FILED United States Court of Appeals Tenth Circuit

March 4, 2013

### <u>PUBLISH</u>

Elisabeth A. Shumaker Clerk of Court

# UNITED STATES COURT OF APPEALS

# **TENTH CIRCUIT**

UNITED STATES OF AMERICA,

Plaintiff - Appellee,

v.

SAMUEL BARAJAS, a/k/a Sammy,

Defendant - Appellant.

No. 12-3003

# APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF KANSAS (D.C. No. 2:10-CR-20077-JWL-2)

Branden A. Bell (and Carl Folsom, III, of Bell, Folsom, P.A., with him on the briefs) Olathe, Kansas, for Defendant - Appellant.

Nathan Judish (Barry R. Grissom, United States Attorney, and Trent M. Krug, Special Assistant United States Attorney, with him on the brief), Kansas City, Kansas, for Plaintiff - Appellee.

Before KELLY, HOLLOWAY, and MATHESON, Circuit Judges.

KELLY, Circuit Judge.

Defendant-Appellant Samuel Barajas was convicted in a jury trial of

conspiracy to distribute more than 500 grams of methamphetamine, 21 U.S.C. §§

846 and 841(a)(1), (b)(1)(B)(viii) (Count 1); aiding and abetting possession with

intent to distribute 50 grams or more of methamphetamine, 21 U.S.C.

§§ 841(a)(1) and (b)(1)(B)(viii) (Count 2); and using a communication facility, a cellular telephone, in committing, causing, and facilitating the conspiracy, 21 U.S.C. § 843(b) (Count 3). Mr. Barajas was sentenced to life in prison on Counts 1 and 2 and four years on Count 3, to run concurrently, and to five years' supervised release on Counts 1 and 2, and one year on Count 3, again to run concurrently. On appeal, he challenges the denial of his motion to suppress all evidence obtained from the wiretap surveillance and GPS pinging of certain cell phones. Exercising jurisdiction under 28 U.S.C. § 1291, we affirm.

### **Background**

This case arises from a DEA investigation into a San Diego County based drug trafficking organization, involved in the importation, transportation, and distribution of large quantities of methamphetamine and cocaine from Mexico throughout the United States. III R. 32–33. As part of its investigation, DEA agents engaged in wiretap surveillance and GPS pinging<sup>1</sup> of cell phones used by

<sup>&</sup>lt;sup>1</sup> At Mr. Barajas's trial, a DEA agent explained the pinging process:

<sup>[</sup>P]ursuant to the court order that authorizes the wiretap, we also received the authorization to conduct first-party and third-party GPS pings or queries, which is—basically, a first-party query would be contacting Sprint/Nextel, asking them to do a GPS query on . . . the target telephone being used by [Mr. Barajas]. Sprint/Nextel would return with the GPS coordinates for the location of that telephone within a certain radius, depending on the telephone's physical

members of the organization, including Mr. Barajas.

In March 2009, agents learned from a confidential source that Jesus Dominguez, a leader of the organization, was importing 30 to 40 pounds of methamphetamine and 20 kilograms of cocaine into the United States each week. <u>Id.</u> at 34. Agents began an investigation into Mr. Dominguez, using traditional investigative techniques at first. <u>Id.</u> at 37. However, agents soon decided that a wiretap of Mr. Dominguez's phone, referred to as Target Telephone (TT) No. 1, was necessary to further the investigation. <u>Id.</u> at 37–38. On May 14, 2009, agents submitted a wiretap application, which included a 30-page affidavit of Special Agent Brent Ashton and proposed wiretap order, to San Diego County Superior Court, seeking authorization under California Penal Code Section 629.52, the California equivalent to the federal wiretap statute. <u>Id.</u> at 27–65. The affidavit set forth Agent Ashton's training and experience in law enforcement and narcotics investigations, along with the facts establishing probable cause and

. . . .

II R. 115–16.

location and distance from cell towers. . . [A] third-party ping[], . . . would be GPS pings on any telephones in communication with the target telephone.

