Filed 5/16/11

**CERTIFIED FOR PUBLICATION**

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA

SECOND APPELLATE DISTRICT

DIVISION SIX

| | |
|---|---|
| THE PEOPLE,<br><br>Plaintiff and Respondent,<br><br>v.<br><br>VINCENT MICHAEL STIPO,<br><br>Defendant and Appellant. | 2d Crim. No. B218512<br>(Super. Ct. No. KA085681-01)<br>(Los Angeles County) |

A subscriber has no expectation of privacy in the subscriber information he supplies to his Internet provider. Therefore, his challenge to a warrant requiring his Internet provider to identify him through his Internet Protocol (IP) number has no merit.

Vincent Michael Stipo appeals a judgment following his no contest pleas to wiretapping (Pen. Code, § 631, subd. (a)) and unlawfully accessing computer information (§ 502, subd. (c)(2)).[1] The trial court denied Stipo's motions to suppress evidence that the police obtained in two searches. We conclude, among other things, that 1) Stipo lacks standing to challenge a search warrant served on Time Warner Cable (Time Warner) directing it to provide subscriber information, and 2) the absence of an incorporation by reference clause for an exhibit to a search warrant affidavit is not a substantial defect. We affirm.

[1] All statutory references are to the Penal Code unless otherwise stated.

## FACTS

In January 2008, a computer hacker unlawfully entered the Hacienda La Puente High School District (District) computer network. The hacker gained control of the District's "routers," changed their "configuration," and installed "unauthorized tunnels" to route the data on the network to the hacker's computer. This gave him access to payroll and employee records, birthdates, social security numbers, and other confidential data.

Michael Droe, the District's computer expert, was able to identify the hacker's IP address as 76-174-58-173 within the Time Warner Roadrunner network.

Police Officer Rene Mesta applied for a search warrant to require Time Warner to identify the subscriber who had IP address 76-174-58-173 at the time of the unauthorized access. Mesta attached to the search warrant affidavit: exhibit one, Droe's summary of facts, and exhibit two, Mesta's investigation report which notes Droe's identification of the suspect's IP address as 76-174-58-173.

The search warrant issued on January 28. Time Warner identified the IP address as Stipo's; it provided his street address and verified that he had a current account with the company. Mesta received this information on May 2.

This, in turn, led to the application and issuance of a warrant on August 1 to search Stipo's residence. Mesta wrote in his affidavit that computer crimes were committed at Stipo's residence and "items sought in connection with the crime . . . will be found" there. At Stipo's residence, the police found a diagram that "mapped the intrusion" into the District's network and digital evidence on his laptop that connected him to the crime.

Stipo moved to quash the search warrants and to suppress evidence the police obtained from his residence and to suppress the IP subscriber information they obtained from Time Warner. (§ 1538.5.) He claimed, among other things, that Mesta's affidavits were insufficient to establish probable cause, exhibits were not properly incorporated into the affidavits, one affidavit listed an incorrect time for the computer

intrusion, and the good faith exception to the warrant requirement did not apply. The trial court denied the motions.

## DISCUSSION

### *Expectation of Privacy*

Stipo claims he has "a reasonable expectation of privacy in the information he had provided [to] his internet service provider . . . ." Therefore he reasons that his challenge to the admissibility of the address information obtained from Time Warner, which led to the search of his residence, has merit.

"[A]ny 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.) The defendant must establish that he or she has a "legitimate expectation of privacy" in the ""particular area searched or thing seized in order to bring a Fourth Amendment challenge."" (*Ibid*., italics omitted.)

Here the warrant was directed to Time Warner. But Stipo claims the information he provided to Time Warner is confidential. In *Smith v. Maryland* (1979) 442 U.S. 735, 743-744, the Supreme Court held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." Here Stipo 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, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed." (*Id*. at p. 744.)

Stipo claims Internet users have a reasonable expectation of privacy regarding the information they receive and transmit. He argues this should include "subscriber information" conveyed to Internet providers. But, as stated by the Tenth Circuit in *U.S. v. Perrine* (10th Cir. 2008) 518 F.3d 1196, 1204, "Every 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."

