

CA NO. 14-50120  
IN THE UNITED STATES COURT OF APPEALS  
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

PAULO LARA,

Defendant-Appellant.

DC NO. CR 13-00392-BRO-1

---

**APPELLANT'S OPENING BRIEF**

---

APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE  
CENTRAL DISTRICT OF CALIFORNIA

HONORABLE BEVERLY REID O'CONNELL  
United States District Judge

HILARY POTASHNER  
Acting Federal Public Defender  
ALEXANDRA W. YATES  
Deputy Federal Public Defender  
321 East 2nd Street  
Los Angeles, California 90012-4202  
Telephone: (213) 894-5059  
Facsimile: (213) 894-0081  
E-mail: Alexandra\_Yates@fd.org

Attorneys for Defendant-Appellant

## TABLE OF CONTENTS

	<b>Page</b>
I. QUESTION PRESENTED.....	1
II. INTRODUCTION .....	1
III. STATEMENT OF PERTINENT AUTHORITIES .....	2
IV. STATEMENT OF JURISDICTION .....	3
V. STATEMENT OF THE CASE .....	3
A. Bail Status.....	3
B. Course of Proceedings.....	3
C. Statement of Facts .....	4
1. Mr. Lara’s State Probation.....	4
2. The Warrantless Searches .....	5
3. The Motion To Suppress.....	7
VI. SUMMARY OF ARGUMENT .....	13
VII. ARGUMENT.....	14
A. Standard of Review .....	14
B. The District Court Should Have Granted Mr. Lara’s Motion To Suppress.....	14
1. The Fourth Amendment Protects Against Warrantless Searches, Except in Narrow Circumstances .....	15
2. In <i>Riley v. California</i> , the Supreme Court Held That Law Enforcement Officers May Not Search an Arrestee’s Cell Phone Without a Warrant.....	17
3. The Warrantless, Suspicionless Search of a Probationer’s Cell Phone Is Unconstitutional .....	23

## TABLE OF CONTENTS

	<b>Page</b>
a. A Cell Phone Search Implicates Heightened Privacy Concerns .....	23
b. Mr. Lara Retained a Reasonable Expectation of Privacy in the Data Stored on His Cell Phone, Despite His Status as a Probationer .....	26
c. Mr. Lara’s State Probation Condition Did Not Provide Notice That the Data on His Cell Phone Was Subject to Warrantless, Suspicionless Search .....	30
d. The Sprint Subscriber Record Was Not Properly Admitted and in Any Event Did Not Affect Mr. Lara’s Reasonable Expectation of Privacy .....	34
e. The Government’s Interests Do Not Outweigh Mr. Lara’s Reasonable Expectation of Privacy .....	38
f. Even if the Initial Search of Mr. Lara’s Phone Was Constitutional, the Warrantless Search of the GPS Data on His Phone Was Not .....	40
VIII. CONCLUSION.....	42

## TABLE OF AUTHORITIES

	<b>Page(s)</b>
<b>FEDERAL CASES</b>	
<i>City of Indianapolis v. Edmond</i> , 531 U.S. 32 (2000).....	38
<i>Ferguson v. City of Charleston</i> , 532 U.S. 67 (2001).....	38
<i>Griffin v. Wisconsin</i> , 483 U.S. 868 (1987).....	28, 29
<i>Maryland v. King</i> , ___ U.S. ___, 133 S. Ct. 1958 (2013).....	27
<i>Nijjar v. Holder</i> , 689 F.3d 1077 (9th Cir. 2014) .....	32
<i>Riley v. California</i> , ___ U.S. ___, 134 S. Ct. 2473 (2014).....	<i>passim</i>
<i>Samson v. California</i> , 547 U.S. 843 (2006).....	27, 32, 38, 40
<i>United States v. Carbajal</i> , 956 F.2d 924 (9th Cir. 1992) .....	15
<i>United States v. Davis</i> , 2011 WL 2036463 (D. Or. May 24, 2011) .....	36
<i>United States v. Heckenkamp</i> , 482 F.3d 1142 (9th Cir. 2007) .....	33
<i>United States v. Jones</i> , ___ U.S. ___, 132 S. Ct. 945 (2012).....	41
<i>United States v. Karo</i> , 468 U.S. 705 (1984).....	41
<i>United States v. King</i> , 608 F.3d 1122 (9th Cir. 2010) .....	31