<sup>[</sup>T]he request is done electronically through a secure website that Sprint has set up, and basically I send the request, they acknowledge the request, and then within a matter of time Sprint/Nextel begins providing the GPS coordinates . . . I plug those GPS coordinates into Google maps, and it would come up with the location of that telephone.

necessity. <u>Id.</u> at 27–56. The affidavit indicated that agents had used telephone tolls, physical surveillance, and a confidential source, but that these techniques, among other measures, were or would be inadequate. <u>Id.</u> After reviewing the application, the judge granted the order. <u>Id.</u> at 57–65.

Through the wiretap of TT No. 1, agents learned of Mr. Barajas, identified then as "Samy last name unknown." II R. 89. After hearing repeated references to "Samy," agents sought a wiretap on his phone, TT No. 24. <u>Id.</u> On February 9, 2010, a judge approved the wiretap application, which included a proposed order and 153-page affidavit of Agent Ashton. III R. 190–348. As before, the affidavit set forth Agent Ashton's training and experience, along with the facts establishing probable cause and necessity. <u>Id.</u>

With respect to probable cause, the affidavit detailed Mr. Barajas's role in the conspiracy. <u>Id.</u> at 226. The affidavit listed intercepted conversations—e.g., May 22, 2009, when Mr. Barajas told Mr. Dominguez that he would take "tickets" to the man, <u>id.</u> at 227; December 7, 2009, when Mr. Dominguez told Mr. Barajas that "the girl" would be bringing the "lawsuits," <u>id.</u> at 295; and January 29, 2010, when Mr. Barajas told Mr. Dominguez to tell "the girl" to leave for Kansas City, <u>id.</u> at 312. The affidavit included Agent Ashton's interpretation of these conversations, and in particular, his belief that the conversation from January 29 detailed a plan to send a courier to Kansas City. <u>Id.</u> at 228, 287–88, 312–33. As for necessity, once again, the affidavit listed the techniques agents had used and those that were or would be unhelpful. <u>Id.</u> at 317–44.

By affidavit, the agents sought "authorization for the interception of wire, electronic pager and electronic cellular telephone communications to and from" TT No. 24. <u>Id.</u> at 223. The affidavit did not request GPS data. However, the proposed order that the judge ultimately approved included an authorization for GPS data. <u>Id.</u> at 194–96. Paragraph 13(i), for example, ordered cell phone providers to "provide any and all . . . (GPS) tracking and/or pinging data during the progress of a call, on an ongoing and/or real time basis." <u>Id.</u> at 196.

Through wiretap surveillance and GPS pinging of TT No. 24, agents were able to frustrate the organization's attempt to send a courier to Kansas City. <u>Id.</u> at 466. With the help of Kansas police, agents seized \$69,800 from the courier's vehicle and 1.68 kilograms of methamphetamine from a residence in Kansas. <u>Id.</u> However, agents soon suspected that Mr. Barajas was using another phone, TT No. 26. II R. 93. Accordingly, on February 25, 2010, agents obtained a wiretap order for TT No. 26, attaching a proposed order and 161-page affidavit to the application. III R. 349–518. This affidavit listed newly intercepted conversations, including a conversation about the recent seizure in Kansas. <u>Id.</u> at 465–66. Once again, the affidavit did not request GPS data, but the wiretap order authorized pinging. <u>Id.</u> at 351, 516.

On March 31, 2010, agents pinged TT No. 26, which showed the phone was located within a 5-meter radius of 4597 Pacific Rivera Way in San Diego,

- 5 -

California. II R. 272. On April 2, 2010, agents set up visual surveillance and observed a Toyota Camry entering the address. <u>Id.</u> at 282, 285. Agents followed the Camry to a body shop, where they placed a call to TT No. 26. <u>Id.</u> at 286–87. Mr. Barajas, the driver, did not pick up the phone, but later returned the call to the agents. <u>Id.</u> at 287. Until this point, agents did not know that "Samy," the user of TT No. 26, was Mr. Barajas. <u>Id.</u> at 288.

