Filed 8/3/05

CERTIFIED FOR PUBLICATION

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA

SECOND APPELLATE DISTRICT

DIVISION EIGHT

THE PEOPLE,

Plaintiff and Respondent,

v.

AVELINO LEON et al.,

Defendants and Appellants.

B173851

(Los Angeles County
Super. Ct. No. BA207150)

APPEAL from a judgment of the Superior Court of Los Angeles County. Robert Perry, Judge. Affirmed.

Kenneth H. Lewis and Peter N. Priamos for Defendant and Appellant Avelino Leon.

Sandra Uribe, under appointment by the Court of Appeal, for Defendant and Appellant Victor Aceves.

Nancy Gaynor, under appointment by the Court of Appeal, for Defendant and Appellant Victor Aceves.

Bill Lockyer, Attorney General, Robert R. Anderson, Chief Assistant Attorney General, Pamela C. Hamanaka, Assistant Attorney General, Steven D. Matthews and Mary Sanchez, Deputy Attorneys General, for Plaintiff and Respondent.

In this appeal from the denial of motions to suppress, we hold that a person who uses a false name to procure a cellular telephone has a privacy interest in his communications over that phone. The Fourth Amendment "prescribe[s] a constitutional standard that must be met before official invasion is permissible." (*Berger v. New York* (1967) 388 U.S. 41, 64.) Absent specific circumstances, eavesdropping on private communications "cannot be tolerated in a free and civilized society." (Pen. Code, § 630.)[1]

Under section 629.50, subdivision (4), law enforcement officials applying for authorization to wiretap must show, among other things, that "conventional investigative techniques had been tried and were unsuccessful, or why they reasonably appear to be unlikely to succeed or to be too dangerous . . . ." The trial court misapplied this standard, finding that, as a result of the "nature of this type of [narcotics] conspiracy," the government was entitled to "leeway . . . to continue its investigation." Contrary to the trial court's conclusion, the "necessity" requirement is not altered in cases involving investigations of narcotics conspiracies.

Although the trial court applied the wrong test, appellants have not demonstrated reversal is warranted. There was no abuse of discretion in the issuing court's determination that a wiretap was necessary. We affirm the denial of the motions to suppress.

FACTUAL AND PROCEDURAL BACKGROUND

Avelino Leon pled no contest to possession of narcotics for sale and Victor Aceves pled no contest to conspiracy to sell cocaine and to the use of a false compartment to hide drugs. Leon was sentenced to 17 years in state prison, and Aceves was sentenced to 15 years 8 months in state prison. Both unsuccessfully sought to

---

[1] All undesignated statutory citations are to this code. The wiretaps in this case were issued in 2000, before the 2002 amendments to the statute. The amendments do not affect the issues discussed in this opinion.

suppress telephonic conversations recorded by the government. They claim that the government failed to show "necessity" in affidavits supporting the applications for wiretaps Nos. 00-02 and 00-04. Both applications were supported by lengthy affidavits of Stephen Diederich, a Special Agent with the Drug Enforcement Administration.

Wiretap No. 00-02

The application for wiretap No. 00-02 described "Target Telephone #1" as subscribed to by Guillermo Rodriguez of 4727 West 17th Street, Lawndale, a fictitious address. Rodriguez, Aceves, Leon, and two unidentified males were named as suspects. Diederich had learned that Leon and Aceves resided together and Diederich had physical descriptions of each.

Diederich indicated, "I am aware drug traffickers often communicate with their drug trafficking associates through cellular telephones and digital display paging devices, in conjunction with residential telephones. I am also aware that drug traffickers often change cellular telephones and digital display paging devices to avoid detection by law enforcement." "I spoke to an AirTouch Cellular Representative who told me that Target Telephone #1 is a prepaid AirTouch cellular telephone. . . . AirTouch does not verify any of the information provided by the subscriber since it is a prepaid telephone. . . . Based on my training and experience, I know that high level traffickers frequently will use prepaid cellular telephones because no identification is required upon activation. In addition, the prepaid cellular telephone can be disposed of at any time and law enforcement will be unable to track down a new telephone for that user since a new prepaid telephone can be purchased under a completely different fictitious name." (Boldface omitted.) "I believe narcotics traffickers were more inclined to use communication devices supplied by A-Tel because A-Tel required no identifying information from the customer at the time a telephone or pager was activated."

