

FOR PUBLICATION
UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,
Plaintiff-Appellee,
v.
JORGE ORTIZ OLIVA, AKA Jorge
Cortez Almonte, AKA Jorge
Meras Barajas,
Defendant-Appellant.

No. 10-30126
D.C. No.
3:07-cr-00050-BR-1

UNITED STATES OF AMERICA,
Plaintiff-Appellee,
v.
PABLO BARAJAS LOPEZ,
Defendant-Appellant.

No. 10-30134
D.C. No.
3:07-cr-00050-BR-5
OPINION

Appeal from the United States District Court
for the District of Oregon
Anna J. Brown, District Judge, Presiding

Argued and Submitted
November 18, 2011*—Portland, Oregon

Filed July 20, 2012

*The panel unanimously concluded that *United States v. Lopez*, No. 10-30134, was suitable for decision without oral argument. *See* Fed. R. App. P. 34(a)(2).

Before: Raymond C. Fisher, Richard A. Paez and
Richard R. Clifton, Circuit Judges.

Opinion by Judge Fisher

COUNSEL

Robert M. Stone (argued), Medford, Oregon, for appellant Jorge Ortiz Oliva.

Marc Friedman, Eugene, Oregon, for appellant Pablo Barajas Lopez.

Dwight C. Holton, United States Attorney, Kathleen Bickers (argued), Assistant U.S. Attorney, Portland, Oregon, for the appellee.

OPINION

FISHER, Circuit Judge:

Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended, 18 U.S.C. §§ 2510-2522, governs interception of wire, oral and electronic communications. Jorge Ortiz Oliva appeals the district court's denial of his motion to suppress evidence obtained from a series of electronic surveillance orders authorizing interception of communications over cellular phones associated with him and his alleged co-conspirators.¹ Oliva contends these orders by their terms authorized more than "standard" intercepts, permitting more intrusive "roving" intercepts without meeting the statu-

¹Pablo Barajas Lopez joined Oliva's suppression motion in the district court and he joins Oliva's appeal here. For the purposes of this opinion, we analyze the motion as it pertains to Oliva. Our analysis and rulings as to the standing issue and the merits, however, apply to both appellants.

tory prerequisites of § 2518(11).² Specifically, he contends that the orders in essence authorized the government to transform the cellular phones into roving electronic bugs through use of sophisticated eavesdropping technology. We agree that if the government seeks authorization for the use of new technology to convert cellular phones into “roving bugs,” it must specifically request that authority, the court must scrutinize the need for such surveillance and the authorization orders must be clear and unambiguous. In this case, however, we credit the district court’s finding that the orders were intended only to authorize standard interception techniques and the government did not do otherwise, and we therefore reject Oliva’s argument. We also reject Oliva’s related argument that the surveillance applications and orders failed to meet the specification requirements of § 2518 to qualify even as standard intercepts. We therefore affirm the district court’s denial of Oliva’s motion to suppress.

BACKGROUND

In January 2006, the Drug Enforcement Agency began investigating a drug trafficking conspiracy involving numerous participants, including Oliva and Lopez. In August 2006, and over the course of the next 10 months, the government obtained a series of 30-day electronic surveillance orders that authorized the monitoring of 23 cellular phones used by 10 persons, nine of whom, including Oliva and Lopez, ultimately became defendants in the underlying criminal proceeding.

In February 2007, the government indicted Oliva, Lopez and multiple alleged co-conspirators for their participation in a drug trafficking conspiracy involving the distribution of methamphetamine, cocaine and marijuana. A jury convicted Oliva and Lopez of all drug counts in October 2009. They have raised various issues on appeal, but here we deal only

²All citations to §§ 2510 and 2518 will refer to 18 U.S.C. §§ 2510 and 2518 respectively, unless otherwise noted.

with Oliva's appeal of the district court's denial of his pretrial motion to suppress evidence obtained from the surveillance orders.³

Specifically, Oliva argues that the surveillance orders improperly authorized roving intercepts and failed to meet the statutory specification requirements, and were thus facially invalid. He raises questions about interception of communications over cellular phones, whose technology differs from conventional land line phones.

DISCUSSION

I. STANDING

As a preliminary matter, we reject the government's contention that Oliva lacks standing to challenge the interceptions because he has neither admitted that the voices in the conversations intercepted were his nor asserted that any of the intercepts took place on his premises. We review a defendant's standing under § 2518 de novo. *See Vaughn v. Bay Envtl. Mgmt., Inc.*, 567 F.3d 1021, 1024 (9th Cir. 2009) (holding that questions of statutory standing are reviewed de novo).