On April 28, 2010, agents pinged TT No. 26, which revealed the phone was located within 11 meters of the same San Diego address. <u>Id.</u> at 347. One day later, agents pinged the phone and learned that it was located near a 24-Hour Fitness health club. <u>Id.</u> Agents went to the location and found a champagnecolored Mercedes, a car they had seen at the San Diego address, in the parking lot. <u>Id.</u> at 348. Agents arrested Mr. Barajas when he exited the club and found TT No. 26 in his pocket. <u>Id.</u> at 351.

On June 17, 2010, the government filed a four-count Indictment against Mr. Barajas. I R. 13–16. Prior to trial, Mr. Barajas moved to suppress all evidence obtained from the wiretaps of TT Nos. 1, 24, and 26, and all GPS and cell site location data from pinging TT Nos. 24 and 26. III R. 5–26. Mr. Barajas argued (1) that the wiretap applications failed to satisfy the necessity requirement of Title III; and (2) that the orders authorizing the acquisition of GPS and cell site location data were not supported by probable cause because the affidavits did not request GPS and cell site location data. <u>Id.</u>

- 6 -

The district court held a hearing on the motion on July 8, 2011, and one month later, issued a memorandum and order denying the motion. <u>Id.</u> at 564. On the first issue, the court concluded that the wiretaps were necessary because, *inter alia*, traditional techniques had proven inadequate. <u>Id.</u> at 568. On the second issue, the court assumed without deciding that pinging is a search, and held the affidavits provided probable cause for the GPS data. <u>Id.</u> at 570. The court explained that Mr. Barajas had failed to show "why the same evidence supporting probable cause with respect to the interception of communications would not also support probable cause with respect to the GPS . . . data." <u>Id.</u> at 570–71. The court added that, absent probable cause, the good-faith exception under <u>United States v. Leon</u>, 468 U.S. 897 (1984), would apply. <u>Id.</u> at 571–72.

Mr. Barajas proceeded to trial, and on September 9, 2011, a jury convicted him of Counts 1–3 of the Indictment. I R. 116–17. The trial court sentenced him to life in prison on Counts 1 and 2 and four years on Count 3, to run concurrently, and to five years' supervised release on Counts 1 and 2, and one year on Count 3, again to run concurrently. II R. 629. Mr. Barajas timely appealed. I R. 149.

#### Discussion

#### A. <u>Motion to Suppress Wiretap Evidence</u>

Mr. Barajas first challenges the district court's order denying his motion to suppress conversations the government recorded pursuant to wiretaps on TT Nos.

1, 24, and 26. He argues the affidavits in support of the wiretaps did not establish necessity for the wiretaps as required under Title III of the Omnibus Crime Control and Safe Streets Act of 1968. <u>See</u> 18 U.S.C. §§ 2518(1)(c), 2518(3)(c). He specifically contends (1) that the affidavit for TT No. 1 did not show that traditional investigative techniques had been tried unsuccessfully or that they reasonably appeared to be unsuccessful if tried; and (2) that the affidavits for TT Nos. 24 and 26 were "boilerplate" repetitions of previous affidavits and failed to establish specific necessity. Aplt. Br. 18–25. We review for abuse of discretion a district court's decision that a wiretap was necessary. <u>United States v. Ramirez-</u>Encarnacion, 291 F.3d 1219, 1222 & n.1 (10th Cir. 2002).

Although the wiretaps were issued under California law, California wiretap law conforms to federal law. <u>People v. Leon</u>, 150 P.3d 207, 211 (Cal. 2007). The state procedure is incorporated under 18 U.S.C. § 2516(2). Thus, we apply federal standards to determine whether the evidence is admissible. <u>United States</u> <u>v. Armendariz</u>, 922 F.2d 602, 607 (10th Cir. 1990) (citing <u>Elkins v. United States</u>, 364 U.S. 206 (1960)).