As a basis for probable cause to grant, Diederich described a Mexico-based drug trafficking organization with associates in Los Angeles. Unidentified male No. 1 (who was later identified as Leon) was in contact with "narcotics traffickers from the Los Angeles-based distribution network cells that received cocaine" from this drug trafficking

organization. While the leader of that organization was arrested, many of the "distribution cells" to which cocaine was delivered were still intact.

Calls from a discarded telephone to which a wiretap previously had been authorized suggested that unidentified male No. 1 was in contact with a Los Angeles-based distribution network. Unidentified male No. 1 was suspected to be a "top-ranked United States-based manager for the [drug trafficking organization]." The heavy number of calls from the target telephone was consistent with narcotics trafficking and the high level of calls to Mexico suggested a "high level narcotics trafficker and money launderer who must communicate with his superiors in Mexico on a regular basis." Based on telephone records, it appeared that "Target Telephone #1" was being used by the holder of the previous target telephone or a close associate. Twenty-seven common numbers were dialed including nine numbers in Mexico.

According to Diederich, normal investigative techniques had failed or appeared unlikely to succeed. Using an informant would have been difficult because "members of large narcotics trafficking organizations usually, for the safety of the organization, generally will only deal in narcotics with individuals who they know and trust well, either through friends, family or close associates." Diederich also expressed concern that introducing an informant would alert members of the organization to an investigation. Finally, an informant would have difficulty learning the full extent of the conspiracy because persons involved in supply, transportation, and distribution of the narcotics often do not know each other and steps are used to retain this anonymity. At the time of the application, Diederich knew of "no individual who could introduce an undercover agent to anyone in the target organizations' hierarchy."

Physical surveillance of Rodriguez and the unidentified males was impossible because Diederich did not know their true identities. Limited surveillance was conducted at Leon's and Aceves's address but resulted in no useful information. Diederich knew of no locations to search. Because of time spent on "trivial errands" it is "highly likely that a surveillance team conducting blanket surveillance (unguided by telephone interceptions) would be detected by the subject prior to the pick up or delivery of any

significant amount of narcotics." A pen register would record telephone numbers called but would not assist in identifying the persons involved in the narcotics transactions. It was unlikely interviews would be successful because members of the organization were unlikely to provide such interviews for fear of jeopardizing their safety.

"Leaders of narcotics trafficking organizations often do not touch narcotics. Based on my training and experience, I believe that the only viable means by which to build a prosecutable case against Rodriguez, Aceves, Avelino [Leon], UM-1 and UM-2 and their associates is through the interception of communications made over the telephones the Target Subjects are using . . . ." (Capitalization omitted.) Diederich requested that three paragraphs be sealed to protect the life of a confidential informant, and that request was granted. Those paragraphs are not included in the record.

Diederich obtained an extension to wiretap No. 00-02 and other related applications for wiretaps are included in the record. We need not describe those applications in substantial detail because they are not the subject of appellants' arguments, except in Leon's argument that the extension to application for wiretap No. 00-02 is based on the first illegal wiretap.

Wiretap No. 00-04

This application concerned "Target Telephones #2, #3, #4, and #5" and two pagers. In this application the targets were Rodriguez, a.k.a. Leon, Aceves, Ramiro Murillo, John Doe #1, and John Doe #2. Diederich had learned that Leon was the "user" of "Target Telephone #1" based on intercepted conversations from that phone. Aceves was identified as the user of "Target Telephone #2." Based on information learned in the other wiretap, Diederich believed that Aceves worked for Leon and controlled Leon's stash locations.

Like the application for wiretap No. 00-02, this application described a large narcotics trafficking organization based in Mexico that shipped narcotics to Los Angeles. Conversations intercepted from "Target Telephone #1" reveal narcotics related conversations with "Target Telephones #2 to #5." This affidavit included additional information about the conspiracy than that provided in the prior affidavit because agents

had learned information from the interception of calls to and from "Target Telephone #1."

Based on the intercepted calls, Diederich directed the Pomona Police Department to "conduct wiretap-guided surveillance at Aceves's residence . . . ." (Capitalization omitted.) While under surveillance, Aceves drove to Kragen Auto Parts and met with Ramiro Murillo. There appeared to be a delivery of cocaine, but officers lost sight of the truck where they thought the cocaine was located and stopped surveillance because they were afraid they had been discovered.