[1] Under federal law, any "aggrieved person" has standing to bring a motion to suppress the contents of intercepted wire or oral communications or evidence derived therefrom. § 2518(10)(a). An "aggrieved person" means a person "who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed." § 2510(11) (emphasis added); *see Alderman v. United States*, 394 U.S. 165, 173 (1969) ("In order to qualify as a person aggrieved by an unlawful search and seizure one must [be] . . . one against whom the search was directed." (quoting *Jones v. United States*, 362 U.S. 257, 261 (1960)))

³We address Oliva's and Lopez's remaining challenges to their convictions and sentences in a concurrently filed memorandum disposition.

(internal quotation marks omitted)); *see also In re Flanagan*, 533 F. Supp. 957, 960 (E.D.N.Y. 1982) (“In the context of wiretapping, the rule has crystalized that the only persons with standing to suppress the fruits of an illegal wiretap are parties at whom the wiretaps were directed, parties to the call that was intercepted, or parties owning the premises where the conversations were intercepted.”), *aff’d in relevant part, In re Grand Jury Subpoena of Flanagan*, 691 F.2d 116, 118 n.2 (2d Cir. 1982). A person named in a surveillance order as the subject of the surveillance thus has standing to challenge the warrant’s sufficiency. *See* 2 James Carr & Patricia L. Bellia, *The Law of Electronic Surveillance* § 6:16 (2012) (“As a general rule, courts limit standing to those individuals whose personal privacy has been breached. No standing exists unless the individual shows either a possessory interest in the site, he was overheard *or named in the order*, or had a reasonable expectation of privacy that was breached.” (emphasis added)).

[2] Oliva was one of the individuals against whom the interceptions were directed. The affidavits in support of the surveillance orders included descriptions of Oliva as a suspect and investigators’ statements certifying their beliefs that he was using the individual cellular phones at issue. Oliva was specifically named as a “subject” of the investigation, and his conversations were the target of the surveillance. We therefore hold that Oliva has standing.

II. SUFFICIENCY OF THE ELECTRONIC SURVEILLANCE ORDERS

We turn to the language of the surveillance orders at issue. As we shall explain, we agree with Oliva that certain terminology in the orders is problematical in the context of cellular phones. Nonetheless, we disagree that the orders must be construed as having authorized improper roving bugs, requiring suppression of the intercepted evidence. We also reject Oliva’s argument that the orders were facially invalid for failure to meet the statutory specification requirements.

A. Standard and Roving Intercepts

[3] Federally authorized interception of wire, oral and electronic communications is governed by Title III of the Omnibus Crime Control and Safe Streets Act of 1968. Title III “ties wiretap authority to specific communications facilities or locations.” *United States v. Hermanek*, 289 F.3d 1076, 1086 (9th Cir. 2002). To obtain authorization for what is commonly known as a “*standard*” *intercept*, the statute requires the government to include in its application, as relevant here, “a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted.” § 2518(1)(b)(ii). The court must “determine[] on the basis of the facts submitted by the applicant that . . . (d) . . . there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.” § 2518(3)(d). The court’s order in turn must specify “the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted.” § 2518(4)(b).⁴

[4] When the government cannot meet the specification requirements of § 2518(1)(b)(ii) and (3)(d), it may still obtain authorization for a different type of intercept — known as a “*roving*” *intercept* — if it can satisfy enhanced authorization

⁴The statute has been understood to apply to both land line phones and cellular phones. Although the “nature and location” of a cellular phone cannot be described in the same way as that of a land line phone, a cellular phone is itself a “facilit[y]” that can be sufficiently identified by such features as its telephone number, electronic serial number (ESN) or international mobile subscriber identity number (IMSI). See *United States v. Goodwin*, 141 F.3d 394, 403 (2d Cir. 1997) (holding that the government’s affidavits met the requirements of § 2518 because they “clearly identified the facilities to be tapped by their telephone numbers and by their electronic serial numbers”).

requirements. *See* § 2518(11). There are two distinct types of roving intercepts.

The first type is a “roving bug,” used to intercept *oral* communications. *See* § 2510(2) (defining “oral communication”). To justify a roving bug, the government must set forth a “full and complete statement as to why . . . specification is not practical,” and it must identify “the person committing the offense and whose communications are to be intercepted.” § 2518(11)(a)(ii). A roving bug permits “interception of [a subject’s] conversations at locations that were ‘not practical’ to specify” in the applications and orders. *United States v. Tomero*, 462 F. Supp. 2d 565, 567 (S.D.N.Y. 2006).