"A defendant bears the burden of proving that a wiretap is invalid once it has been authorized." <u>Ramirez-Encarnacion</u>, 291 F.3d at 1222. In order to obtain a wiretap, the government must show, among other things, that a wiretap is necessary. <u>See</u> 18 U.S.C. §§ 2518(1)(c), 2518(3)(c). The government must submit "a full and complete statement as to whether or not other investigative

- 8 -

procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried." Id. § 2518(1)(c). Such measures include: "(1) standard surveillance; (2) questioning and interrogating witnesses or suspects, including through the use of grand jury proceedings; (3) search warrants; (4) infiltration of criminal groups by confidential informants and undercover agents; (5) pen registers; and (6) trap and trace devices." United States v. Foy, 641 F.3d 455, 464 (10th Cir. 2011) (citation omitted). We do not require, however, that agents "exhaust all other conceivable investigative procedures before resorting to wiretapping." Id. (quoting United States v. Zapata, 546 F.3d 1179, 1186 (10th Cir. 2008)). Rather, we review the government's actions "in a common sense fashion," and consider "all the facts and circumstances in order to determine whether the government's showing of necessity is sufficient to justify a wiretap." United States v. Verdin-Garcia, 516 F.3d 884, 890 (10th Cir. 2008) (quotation omitted).

We have thoroughly reviewed the affidavits for TT Nos. 1, 24, and 26, and find them sufficient to support the district court's conclusion that the wiretaps were necessary. In each affidavit, Agent Ashton explains why traditional investigative techniques—e.g., confidential sources and visual surveillance—were ineffective and why other techniques—e.g., trash searches and search warrants—would prove ineffective if tried. <u>See</u> III R. 37–49, 317–44, 469–497. We have upheld wiretaps on similar showings. <u>See Foy</u>, 641 F.3d at 464; <u>Zapata</u>,

- 9 -

546 F.3d at 1187; <u>Verdin-Garcia</u>, 516 F.3d at 890–92. Furthermore, in cases that involve a conspiracy, like this one, we have allowed wiretaps because the "goal of uncovering the size and scope of the conspiracy may justify the authorization of wiretaps." <u>Foy</u>, 641 F.3d at 464–65; <u>see Zapata</u>, 546 F.3d at 1188 ("[T]he government's motivation in using the wiretaps was to gain insight into the full extent of the conspiracy."). We will not disturb the district court's finding that these wiretaps were necessary.

As for Mr. Barajas's argument that the affidavits for TT Nos. 24 and 26 are mere repetitions of previous affidavits, we disagree. These affidavits, 153- and 161-pages respectively, are more than triple the length of the first affidavit, and more importantly, include new details about the organization. We have upheld wiretaps in ongoing investigations when they display, as they do here, a "new discussion of information learned, surveillance conducted, and so on, subsequent to the previous wiretap application." <u>Verdin-Garcia</u>, 516 F.3d at 892. Thus, the government met its burden in showing these wiretaps were necessary, and the district court correctly denied Mr. Barajas's motion to suppress.

#### B. <u>Motion to Suppress Evidence Obtained through GPS Pinging</u>

Mr. Barajas next challenges the district court's order denying his motion to suppress GPS data the government obtained through pinging TT Nos. 24 and 26. He contends that pinging should not have been covered by the wiretap orders because there was no probable cause in the affidavits to support the search for

- 10 -

GPS data. Aplt. Br. 29. Here Mr. Barajas makes three arguments: (1) pinging is a search under the Fourth Amendment; (2) the wiretap affidavits did not provide probable cause for pinging because they failed to request GPS data; and (3) the good-faith exception to the exclusionary rule does not apply. <u>Id.</u> at 27–31. Like the district court, we will assume without deciding that pinging is a search,<sup>2</sup> and proceed to Mr. Barajas's second and third arguments.