In application No. 00-04, Diederich indicated other methods of investigation were not likely to succeed for many of the same reasons outlined in wiretap application No. 00-02. He explained that "the interceptions thus far have been helpful but have not sufficed to accomplish the goals of this investigation." Those goals included identifying the full scope of the narcotics trafficking organization.

Trial Court's Findings

The trial court denied the motion to suppress. It found that "[t]here are specific articulable facts; they are not just generic conclusions. They are fact specific in terms of the progress or lack of progress of the investigation, and they change based upon new developments." The court found "[t]here is no claim or allegation of omission or misrepresentation or even intentional or negligent falsehoods here."

The court followed *U.S. v. McGuire* (9th Cir. 2002) 307 F.3d 1192, stating that "the issue is whether . . . this is the type of conspiratorial group, conspiratorial nature here, which allows the government certain leeway regarding the necessity requirement. And *McGuire* has recognized that, and this court will recognize that the nature of this type of conspiracy, that is presented in these affidavits, is of such a conspiracy that it demands additional leeway on behalf of the government to continue its investigation."

DISCUSSION

The first section discusses appellants' privacy interests in their communications over the target telephones.[2] The second section focuses on the necessity requirement, part of the procedure for obtaining a court order authorizing a wiretap.

I. Appellants Had a Privacy Interest in Their Communications

It is undisputed that Leon obtained "Target Telephone #1" using the name Rodriguez. According to the Attorney General "appellant Leon could not show he had a reasonable expectation of privacy in a cell phone that was not even in his name."

A. Leon's Fourth Amendment Privacy Interest

The Fourth Amendment to the federal constitution protects only a reasonable expectation of privacy, which "by definition means more than a subjective expectation of not being discovered." (*Rakas v. Illinois* (1978) 439 U.S. 128, 143, fn. 12.) Society does not condone a reasonable expectation of privacy in criminal activity. (*People v. Cook* (1985) 41 Cal.3d 373, 384.) "[S]ubjective expectations of privacy that society is not prepared to recognize as legitimate have no [Fourth Amendment] protection." (*People v. Reyes (*1998) 19 Cal.4th 743, 751.) "A burglar plying his trade in a summer cabin during the off season may have a thoroughly justified subjective expectation of privacy, but it is not one which the law recognizes as 'legitimate' . . . his expectation is not 'one that society is prepared to recognize as "reasonable." ' " (*Rakas v. Illinois*, *supra*, 439 U.S. at pp. 143-144, fn. 12.) Similarly, a hotel guest using stolen identification to rent a room does not have a reasonable expectation of privacy in the hotel room. (*U.S. v. Cunag* (9th Cir. 2004) 386 F.3d 888, 894.)

---

[2] The parties discuss this as an issue of standing, but the high court has rejected that analysis. "[W]e think the better analysis forthrightly focuses on the extent of a particular defendant's rights under the Fourth Amendment, rather than on any theoretically separate, but invariably intertwined concept of standing." (*Rakas v. Illinois*, *supra*, 439 U.S. at p. 139.)

More analogous to this case, courts have held that the use of a false name renders unreasonable a person's expectation of privacy. For example, in *U.S. v. Melucci* (1st Cir. 1989) 888 F.2d 200, a defendant who used a false name to obtain a storage locker and who failed to pay rent had no legitimate expectation of privacy in the locker.[3] (*Id.* at p. 202.) Another court held a defendant had no legitimate expectation of privacy in a mailbox bearing someone else's name. (*United States v. Lewis* (8th Cir. 1984) 738 F.2d 916, 919-920, fn. 2.) "A mailbox bearing a false name with a false address and used only to receive fraudulently obtained mailings does not merit an expectation of privacy that society is prepared to recognize as reasonable." (*Ibid.*) The Fifth Circuit found questionable an argument that a defendant would have a legitimate privacy interest in a package addressed to him under an alias. (*U.S. v. Daniel* (5th Cir. 1993) 982 F.2d 146, 149.)

Conversely, the more recent case, *U.S. v. Pitts* (7th Cir. 2003) 322 F.3d 449 (*Pitts*), found that a defendant who uses an alias to send and receive mail does not forfeit his Fourth Amendment protections. "[T]he legitimate expectation of privacy does not depend on the nature of the defendant's activities, whether innocent or criminal." (*Id.* at p. 458.) "There is nothing inherently wrong with a desire to remain anonymous when sending or receiving a package, and thus the expectation of privacy for a person using an alias in sending or receiving mail is one that society is prepared to recognize as reasonable." (*Id.* at p. 459.)