The second type is a “roving wiretap,” used to intercept *wire* communications. *See* § 2510(1) (defining “wire communication”). For a roving wiretap, the government must not only identify “the person believed to be committing the offense and whose communications are to be intercepted,” but also make “a showing that there is probable cause to believe that the person’s actions could have the effect of thwarting interception from a specified facility.” § 2518(11)(b)(ii).⁵ We have explained that “[r]oving wiretaps are an appropriate tool to investigate individuals” who use different telephone booths or “change numbers frequently to avoid detection.” *Hermanek*, 289 F.3d at 1087.

B. Nature of the Orders Here

Beginning in August 2006, the government sought and obtained a number of orders permitting surveillance of cellular phones associated with Oliva, Lopez and other subjects of the government’s investigation. Each order authorized the government to intercept “wire communications” to and from

⁵Sections 2518(11)(a)(i) and (b)(i) also require special levels of approval from federal officials, beyond the approval required to obtain standard intercepts.

certain target phones and phone numbers. Oliva argues that language in each order actually gave the government broader authority, transforming the orders from standard intercepts into authorizations for roving bugs or roving wiretaps.

First, the orders authorized interception of “background conversations intercepted in the vicinity of Target Phones 1 and 2 while the telephone is off the hook or otherwise in use.”⁶ According to Oliva, this language authorized roving bugs. Second, the orders authorized interception not only of the target phone numbers but also of “any changed telephone number or any other telephone number subsequently assigned to or used by the instrument bearing the same ESN and/or IMSI as the Target Phones 1 and 2 within the thirty (30) day period.” Oliva reads this as authorizing roving wiretaps.

Oliva moved in the district court to suppress evidence obtained pursuant to the orders, contending that each warrant on its face was invalid because the government had failed to comply with the enhanced requirements for roving intercepts under § 2518(11)(a) and (b). The government conceded it did not meet the enhanced requirements, but argued it was not required to do so because it had not requested, and the orders did not authorize, the use of roving intercepts.

The district court rejected Oliva’s challenge, finding that the orders did not authorize “roving bug[s] within the meaning of the statute” or “roving wiretap[s],” and denied the motion to suppress. We review *de novo* the denial of a motion to suppress. *See United States v. Lynch*, 367 F.3d 1148, 1159 (9th Cir. 2004). We review the court’s underlying findings for clear error. *See United States v. Davis*, 530 F.3d 1069, 1077 (9th Cir. 2008).

⁶Each surveillance order applied to between one and five target phones specified in the order. For the purposes of this opinion, because all orders contained the same language, we cite to the order pertaining to “Target Phones 1 and 2.” Our analysis, however, applies to all of the orders.

1. Authorization to Intercept “Background Conversations” While the Telephone is “Off the Hook or Otherwise in Use”

The surveillance orders authorized the government to tap “background conversations intercepted in the vicinity of [a target phone number] while the telephone is off the hook or otherwise in use.”⁷ Oliva asserts that this language, as applied to cellular phones, authorized the government to intercept “background communications when the cell phones were powered on but not actively engaged in a call.” He contends such authority allowed the government to employ advanced technology to convert the targeted cellular phones into general listening devices, picking up any conversations within the range of the phone even when it was not actively in use during a telephone conversation. According to Oliva, by authorizing such technology each order permitted use of a roving bug.

Oliva’s argument rests on his claim that law enforcement authorities have the technology to transform cellular phones into listening devices — i.e., roving bugs — that record ambient conversations even when the user thinks the phone is “off.” Whether, and to what extent, this technology exists is not clear. In the district court, Oliva produced a December 1, 2006 article from CNET News entitled, “FBI taps cell phone mic as eavesdropping tool.” The article reports that “[t]he FBI appears to have begun using a novel form of electronic surveillance in criminal investigations: remotely activating a

⁷The 2011 U.S. Attorneys’ Manual includes the terminology used in these orders, specifying that an application for electronic surveillance “[w]ith regard to a cellular telephone” should “request that the authorization apply to background conversations intercepted in the vicinity of the target phone while the phone is off the hook or otherwise in use. See *United States v. Baranek*, 903 F.2d 1068 (6th Cir. 1990).” U.S. Attorneys’ Manual, Criminal Resource Manual 28, available at http://www.justice.gov/usao/eousa/foia_ing_/usam/title9/crm00028.htm (last visited July 13, 2012).