*U.S. v. Forrester* (9th Cir. 2008) 512 F.3d 500 draws an analogy between telephone users discussed in *Smith* and Internet users. These users "rely on third-party equipment in order to engage in communication. [*Smith v. Maryland*, *supra*, 442 U.S. 735] 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." (*Id.* at p. 510.)

*Search Warrant Affidavit Deficiencies*

Stipo claims the magistrate had insufficient information to authorize the searches. We disagree. "In reviewing a search conducted pursuant to a warrant, an appellate court inquires 'whether the magistrate had a substantial basis for concluding a fair probability existed that a search would uncover wrongdoing.'" (*People v. Carrington* (2009) 47 Cal.4th 145, 161.)

Stipo contends the affidavit for the January 28th search warrant was deficient. He notes that Mesta relied on two exhibits that were attached to his affidavit. Exhibit one, Droe's computer analysis report, contains a factual summary and concludes an unauthorized person obtained access to the server of the District's computer system. Exhibit two, Mesta's investigation report, reflects that the hacker changed the server "causing confidential information to be re-routed to the individual['s] computer," and that the suspect's IP address is 76-174-58-173.

Stipo notes that Mesta said exhibit one is incorporated by reference, but not exhibit two. Because of this omission, he asserts that the facts stated in exhibit two are not part of the affidavit. We disagree. Mesta refers to exhibit two in his affidavit and states it is attached. He included it as part of the evidence to support the warrant and based his conclusion there was probable cause to issue the warrant on the facts in that exhibit. This is sufficient to make exhibit two an integral part of the affidavit.

The absence of an incorporation clause is not a substantial defect. Incorporation by reference is a technical phrase, and police officers are not expected to use a lawyer's terminology. (*U.S. v. Ventresca* (1965) 380 U.S. 102, 108 ["Technical requirements of elaborate specificity once exacted under common law pleadings have no proper place in this area"].) Moreover, "'[A]bsent some palpable indication to the contrary, it is assumed the magistrate considered all the material presented him in support of an application for search warrant.'" (*People v. Jordan* (1984) 155 Cal.App.3d 769, 778.) "The failure to fill in the blank referring to the attachments, although careless, is not a 'substantial irregularity' so as to call the warrant into question." (*Ibid.*)

Here Mesta implicitly incorporated exhibit two into his affidavit. He simply omitted using the phrase "incorporated by reference." This oversight is far from fatal. In the subsequent August search warrant affidavit, Mesta expressly incorporated by reference the prior search warrant, which included this exhibit.

*Incorrect Time on the Affidavit*

Stipo contends probable cause is lacking because in the January search warrant affidavit, Mesta states the unauthorized entry took place at *11:57 a.m.* Stipo notes that in an exhibit to the affidavit, Droe said that entry took place at *11:37 a.m.*

But the trial court correctly found that Mesta's mistake did not invalidate the warrant. It said, "[E]ven if it was a mistake in terms of identifying the time, . . . they identified that I.P. address as the one who attempted intrusion . . . in the time frame in which the intrusions were taking place." Where the affidavit establishes the facts of the crime, a mistake as to time does not automatically negate probable cause. (*Tidwell v.*

*Superior Court* (1971) 17 Cal.App.3d 780, 787-788 [mistaken date did not invalidate warrant].) A reasonable inference is that the 20-minute difference was the result of Mesta inadvertently substituting a "5" for a "3." Mesta's affidavit and Droe's report are otherwise consistent as to all the details, including the date of the intrusion, the IP address and that the intrusion took place in the eleventh hour before noon. A magistrate would likely rely heavily on the more detailed facts in Droe's summary that set forth the correct time.

*Time Warner's Failure to File a Declaration*

Stipo notes that Mesta used Time Warner information for the second warrant application, but the company did not file a declaration "verifying the authenticity of its records." Instead, it provided a letter. Stipo argues this is a failure to comply with section 1524.2, subdivision (b)(4). We disagree.