Pitts distinguishes the alias user from the burglar or thief. The burglar or thief, by definition, engages in criminal conduct. In contrast, the person who uses an alias commits no inherent wrong. Legitimate reasons for use of an alias include the concern of the survivor of domestic violence to maintain safety, the apprehension of the victim of

---

[3] Arguably the failure to pay rent itself is sufficient to find that the defendant had no expectation of privacy in an area he was no longer renting. However, the court relied on both the use of a false name and the failure to pay rent.

identity theft in sharing information, the celebrity who “may wish to avoid harassment or intrusion; a government official [who] may have security concerns . . . .” (*Pitts*, *supra*, 322 F.3d at p. 458.) “The decision in favor of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one’s privacy as possible.” (*McIntyre v. Ohio Elections Comm’n* (1995) 514 U.S. 334, 341-342 [discussing anonymous authors].) Criminals do not “forfeit the privacy interests of all persons by using a confidential domain for nefarious ends.” (*Pitts*, *supra*, 322 F.3d at p. 458.)

Leon’s use of an alias to obtain a cell phone does not determine his reasonable expectation of privacy in his communications over that phone. While Leon may have committed fraud vis-à-vis the phone company, that does not foreclose him from raising a Fourth Amendment challenge.[4] (Cf. *U.S. v. Smith* (6th Cir. 2001) 263 F.3d 571, 587 [“The breach of the contract with Alamo [the car rental agency] does not foreclose [the defendant’s] standing to challenge a constitutional violation.”]; *U.S. v. Best* (8th Cir. 1998) 135 F.3d 1223, 1225 [driver not authorize by car rental agreement could assert a Fourth Amendment violation if authorized to drive by person who rented car]; but see *U.S. v. Riazco* (5th Cir. 1996) 91 F.3d 752, 754 [driver of rental car had no reasonable expectation of privacy when name not included on rental agreement].)

In the landmark case, *Katz v. United States* (1967) 389 U.S. 347 (*Katz*), the United States Supreme Court held that a person in a telephone booth is entitled to the protection of the Fourth Amendment. (*Id*. at p. 353.) “One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.” (*Id*. at p. 352.) “The Fourth Amendment governs not

---

[4] We assume Leon committed fraud. However, according to Diederich, the company sought no identification in issuing him the prepaid phone.

only the seizure of tangible items, but extends as well to the recording of oral statements, overheard without any 'technical trespass under . . . local property law.' " (*Id.* at p. 353, quoting *Silverman v. United States* (1961) 365 U.S. 505, 511.) Similarly, our high court has held "one who places a call from a public telephone booth can be seen and sometimes heard by passersby, but that does not permit the government to eavesdrop electronically on the conversation without a search warrant." (*People v. Cook* (1985) 41 Cal.3d 373, 380 (*Cook*).)

Just as in *Katz* and *Cook* where the defendants had reasonable expectations of privacy in their communications made in a phone booth, Leon had a reasonable expectation of privacy in his conversations made over a cell phone would be private. The expectation of privacy in the contents of telephone conversations does not become unreasonable just because the phone was procured using an alias.[5]

B. Leon's Statutory Privacy Interest

The Attorney General focuses only on the Fourth Amendment in arguing that Leon cannot challenge the wiretap. " 'In general, relevant evidence that is illegally obtained under California law is nonetheless admissible, so long as federal law does not bar its admission. [Citations.]' " (*People v. Zepeda* (2001) 87 Cal.App.4th 1183, 1194, quoting *People v. Hines* (1997) 15 Cal.4th 997, 1043-1044.) However, section 629.72 provides an alternate test. It allows a person to move to suppress the intercepted communication "on the basis that the contents or evidence were obtained in violation of

---

[5] Citing legal authority for the proposition that "a defendant who disclaims possession of an object . . . [cannot] take a contrary position in an effort to attain standing to seek to exclude that object from evidence," (*People v. Dasilva* (1989) 207 Cal.App.3d 43, 48), the Attorney General argues that Leon "attempted to disassociate himself" from the cell phone by using a false name. The authority cited by the Attorney General is inapposite. This is not a case where a defendant has expressly denied ownership of an item and then subsequently inconsistently claimed ownership in the same item. For the same reason *United States v. Hawkins* (11th Cir. 1982) 681 F.2d 1343, a case finding no privacy interest in suitcase defendant disclaimed, is not helpful.

the Fourth Amendment of the United States Constitution *or of this chapter.*" (Italics added.) If an application for a wiretap is granted without meeting the core requirements of the chapter, the evidence must be suppressed. (Cf. *People v. Jackson* (2005) 129 Cal.App.4th 129.)