mobile phone's microphone and using it to eavesdrop on nearby conversations." According to the article, the technique, described as a roving bug, "came to light" in *Tomero*, 462 F. Supp. 2d 565, a 2006 case from the Southern District of New York. *Tomero* referred to the "installation of a listening device in [a] cellular telephone. The device functioned whether the phone was powered on or off, intercepting conversations within its range wherever it happened to be." *Id.* at 567 (footnote omitted). The CNET article also referred to a 2005 report from *Financial Times* describing a possibly related technology. The *Financial Times* article reported that, "[i]f ordered to do so, mobile telephone operators can . . . tap any calls, but more significantly they can also remotely install a piece of software on to any handset, without the owner's knowledge, which will activate the microphone even when its owner is not making a call, giving security services the perfect bugging device." Mark Odell, *Use of Mobile Helped Police Keep Tabs on Suspect and Brother*, *Fin. Times*, Aug. 2, 2005, available at <http://www.ft.com/intl/cms/s/0/4239e29e-02f2-11da-84e5-00000e2511c8.html> (last visited July 13, 2012). Without resolving whether this technology exists, the district court rejected Oliva's theory.

The language of the orders is susceptible to Oliva's interpretation. The terminology — "background conversations intercepted in the vicinity of [a target phone number] while the telephone is off the hook or otherwise in use" — could encompass the use of the alleged technology described by Oliva. But the government's interpretation, accepted by the district court, is equally if not more plausible: the intent was to authorize interception of background conversations overheard while the cellular phones were actually being used to communicate. The government represented and the district accepted that no evidence was detected or offered that came from "background conversations from cellular telephones that were powered on, but not connected to . . . a live call."

The terminology “off the hook” is problematical, however, when applied to cell phones, the term having been borrowed from orders concerning land lines, for which the concept has meaning because land line phones typically have hooks, referred to as switch hooks.⁸ “The hook switch is used to connect or disconnect the receiver and transmitter from the line.” Cyril M. Jansky & Daniel C. Faber, *Principles of the Telephone* 5 (1916). When the receiver is “on the hook,” its weight pulls the switch down and holds the receiver circuit open, leaving the line free for signaling purposes. *Id.* at 72. When the receiver is “off the hook,” the switch hook raises and closes the receiver circuit to incoming calls, so that the line can be used for communication. *Id.* Judicial decisions talking about telephones being off the hook have involved traditional land line technology, referring to the situation in which a receiver is off the hook and a telephone call is not necessarily in progress. *See, e.g., United States v. Baranek*, 903 F.2d 1068, 1069 (6th Cir. 1990) (concerning a conversation recorded by agents after the phone line “stayed open” because the defendant had “neglected to replace the telephone properly”); *United States v. Willoughby*, 860 F.2d 15, 18 (2d Cir. 1988) (concerning a conversation that was “automatically recorded” because it “took place while [the defendant] was holding the . . . telephone’s handset off the hook”); *United States v. Blanco*, No. 93-CV-20042, 1994 WL 695396, at *8 (N.D. Cal. Dec. 8, 1994) (upholding an order authorizing law enforcement to intercept from a land line “background conversations . . . in the vicinity of the target telephone while the telephone is off the hook or otherwise in use”); *United States v. Feola*, 651 F. Supp. 1068, 1107 (S.D.N.Y. 1987) (upholding an order allowing “interception of conversations had in

⁸*See Definition of: switch hook*, PC Magazine, available at http://www.pcmag.com/encyclopedia_term/0,1237,t=hook+switch&i=52310,00.asp (last visited July 13, 2012) (“Definition of: switch hook. Also called a ‘hook switch,’ it is the control mechanism that answers and hangs up a call on a telephone. When you place the handset in the telephone cradle, it depresses the switch hook’s button and hangs up (puts the phone ‘on hook’).”).

[the defendant's] apartment while his telephone was off the hook").

The "off the hook" language, however, lacks meaning when applied to cellular phones. Terminating a call on a cellular phone does not turn the phone completely off. To do so requires a separate and more deliberate step that the user may not appreciate is necessary, and may leave the cellular phone open to electronic eavesdropping quite different from what can occur with accidentally failing to hang up a land line phone. Unlike a relatively stationary land line phone, a cellular phone whose microphone remains on even though the call is terminated becomes a truly "roving bug." If that is what the government's application for a warrant actually seeks, it cannot do so using arcane, outmoded terminology like "off the hook."