# 1. <u>Probable Cause</u>

When reviewing a district court's denial of a motion to suppress, we view the evidence in the light most favorable to the prevailing party and accept the court's factual findings unless they are clearly erroneous. <u>United States v. Ruiz</u>, 664 F.3d 833, 838 (10th Cir. 2012). We review de novo the legal determination of reasonableness under the Fourth Amendment. <u>Id.</u> When a search is conducted pursuant to a warrant, our review is more deferential: "we look to ensure that the judge had a substantial basis for concluding that the affidavit in support of the warrant established probable cause." <u>United States v. Burkhart</u>, 602 F.3d 1202, 1205 (10th Cir. 2010) (quotation omitted). "An affidavit establishes probable cause for a search warrant if the totality of the information it contains establishes the fair probability that contraband or evidence of a crime will be found in a

<sup>&</sup>lt;sup>2</sup> This question is somewhat unsettled after the Supreme Court's decision in <u>United States v. Jones</u>, 132 S. Ct. 945 (2012). Only the Sixth Circuit has weighed in on this topic, holding that pinging is not a search under the Fourth Amendment. <u>See United States v. Skinner</u>, 690 F.3d 772, 777 (6th Cir. 2012).

particular place." <u>United States v. Roach</u>, 582 F.3d 1192, 1200 (10th Cir. 2009) (quotation omitted). There must be a "nexus between . . . suspected criminal activity and the place to be searched[;]" a court may not "pil[e] hunch upon hunch." <u>Id.</u> (quotations omitted). "Sufficient information must be presented to the magistrate to allow that official to determine probable cause; his action cannot be a mere ratification of the bare conclusions of others." <u>United States v. Cooper</u>, 654 F.3d 1104, 1124 (10th Cir. 2011) (quoting <u>Illinois v. Gates</u>, 462 U.S. 213, 239 (1983)).

Mr. Barajas argues there is no probable cause for GPS pinging because the affidavits did not request GPS data.<sup>3</sup> Aplt. Br. 29. He contends the judge had no basis for concluding that evidence of the drug trafficking conspiracy would be found in the GPS data because the affidavits only indicated that "communications between the suspects" would contain evidence of the conspiracy. Aplt. R. Br. 16–19 (emphasis omitted). The district court rejected this argument, finding that Mr. Barajas had failed to show "why the same evidence supporting probable cause with respect to the interception of communications would not also support probable cause with respect to the GPS . . . data." III R. 570–71.

<sup>&</sup>lt;sup>3</sup> Mr. Barajas also suggests the orders were "a sort of writ of assistance . . . used in colonial times to authorize general searches." Aplt. Br. 29. Although placed within an argument on probable cause, this point challenges the warrant's particularity. <u>Cf. United States v. Cooper</u>, 654 F.3d 1104, 1124–27 (10th Cir. 2011) (separate inquiries for probable cause and particularity). Because Mr. Barajas does not contest particularity, we do not consider it on appeal.

As an initial matter, we agree with the district court that nothing in the Fourth Amendment prevents us from considering whether certain facts in the affidavit support probable cause for the GPS data in addition to the wiretaps. Warrants frequently authorize a search of more than one place, and one set of facts may provide probable cause for both searches. See, e.g., United States v. Tisdale, 248 F.3d 964, 971 (10th Cir. 2001) (facts of attempted burglary provided probable cause to search defendant's car and house); see also Groh v. Ramirez, 540 U.S. 551, 557 (2004) ("The Fourth Amendment by its terms requires particularity in the warrant, not in the supporting documents."). Moreover, we are mindful that "the Fourth Amendment's commands, like all constitutional requirements, are practical and not abstract." United States v. Ventresca, 380 U.S. 102, 108 (1965). "[C]ourts should not invalidate [a] warrant by interpreting the affidavit in a hypertechnical, rather than a commonsense, manner." <u>Id.</u> at 109. Thus, we reject Mr. Barajas's suggestion that our probable cause determination hinges on the government's failure to specifically request GPS data.