In arguing that this statutory language is irrelevant, the Attorney General cites *In re Lance W.* (1985) 37 Cal.3d 873, 879, for the following proposition: California Constitution, article I, section 28, subdivision (d), enacted by the voters on June 8, 1982, "abrogated both the 'vicarious exclusionary rule' under which a defendant had standing to object to the introduction of evidence seized in violation of the rights of a third person, and a defendant's right to object to and suppress evidence seized in violation of the California, but not the federal, Constitution." The Attorney General's reliance on Article I, section 28(d), enacted is misplaced.

By its own terms, that provision does not apply to legislation "hereafter enacted by a two-thirds vote of the membership in each house of the Legislature . . . ." (Cal. Const., art. I, § 28, subd. (d).) Article I, section 28, subdivision (d) was passed in 1982. In 1985, the prohibition against wiretapping in section 632 was reenacted by two-thirds of the Legislature. (California Legislature, 1985-1986 Regular Session, Senate Final History p. 965.)

Then in 1995, section 629.72 was enacted by more than a two-thirds majority in each house. (California Legislature, 1995-1996 Regular Session, Senate Final History, p. 703.) Thus, subsequent to the passage of article I, section 28, subdivision (d), the Legislature has, by more than a two-thirds majority in each house, reaffirmed the prohibition on wiretaps and created rules regulating motions to suppress statements obtained by a wiretap. The admission of evidence is therefore governed by section 629.72 in addition to the Fourth Amendment.

Leon had a privacy interest in the contents of his conversation under California law. In California, a strong public policy favors maintaining privacy of cell phone communications. The United States Supreme Court recognized California's prohibition against eavesdropping established in 1862 when it held that the Fourth Amendment

standards applied to a statute allowing law enforcement to eavesdrop on private communications. (*Berger v. New York*, *supra*, 388 U.S. at p. 45.) The California Legislature determined that "advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." (§ 630.) No exception to the prohibition on wiretapping is premised on the name used to procure the device for which the wiretap is sought. (§ 632.6.) Absent a court order, government agents were not permitted to listen to Leon's conversations even though Leon used the name Rodriguez to purchase the cell phone.[6]

C. Aceves's Privacy Interest

Aceves argues that his privacy interest in "Target Telephone #1" was violated because he was a party to the telephone conversations. As the Attorney General argues, Aceves forfeited this claim by failing to raise it at the suppression hearing.[7]

---

[6] The exception to the prohibition on wiretapping made to ease law enforcement investigations was codified in 1988, after 18 years of failed legislation. The Legislative history indicates that similar bills had been introduced every year beginning in 1970. (Assembly Committee on Public Safety, Supplemental Analysis SB 83 March 21, 1988.) The Attorney General at that time, John Van De Kamp, in an effort to persuade the Governor to sign the legislation described it as "carefully designed to give the public greater protection against serious crime while preventing any potential abuse by law enforcement." (Letter to George Deukmejian May 19, 1988, p. 4.) The law enforcement exception to the prohibition against wiretap remains viable and has been expanded to parallel federal law. (*People v. Zepeda* (2001) 87 Cal.App.4th 1183, 1195.)

[7] In the trial court, counsel for Aceves based his claim on the fact that there were allegations of a conspiracy. However, the United States Supreme Court has made clear that Fourth Amendment rights are personal rights. (*Alderman v. United States*, *supra*, 394 U.S. at pp. 171-172.)

Nevertheless, in order to forestall a claim of ineffective assistance of counsel, we consider Aceves's argument on the merits.