Section 1524.2 is consistent with the federal Electronic Communications Privacy Act (ECPA) (18 U.S.C. § 2701 et seq.; § 1524.2, subd. (a)(1)), which sets forth procedures for obtaining subscriber information from Internet service providers. Section 1524.2, subdivision (b)(4) provides, in relevant part, that "[t]he foreign corporation shall verify the authenticity of records that it produces by providing an affidavit that complies with the requirements set forth in Section 1561 of the Evidence Code. *Those records shall be admissible in evidence as set forth in Section 1562 of the Evidence Code*." (Italics added.) This provision deals with the requirements for declarations that are used to admit evidence at trial. But Mesta was seeking a warrant. The Time Warner letter was not sworn, but it was signed and the company said it was providing the IP information "[p]ursuant to the specific obligations imposed by 18 U.S.C. § 2703(c)(2)" of the ECPA.

Like the ECPA, section 1524.2 governs procedures for Internet providers to disclose information, but these statutes do not purport to establish grounds to suppress evidence. (See *U.S. v. Kennedy* (D.Kan. 2000) 81 F.Supp.2d 1103, 1110.) We conclude that criminal defendants do not have exclusionary relief remedies under the ECPA and its state law counterpart--section 1524.2. The following cases are instructive: *U.S. v.*

*D'Andrea* (D.Mass. 2007) 497 F.Supp.2d 117, 121; *U.S. v. Sherr* (D.Md. 2005) 400 F.Supp.2d 843, 848; *Kennedy*, at page 1110; *People v. Carter*, *supra*, 36 Cal.4th at page 1141; *In re Lance W.* (1985) 37 Cal.3d 873, 887-888. Such defendants also lack standing to challenge Internet provider searches. (*U.S. v. Perrine, supra,* 518 F.3d at p. 1204.)

It is beside the point that Time Warner's letter is inadmissible at trial. An Internet service provider is in the best position to know the IP addresses of its subscribers. The letter was a response to a warrant. In the determination of probable cause, a magistrate reasonably could conclude the letter was reliable because the company had the incentive to respond truthfully. There are criminal penalties for providing false information. (*Florida v. J.L.* (2000) 529 U.S. 266, 270; *U.S. v. Koerth* (7th Cir. 2002) 312 F.3d 862, 871.) Stipo has not shown that the letter was inaccurate, unreliable, or that it invaded any Fourth Amendment privacy interest. (*In re Lance W., supra*, 37 Cal.3d at pp. 887-888; *U.S. v. Kennedy, supra*, 81 F.Supp.2d at p. 1110.) Moreover, the letter was a corroborating exhibit. The result would not change if Mesta had neglected to attach it, because his affidavit contained the facts that identified the IP address as Stipo's.

*Stale Warrant Information and Probable Cause*

Stipo contends his motion should have been granted because "the warrant application contained stale information." We disagree.

"No bright-line rule defines the point at which information is considered stale." (*People v. Carrington*, *supra*, 47 Cal.4th 145, 163.) "'[T]he question of staleness depends on the facts of each case.'" (*Ibid.*) "Courts have upheld warrants despite delays between evidence of criminal activity and the issuance of a warrant, when there is a reason to believe that criminal activity is ongoing or that evidence of criminality remains on the premises." (*Id.* at p. 164.)

The first search warrant was issued on January 28; the second on August 1. The trial court found that, despite the delay, there was a reason to believe that criminal activity was ongoing and that evidence of criminality would be at Stipo's residence. It

noted that Stipo had created an "information dump on all employee information" that could be used for identity theft. It found that this information "has value . . . in terms of future use or sales," and it likely would be retained by Stipo. Stipo has not shown that the court's inferences were unreasonable. Substantial delays do not render warrants stale where the defendant is not likely to dispose of the items police seek to seize. (*U.S. v. Lacy* (9th Cir. 1997) 119 F.3d 742, 746; see also *U.S. v. Newsom* (7th Cir. 2005) 402 F.3d 780, 783 ["Information a year old is not necessarily stale as a matter of law"]; *U.S. v. Ninety-Two Thousand Four Hundred Twenty-Two Dollars and Fifty-Seven Cents* (3rd Cir. 2002) 307 F.3d 137, 148 [a substantial delay is a less important factor where the defendant is likely to retain the evidence].)