[5] Title III makes clear that the government cannot obtain — nor may courts approve — electronic surveillance orders by using ambiguous terminology that can be misconstrued to authorize interception of communications beyond what is intended. Before the government can employ technologies that can eavesdrop on background conversations even if the cell phone is "off" — essentially converting the phone to a bugging device — it would have to comply with the statutory requirements for such intrusive surveillance. That means specifically requesting such authority, the court scrutinizing the need for it and the order authorizing the surveillance in clear and unambiguous terms with respect to the use of the technology permitted and its boundaries. *See* § 2518(1) ("Each application for an order authorizing or approving the interception of a wire, oral, or electronic communication . . . shall include . . . (b) . . . (iii) a particular description of the type of communications sought to be intercepted"); § 2518(3)(c) (requiring the court to determine that other investigative procedures are inadequate); § 2518(4) ("Each order authorizing or approving the interception of any wire, oral, or electronic communication under this chapter shall specify . . . (c) a particular

description of the type of communication sought to be intercepted”).⁹ *Cf. United States v. Jones*, 132 S. Ct. 945, 951 n.3 (2012) (noting that Fourth Amendment analysis remains the same irrespective of “[w]hatever new methods of investigation may be devised”); *Kyllo v. United States*, 533 U.S. 27, 36 (2001) (noting that when considering the effect of technology on Fourth Amendment rights, we must adopt rules that “take account of more sophisticated systems that are already in use or in development”).

[6] In this case, notwithstanding the opportunity for abuse that the orders’ ambiguous language may have afforded the government, the government disavowed that it intended to or did obtain evidence that came from other than direct or background conversations while the cellular phones were being used for conversations. There is no showing that the district court clearly erred in accepting those representations. We therefore decline to adopt Oliva’s broader reading of the disputed language as having authorized the government to utilize unlawful roving bugs. Even if the language might be construed as having done so, there is no showing the evidence Oliva seeks to suppress resulted from such surveillance.

2. *Authorization to Intercept Communications to “Any Changed Telephone Number”*

As noted earlier, under Title III, the district court may authorize a standard intercept of communications over a land line or cellular telephone only if the government’s application includes “a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted.” § 2518(1)(b)(ii). The court must determine that “there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or

⁹We express no opinion on whether use of the technology Oliva alleged exists is authorized by federal law or permitted under the Fourth Amendment.

electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such a person.” § 2518(3)(d). Likewise, each surveillance order must specify “the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted.” § 2518(4)(b).

Oliva argues that these specification requirements were not satisfied here. Pursuant to the government’s requests, the orders authorized interception not only of named target phone numbers, but also of “any changed telephone number or any other telephone number subsequently assigned to or used by the instrument bearing the same ESN and/or IMSI as the Target Phones 1 and 2 within the thirty (30) day period.” Oliva maintains that these affidavits and orders did not specify the “facilities,” and thus did not authorize valid standard wire intercepts. From this premise, Oliva again argues that the orders constituted roving intercepts — specifically, roving wiretaps. The government concedes its applications did not meet the requirements for roving wiretaps, but disputes that is what it sought or the court approved.

We do not accept Oliva’s fundamental premise. The orders met the specification requirements and authorized valid standard wire intercepts. The Second Circuit addressed a comparable situation in *Goodwin*, 141 F.3d 394. There, the government’s surveillance applications specified the telephone numbers and ESNs of certain target cellular phones. *See id.* at 397. The defendant argued that the resulting orders authorized roving wiretaps because “a cellular phone has no fixed location, and that it therefore would be impossible for the government or the district court to specify the facility from which or the place where the communication was to be intercepted.” *Id.* at 403. The court rejected this argument, explaining:

The government’s affidavits in support of its application clearly identified the facilities to be tapped by

their telephone numbers and by their electronic serial numbers. The requirements of 18 U.S.C. §§ 2518(1)(b)(ii) and 2518(4)(b) were therefore satisfied, and authorization by a Deputy Assistant Attorney General was sufficient. In sum, [the defendant's] argument — that because one may rove about with a cellular telephone interception of a cellular telephone is necessarily a “roving wiretap” — does not comport with the terms or purposes of the wiretap statute.

Id. at 403.

[7] Oliva would distinguish *Goodwin* because the applications there appear to have been limited to a phone with a particular phone number *and* a particular ESN, whereas the surveillance affidavits and orders here extended to *any* phone number, so long as the phone used an ESN or IMSI specified in the orders. This distinction is immaterial. *See United States v. Duran*, 189 F.3d 1071 (9th Cir. 1999). As in this case, the surveillance orders in *Duran* authorized interception of *any* phone number, so long as the phone used an ESN or IMSI specified in the order. *See id.* at 1083 (authorization applied to “any changed telephone number assigned to a telephone with the same electronic serial number” as the target telephone number). We specifically held that under the order, “the statutory preconditions to judicial authorization were satisfied,” *id.* at 1086, noting that the government had not sought a roving wiretap. *See id.* at 1084 n.7. Accordingly, we hold that the similar orders in this case, and the affidavits upon which they were based, satisfied the standard wire intercept specification provisions of § 2518(1)(b)(ii) and (4)(b), and we reject Oliva’s argument that they constituted de facto roving wiretaps.

AFFIRMED.