However, it does not necessarily follow that the facts in the affidavit are sufficient for probable cause. We still must find the judge had a "substantial basis," <u>Burkhart</u>, 602 F.3d at 1205 (quotation omitted), to conclude that "contraband or evidence of a crime will be found in a particular place," <u>Roach</u>, 582 F.3d at 1200 (quotation omitted). The district court answered this question in the affirmative: In this case, the affidavits established that defendant was involved in criminal activity and that he was using his cell phones (TT24 and TT26) in connection with that activity; thus, there was probable cause to believe that the fruits, instrumentalities, or evidence of drug-trafficking could be obtained by use of GPS . . . data for TT24 and TT26.

III R. 471. We, however, are not so sure that Mr. Barajas's use of the phones for criminal activity is enough to authorize access to the GPS data. We require a "nexus" between the criminal activity and the place to searched, <u>Roach</u>, 582 F.3d at 1200 (quotation omitted), and demand that an affiant provide the judge with "[s]ufficient information," <u>Cooper</u>, 654 F.3d at 1124 (quotation omitted). Absent an explanation of how Mr. Barajas's location would reveal information about the workings of the conspiracy—or more accurately, Mr. Barajas himself—we cannot be certain that probable cause exists. Ultimately, we need not resolve this question because any deficiency in probable cause is cured by the good-faith exception.

## 2. <u>Good-Faith Exception</u>

In <u>United States v. Leon</u>, 468 U.S. 897, 913 (1984), the Supreme Court created a good-faith exception to the usual rule that courts should exclude evidence obtained in violation of the Fourth Amendment. The good-faith exception provides that "evidence seized pursuant to the warrant need not be suppressed if the executing officer acted with an objective good-faith belief that the warrant was properly issued by a neutral magistrate." <u>United States v.</u>

- 14 -

Campbell, 603 F.3d 1218, 1225 (10th Cir. 2010) (quotation omitted).

Before delving into <u>Leon</u>, we note that we do not decide whether the goodfaith exception applies in the Title III context, a question unresolved in our circuit, <u>see United States v. Arrington</u>, 216 F.3d 1088, 2000 WL 775576, at \*6 (10th Cir. June 16, 2000) ("[T]he applicability of <u>Leon</u> to the Title III context is unsettled . . . ."), and on which other circuits are split.<sup>4</sup> We need not wade in these murky waters because, as the parties conceded and as we agree, there is no Title III suppression mechanism for GPS data.<sup>5</sup> Our analysis starts and ends with <u>Leon</u>.

Under <u>Leon</u>, we presume good-faith when an officer acts pursuant to a warrant unless one of "four contexts" apply. <u>See Burkhart</u>, 602 F.3d at 1208

<sup>&</sup>lt;sup>4</sup> The Fourth, Eighth, and Eleventh Circuits have held the exception does apply, <u>see United States v. Lomeli</u>, 676 F.3d 734, 742 (8th Cir. 2012) (citing <u>United States v. Moore</u>, 41 F.3d 370, 376 (8th Cir. 1994)); <u>United States v.</u> <u>Brewer</u>, 204 F. App'x 205, 208 (4th Cir. 2006); <u>United States v. Malekzadeh</u>, 855 F.2d 1492, 1497 (11th Cir. 1988), and the Sixth Circuit has held that it does not, <u>see United States v. Rice</u>, 478 F.3d 704, 711–14 (2007).

<sup>&</sup>lt;sup>5</sup> In 1968, Congress passed Title III as part of the Omnibus Crime Control and Safe Streets Act, which provided requirements, procedures, and protections for electronic surveillance via wiretaps. Pub. L. No. 90-351, § 802, 82 Stat. 216. Evidence obtained in violation of Title III is suppressed. 18 U.S.C. § 2515. In 1986, Congress amended Title III with the Electronic Communications Privacy Act, and clarified that only wire and oral communications are subject to statutory suppression. Pub. L. No. 99-508, § 101(c), 100 Stat. 1848, 1851; <u>see</u> 18 U.S.C. 2518(10)(a) ("Any aggrieved person . . . may move to suppress the contents of any wire or oral communication . . . ."). GPS data is neither a wire nor oral communication, thus Title III suppression does not apply.