"A defendant who believes the information was 'obtained in violation of the Fourth Amendment of the United States Constitution or of this chapter' may move to suppress its use at trial under section 629.72." (*People v. Jackson*, *supra*, 129 Cal.App.4th at p. 145.) Section 629.72 is broadly worded allowing "[a]ny person in any trial, hearing or proceeding" to "move to suppress some or all of the contents of any intercepted . . . electronic cellular telephone communications . . . ." "Any person" includes Aceves.

Even under the more narrow test of the Fourth Amendment, Aceves had a reasonable expectation of privacy in the conversations in which he was a participant. "Those who converse and are overheard . . . also have a valid objection [under the Fourth Amendment] unless the owner of the premises has consented to the surveillance [by the government]." (*Alderman v. United States* (1967) 394 U.S. 165, 179, fn. 11.) Under California law, the "term 'confidential communication' includes any communication carried on in circumstances as may reasonably indicate that *any party* to the communication desires it to be confined to the parties thereto . . . ." (§ 632, subd. (c), italics added.) For the same reason, Aceves had a privacy interest in his communications over "Target Telephone #2."

II. The Issuing Court Did Not Abuse Its Discretion in Finding Necessity for the Wiretaps

In order to authorize a wiretap, a court must find that "[n]ormal investigative procedures have been tried and have failed or reasonably appear either to be unlikely to succeed if tried or to be too dangerous." (§ 629.52, subd. (d).) The "necessity" requirement is "designed to assure that wiretapping is not resorted to in situations where traditional investigative techniques would suffice to expose the crime." (*United States v. Kahn* (1974) 415 U.S. 143, 153, fn. 12.) It also is designed to limit wiretaps, an intrusive method of investigation. (*U.S. v. Bennett* (9th Cir. 2000) 219 F.3d 1117, 1121.)

Leon argues the government improperly used wiretaps as an initial investigatory step, and the affidavits reveal no use of normal investigative procedures. He argues that

the affidavits fail to provide specific grounds why a particular investigative technique would fail or be too dangerous. "[T]he purpose of the wiretap statute is not to make an investigator's life easier, or less expensive, it is to be available only when normal investigative procedures have already failed, are too dangerous, or not reasonably likely to work." Leon faults Diederich's affidavits for failing to discuss the use of helicopters and airplanes which according to him are "common place in 'serious' (or even less serious investigations) . . . ."

Aceves argues that wiretap application No. 00-02 contains boilerplate descriptions, that the officers were aware of Aceves's identity and could have conducted additional surveillance that "would have been more fruitful in due time." Aceves also argues that the fact surveillance produced evidence of a meeting between him and another suspected drug dealer shows that a wiretap was not necessary.

Appellants rely heavily on *U.S. v. Blackmon* (9th Cir. 2001) 273 F.3d 1204, 1206 (*Blackmon*.) The Attorney General argues both that *Blackmon* is distinguishable and that this court should follow *U.S. v. McGuire*, *supra*, 307 F.3d 1192. While neither *Blackmon* nor *McGuire* is binding, the federal cases assist in applying California law, which is modeled after federal law. (*People v. Zepeda*, *supra*, 87 Cal.App.4th at p. 1196.)

In *Blackmon*, *supra*, 273 F.3d 1204, the majority held that "wiretap evidence should be suppressed because the wiretap application contained material misstatements and omissions, and because the application does not otherwise make a particularized showing of necessity." (*Id*. at p. 1206.) Blackmon lived in a housing project with another suspect, Miller. The FBI investigated Miller for six months using traditional investigative techniques and then applied for a wiretap application. (*Id.* at p. 1206.) Without conducting further investigations other than trap and trace devices and pen registers, the FBI applied for a wiretap of Blackmon.

The court found that several statements in the Blackmon wiretap application applied to Miller but not to Blackmon. "The record is clear that no surveillance that the government attempted against Blackmon ever failed." (*Blackmon*, *supra*, 273 F.3d at p. 1208.) Thus, the statement in the affidavit that " 'on several occasions, law

enforcement surveillance teams were compromised in an attempt to conduct surveillance operations on Blackmon and associates' " was false. (*Ibid*.) The statement that informants possessed only limited knowledge also was "untrue." (*Ibid*.) The government had conceded that "one informant had special access to Blackmon and had in fact seen him 'cooking' cocaine in his apartment. Furthermore, the informants knew the sources of the narcotics and the locations where the narcotics were stored and had participated in numerous controlled purchases of narcotics from Blackmon." (*Id*. at p. 1209.) The majority then concluded that, if "purged" of the misstatements, the affidavits failed to show necessity. (*Id.* at p. 1210.)

