not involved in this process whatsoever. "Importantly, the protection against unreasonable searches and seizures applies <u>only</u> to cases involving governmental

the suspect and his employment, Officer Hall discovered the suspect was working for a baggage delivery service at the Orlando airport at the time the computers were stolen and, thus, had access to them. The verification of the information provided by Absolute was sufficient to establish the reliability of the information. Moreover, Officer Hall testified to having had prior experience with this tracing system, and Absolute informed him that the software on the victim's computer had sent identifiably correct information on six prior dates. As for Officer Hall himself, the affidavit sets forth his credentials, including that he has a bachelor's degree in criminology and was assigned to the Airport Investigative Unit, where he had investigated numerous instances of stolen property. Clearly, the information contained in the affidavit provided a fair probability to warrant a cautious person, the issuing judge, to believe that the stolen computers were at the location specified in the warrant. As the courts have repeatedly held, proof beyond a reasonable doubt is not the standard for probable cause. Hence, whether Officer Hall knew the particular scientific or technical principles of how the computer software worked and how Absolute was able to use it to track the stolen computers in the instant case was not necessary to obtain a search warrant based on probable cause. Had the reviewing circuit judge given deference to the issuing judge's determination and accorded the requisite presumption of correctness, it is difficult to see how the decision to issue the warrant could be viewed as improper.

We note, parenthetically, that Oliveras does not argue in support of the reasoning applied by the reviewing circuit judge. Rather, Oliveras continues to assert on appeal

6

action; it does not apply when the search or seizure was conducted by a private individual." <u>Armstrong v. State</u>, 46 So. 3d 589, 593-94 (Fla. 1st DCA 2010) (emphasis in original) (citing <u>Smith v. Maryland</u>, 442 U.S. 735, 740 (1979)); <u>Pomerantz v. State</u>, 372 So. 2d 104, 108 (Fla. 3d DCA 1979), <u>review denied</u>, 44 So. 3d 581 (Fla. 2010).

that suppression was proper based on Officer Hall's failure to obtain a warrant or court order under section 934.23 before obtaining the information from Absolute. We do not believe that section 934.23 is applicable. That statute provides in pertinent part:

An investigative or law enforcement officer may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for 180 days or less only pursuant to a warrant issued by the judge of a court of competent jurisdiction.

§ 934.23(1), Fla. Stat. (2009).

Here, law enforcement never required Absolute to do anything. To the contrary, the victim consented and, in fact, requested Absolute to provide information to the police. The victim had paid for the emanation of this information from her computer and, in fulfillment of their contract, Absolute complied. While section 934.22, Florida Statutes (2009), generally prohibits a provider of electronic communications from voluntarily divulging the contents of a communication, there is an exception in section 934.22(2) that "[a] provider . . . may divulge the contents of a communication . . . [t]o an addressee or intended recipient of such communication or an agent of such addressee or intended recipient." § 934.22(2)(a), Fla. Stat. (2009). Here, the victim is the intended recipient of the tracking and identification information because she paid for that information to be captured from her own computer, pursuant to her contract with Absolute. The victim was entitled to the information and to request Absolute to provide it to Officer Hall. Moreover, the information gleaned by Absolute pertains only to the thief, who lacked any reasonable expectation of privacy with respect to any communication he transmitted to, through, or from the stolen computer.

7

We conclude that the provisions of section 934.23, Florida Statutes, are not applicable under the facts of this case and that the trial court's reason for suppressing the evidence is erroneous. Accordingly, we reverse the order granting the motion to suppress.

REVERSED.

ORFINGER, C.J. and JACOBUS, J., concur.