This case is unlike those where the police delay obtaining a warrant in a situation where they personally know the person who will be named in the warrant. Here, the police knew only that an unknown person had committed a crime. It was therefore necessary to conduct an investigation to determine the identity of that person. The network intrusion was in January, and Mesta promptly applied for a warrant on January 28. But Mesta did not first obtain the names of potential suspects from Time Warner until early May. Consequently, he was not able to obtain a search warrant for Stipo's residence until that time. And his investigation involved multiple suspects.

We agree with the People that it was objectively reasonable for the police to believe that Stipo's computer equipment and crime evidence would be at his home. Mesta states in his affidavit that "items sought in connection with the crime"--computer hardware and software--would be found at Stipo's residence. Courts have recognized that computer equipment may be the "instrumentality of the crime," as well as the device that records the computer offense. (*Davis v. Gracey* (10th Cir. 1997) 111 F.3d 1472, 1480.) Time Warner notified Mesta that Stipo had maintained his IP address and current subscription. "'The IP . . . address is unique to a specific computer. Only one computer would be assigned a particular IP address.'" (*U.S. v. Perrine, supra*, 518 F.3d at p. 1199,

fn. 2.) Stipo also had been a long term customer of his Internet provider, and his account was active when Time Warner disclosed the subscriber information.

Equipment is essential to a computer hacker. Stipo has not shown that he would have any reason to dispose of his computer equipment. Mesta took steps to keep the investigation confidential, and Time Warner did not notify Stipo about the warrant. Because Stipo was not aware of Mesta's investigation, he had no reason to destroy evidence. Stipo's computer hard drive records the history of his computer activity. (*Tecklenburg v. Appellate Div. of Superior Court* (2009) 169 Cal.App.4th 1402, 1407-1408.) A reasonable inference is that traces of the network intrusion would be present because they are automatically entered and very difficult to remove. (*Ibid.*; *Hatch v. Superior Court* (2000) 80 Cal.App.4th 170, 181; *People v. Gall* (Colo. 2001) 30 P.3d 145, 161-162.) As the trial court noted, the intercepted District information was also a continual resource for identity theft. There was sufficient probable cause to believe that relevant evidence would be present. (*People v. Carrington, supra,* 47 Cal.4th at p. 161.)

*Good Faith*

The People contend that even if there were deficiencies in the applications for warrants, "the evidence cannot be suppressed because the officer executing the warrants acted in good faith." We agree.

"'[S]earches pursuant to a warrant will rarely require any deep inquiry into reasonableness,' [citation] for 'a warrant issued by a magistrate normally suffices to establish' that a law enforcement officer has 'acted in good faith in conducting the search.'" (*U.S. v. Leon* (1984) 468 U.S. 897, 922.) Consequently, evidence seized will not be excluded where officers rely on warrants that are later ruled to be invalid if their reliance was objectively reasonable. But this good faith doctrine does not apply where the police omit material facts, make false statements or act with a reckless disregard for the truth. (*Id*. at p. 923.) Here there is no evidence of such bad faith, and Mesta's reliance on the warrants was objectively reasonable.

We have reviewed Stipo's remaining contentions and conclude he has not shown error.

The judgment is affirmed.

CERTIFIED FOR PUBLICATION.

GILBERT, P.J.

We concur:

COFFEE, J.

PERREN, J.

Thomas C. Falls, Judge

Superior Court County of Los Angeles

---

Marilee Marshall, under appointment by the Court of Appeal, under appointment by the Court of Appeal, for Defendant and Appellant.

Edmund G. Brown, Jr., Attorney General, Dane R. Gillette, Chief Assistant Attorney General, Pamela C. Hamanaka, Senior Assistant Attorney General, Scott A. Taryle, Supervising Deputy Attorney General, Stephanie A. Miyoshi, Deputy Attorney General, for Plaintiff and Respondent.