U.S. v. McGuire, *supra*, 307 F.3d 1192, involved the Montana Freemen, a group hostile to the United States government. (*Id.* at p. 1195.) The court found no abuse of discretion in determining necessity. (*Id.* at p. 1197.) "FBI agents could not have conducted on-site surveillance of the Freemen property because of its remote, rural location and group members' alertness to law enforcement activities, which created grave dangers. Agents also would have faced risks in executing any search warrant at the compound, because of the group's known violent propensity and undisputed possession of assault weapons. Federal agents would have had difficulty infiltrating the group with FBI informants, as a result of the Montana Freemen's close-knit nature. Interviewing witnesses would have helped little, as the only persons knowledgeable about the content of the defendants' transactions were the defendants themselves, and the defendants had limited incentive to cooperate. Although three witnesses were cooperating with the FBI when it applied for wiretapping authority, those witnesses were able to give agents only limited information, not including the names of all members of the conspiracy." (*Id.* at p. 1197.) The court also stressed that the wiretap was necessary to avoid jeopardizing the lives of the investigating agents. (*Ibid*.)

"Just as important as these practical considerations, however, was the nature of the entity the government was investigating. The law has long recognized that conspiracies pose a greater threat to society than individual action toward the same end." (*U.S. v. McGuire*, *supra*, 307 F.3d at p. 1197.) "Like the Hydra of Greek mythology, the

conspiracy may survive the destruction of its parts unless the conspiracy is completely destroyed. For even if some or many conspirators are imprisoned, others may remain at large, free to recruit others eager to break the law and to pursue the conspiracy's illegal ends." (*Id.* at pp. 1197-1198.) The court found these principles to be particularly applicable to a case where the goals of the conspiracy were the overthrow of the government and the conspirators were armed with deadly weapons. (*Id.* at p. 1198.) "The threat posed by the Montana Freemen was grave, so the FBI was entitled to ample leeway to investigate it." (*Ibid.*)

Both *Blackmon* and *McGuire* hold that an application for a wiretap must include a full statement regarding necessity and must "recite facts indicating that 'normal investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous.' " (*U.S. v. McGuire*, *supra,* 307 F.3d at p. 1196; *Blackmon*, *supra*, 273 F.3d at p. 1207.) This principle is consistent with California law. (*People v. Zepeda*, *supra*, 87 Cal.App.4th at p. 1195.) Many distinctions between *Blackmon* and *McGuire* are easily harmonized. While *Blackmon* found several material misstatements in the affidavit supporting the wiretap application, *McGuire* found no similar misstatements and therefore accepted the information in affidavits as reliable for purposes of assessing necessity. In *Blackmon*, the court was troubled by "boilerplate assertions" true of most narcotics investigation, whereas in *McGuire*, the court underscored the uniqueness of the conspiracy described in the affidavits supporting the wiretap. (*U.S. v. McGuire*, *supra*, 307 F.3d at p. 1198; *Blackmon*, *supra*, 273 F.3d at pp. 1210-1211.)

It is more difficult to reconcile *McGuire*'s holding that conspiracies pose a greater threat to society, and therefore, law enforcement should have greater leeway in investigating them (*U.S. v. McGuire*, *supra*, 307 F.3d at p. 1198) with the rule implicitly followed in *Blackmon* that "[a] suspicion that a person is a member of a conspiracy . . . is not a sufficient reason to obtain a wiretap." (*U.S. v. Carneiro* (9th Cir. 1988) 861 F.2d 1171, 1181.) The trial court erred in following *McGuire* to find that because this case

involved a conspiracy to smuggle narcotics, the government was entitled to greater leeway in its investigation.

Procedural restrictions on wiretaps were implemented to avoid violations of the Fourth Amendment found in *Berger v. New York*, *supra*, 388 U.S. at p. 87, a case where a wiretap was used to crack a conspiracy. (*U.S. v. Carneiro*, *supra*, 861 F.2d at p. 1175.) "The need for particularity and evidence of reliability in the showing required when judicial authorization of a search is sought is especially great in the case of eavesdropping. By its very nature eavesdropping involves an intrusion on privacy and is broad in scope." (*Berger v. New York*, *supra*, 388 U.S. at p. 56.) In considering the argument that eavesdropping is an important technique of law enforcement, the high court concluded that "we cannot forgive the requirements of the Fourth Amendment in the name of law enforcement." (*Id.* at p. 62.) "Few threats to liberty exist which are greater than that posed by the use of eavesdropping devices." (*Id.* at p. 63.) Additionally, under section 629.50, necessity must be shown in all cases regardless of the nature of the crime being investigated.