(quotation omitted). Mr. Barajas claims that one such context applies here—the "affidavit [was] so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable." Aplt. R. Br. 27 (citing <u>Leon</u>, 468 U.S. at 923). He argues that the affidavit is "devoid of facts" as to why "communications between the suspects" might be found in the GPS data. <u>Id.</u> at 29.

The stumbling block to Mr. Barajas's argument is that he construes the affidavit too technically, focusing on what the affidavit *literally* requests and where the government *literally* searched. But, as noted above, "the Fourth Amendment's commands . . . are practical and not abstract." Ventresca, 380 U.S. at 108. We cannot limit our analysis to what the affidavit requests. Rather, we must ask whether the affidavit as a whole "establishes a minimally sufficient nexus between the illegal activity and the place to be searched." United States v. <u>Henderson</u>, 595 F.3d 1198, 1202 (10th Cir. 2010) (quoting <u>United States v.</u> Gonzales, 399 F.3d 1225, 1230 (10th Cir. 2005)). Under this inquiry, we find the following "nexus"—"Samy" was using the phones for criminal activity but the government did not know who "Samy" was, thus access to the GPS data would help the government identify "Samy" and pursue the organization. We would prefer this explanation in the affidavit, but we impose a lower standard in goodfaith determinations than we do with probable cause, only requiring "a minimal nexus" as compared to "a substantial nexus." Gonzales, 399 F.3d at 1230 (citing

- 16 -

<u>United States v. Carpenter</u>, 360 F.3d 591, 596 (6th Cir. 2004) (en banc)). Thus, we cannot say the affidavit is "devoid of facts."

However, even if the affidavit is not "devoid of facts," the good-faith exception will not apply when an officer "knows or should have known that a search warrant was invalid." <u>Henderson</u>, 595 F.3d at 1202 (quotation omitted). We presume that law enforcement officials have a reasonable knowledge of the law. <u>Id.</u> (citing <u>Leon</u>, 468 U.S. at 919 n.20). Mr. Barajas suggests the agents knew or should have known the order was invalid because they knew (1) that GPS data is not typically intercepted pursuant to a wiretap order; and (2) that the affidavit did not request GPS data. Aplt. Br. 30; Aplt. R. Br. 30. We disagree.

First, we have no reason to believe the government cannot obtain GPS data through a wiretap order. Assuming pinging is a search, the burden to obtain GPS data would be no greater than a wiretap—probable cause. But even if Mr. Barajas is correct, he cannot show the agents were on notice of this fact because the law on electronic surveillance is very much unsettled. <u>See In re Application of U.S.</u> for an Order Directing a Provider of Electronic Comme'n Serv. to Disclose <u>Records to the Gov't</u>, 620 F.3d 304, 310 n.6, 311 (3d Cir. 2010) (noting the debate among courts on the procedure for electronic surveillance and taking "no position whether a request for GPS data is appropriate under a § 2703(d) order"); <u>see also</u> Henderson, 595 F.3d at 1202 (officers acted in good-faith when relying

- 17 -

on an affidavit based on a standardized form the court *later* determined did not establish probable cause); <u>United States v. Rowland</u>, 145 F.3d 1194, 1207 (10th Cir. 1998) (applying the good-faith exception to an anticipatory warrant when the law was unsettled). The agents' knowledge of the gap between the affidavit and the order gives us more pause, but we cannot say this gap was intentional.

Finally, in his reply brief, Mr. Barajas offers two additional reasons why the good-faith exception does not apply: (1) pinging turns cell phones into tracking devices, but the agents were not authorized to intercept transmissions from tracking devices; and (2) the search exceeded the scope of the warrant because the warrant permitted pinging during the progress of the call, but the agents pinged the cell phones at all times. Aplt. R. Br. 31–34. We will not address either argument, however, because Mr. Barajas did not raise either in his opening brief. <u>See White v. Colorado</u>, 82 F.3d 364, 366 n.4 (10th Cir. 1996) (court need not consider argument raised for the first time in appellate reply brief).

## AFFIRMED.