Although the trial court erred in concluding that the "nature of this type of conspiracy" loosened the necessity requirement, there is no need to remand for the trial court to determine whether the issuing court abused its discretion in finding necessity. (*People v. Zepeda*, *supra*, 87 Cal.App.4th at p. 1204; *United States v. Brone* (1986) 792 F.2d 1504, 1506 [issuing judge's decision that wiretaps were necessary is reviewed for abuse of discretion].)[8] Appellants presented no evidence that Diederich's statements

---

[8] In *People v. Zepeda*, *supra*, 87 Cal.App.4th at p. 1204, the court stated that the "trial court's determination that the 'necessity' requirement was met is reviewed for abuse of discretion." The authority *Zepeda* cites for this proposition indicates that the review of the issuing judge's decisions is for abuse of discretion because it is the issuing judge who has discretion. (See *U.S. v. Bennett*, *supra*, 219 F.3d at p. 1121; *U.S. v. Carneiro*, *supra*, 861 F.2d at p. 1176.)

were inaccurate, and therefore this court is in the same position as the trial court to review the issuing court's necessity determination.

Appellants have shown no misrepresentations similar to those in *Blackmon*. While appellants argue that the government had other investigatory tools available to them, with the exception of the use of airplanes, the affidavits explain why these tools are not likely to be helpful in conducting the investigation. The affidavits for wiretaps Nos. 00-02 and 00-04 explain the difficulty in penetrating the conspiracy with an informant and the limited progress made by the informants who had been used. Diederich also described concerns for alerting the suspects of the investigation such as through constant surveillance and the use of search warrants. The affidavit in support of wiretap No. 00-04 indicated that surveillance efforts were discovered and jeopardized the investigation. Even though additional surveillance may have assisted the investigation as appellants speculate, the issuing court did not abuse its discretion in determining that the government established necessity because the affidavits explain why such additional blanket surveillance would jeopardize the investigation. (See *U.S. v. Iiland* (10th Cir. 2001) 254 F.3d 1264, 1268 [wiretap proper where "increased visual surveillance would have increased the possibility of detection"].) The government is not required to exhaust every conceivable technique in order to show necessity for a wiretap. (*U.S. v. Bennett*, *supra*, 219 F.3d at p. 1122; *U.S. v. Iiland*, *supra*, 254 F.3d at p. 1268.)

As appellants argued, " 'Bald conclusory statements without factual support are not enough.' " (*U.S. v. Commito* (9th Cir. 1990) 918 F.2d 95, 97, quoting *United States v. Martinez* (9th Cir. 1978) 588 F.2d 1227, 1231.) " ' "[T]he affidavit [read in its entirety] must show with specificity why in this particular investigation ordinary means of investigation will fail." ' " (*Ibid.,* italics omitted, quoting *United States v. Ippolito* (9th Cir. 1985) 774 F.2d 1482, 1486, quoting *United States v. Robinson* (D.C. Cir. 1983) 698 F.2d 448, 453.) However, contrary to appellants' assertions, Diederich's affidavits were not simply boilerplate descriptions of large narcotics conspiracies. They specifically described the conspiracy under investigation and the need for a wiretap. The two affidavits involve efforts to investigate the same conspiracy and are similar. But the

information in support of wiretap No. 00-04 includes information learned in the course of the investigation.[9] Neither appellant has demonstrated the issuing court abused its discretion in determining the wiretaps were necessary.

DISPOSITION

The order denying appellants' motions to suppress is affirmed.

CERTIFIED FOR PUBLICATION

COOPER, P.J.

We concur:

RUBIN, J.

BOLAND, J.

---

[9] Because the initial permission to intercept communications was valid, there is no merit to Leon's claim that communications obtained in the extension order are the product of an initial improper interception and there is no need to consider the parties' dispute whether *United States v. Leon* (1984) 468 U.S. 897 is applicable in this context.