## TABLE OF AUTHORITIES

	<b>Page(s)</b>
<b>FEDERAL CASES</b>	
<i>United States v. King</i> , 687 F.3d 1189 (9th Cir. 2012) .....	27
<i>United States v. King</i> , 736 F.3d 805 (9th Cir. 2013) .....	<i>passim</i>
<i>United States v. Knights</i> , 534 U.S. 112 (2001).....	<i>passim</i>
<i>United States v. Lozano</i> , 623 F.3d 1055 (9th Cir. 2010) .....	36, 37
<i>United States v. Payton</i> , 573 F.3d 859 (9th Cir. 2009) .....	32
<i>United States v. Scott</i> , 450 F.3d 863 (9th Cir. 2006) .....	29
<i>United States v. Skinner</i> , 2007 WL 1556596 (E.D. Tenn. May 24, 2007) .....	35
<i>United States v. Song Ja Cha</i> , 597 F.3d 995 (9th Cir. 2010) .....	14
<i>United States v. Suarez-Blanca</i> , 2008 WL 4200156 (N.D. Ga. Apr. 21, 2008).....	35, 36, 37
<i>Wong Sun v. United States</i> , 371 U.S. 471 (1963).....	14
<b>FEDERAL STATUTES, RULES, AND CONSTITUTIONAL AMENDMENTS</b>	
18 U.S.C. § 922 .....	3
18 U.S.C. § 3231 .....	3
18 U.S.C. § 3563 .....	31
28 U.S.C. § 1291 .....	3

## TABLE OF AUTHORITIES

	<b>Page(s)</b>
<b>FEDERAL STATUTES, RULES, AND CONSTITUTIONAL AMENDMENTS</b>	
Fed. R. Evid. 401 .....	35
Fed. R. Evid. 602 .....	35
Fed. R. Evid. 901 .....	35
U.S. Const. amend. IV .....	3, 15
<b>STATE CASES</b>	
<i>People v. Diaz</i> , 51 Cal. 4th 84 (2011) .....	18
<i>People v. Lord</i> , 2009 WL 2244172 (Cal. Ct. App. July 28, 2009) .....	31
<i>People v. Olguin</i> , 45 Cal. 4th 375 (2008) .....	28
<i>People v. Ramirez</i> , 2009 WL 2197070 (Cal. Ct. App. July 24, 2009) .....	31
<i>People v. Realmuto</i> , 2010 WL 3221963 (Cal. Ct. App. Aug. 17, 2010) .....	31
<b>STATE STATUTES</b>	
California Health and Safety Code § 11378 .....	4
California Health and Safety Code § 11379 .....	4
California Penal Code § 1203 .....	31
<b>MISCELLANEOUS</b>	
Thom File, <i>Computer and Internet Use in the United States</i> , U.S. Census Bureau, (May 2013) .....	26

## TABLE OF AUTHORITIES

	<b>Page(s)</b>
<b>MISCELLANEOUS</b>	
Erinn J. Herberman and Thomas P. Bonczar, <i>Probation and Parole in the United States, 2013</i> , Bureau of Justice Statistics (Oct. 2014) .....	23
Mark Hugo Lopez, Ana Gonzalez-Barrera, & Eileen Patten, <i>Closing the Digital Divide: Latinos and Technology Adoption</i> , Pew Research Center (Mar. 7, 2013).....	25
Dan Rowinski, <i>Dropping Prices Are Driving Mass Smartphone Adoption Across the World</i> , readwrite (Nov. 27, 2013), .....	26
Aaron Smith, <i>African Americans and Technology Use</i> , Pew Research Center (Jan. 6, 2014).....	25
Gerry Smith, <i>Smartphones Bring Hope, Frustration as Substitute for Computers</i> , Huffington Post (June 6, 2012) .....	25
Kathryn Zickuhr & Aaron Smith, <i>Digital Differences</i> , Pew Research Center (Apr. 13, 2012).....	24

## **I. QUESTION PRESENTED**

Whether, as the district court held, a probation condition that authorizes warrantless, suspicionless searches of a probationer's property also permits warrantless, suspicionless searches of his cell phone data, including photographs, text messages, and location information; or instead, as the U.S. Supreme Court more recently held, a warrant is generally required to search a cell phone.

## **II. INTRODUCTION**

Defendant-Appellant Paulo Lara was a California state probationer subject to the condition that his person and property, including any container, could be searched or seized at any time, with or without a warrant, probable cause, or reasonable suspicion. During a routine probation search, probation officers searched through Mr. Lara's cell phone and discovered photographs of a gun along with text messages suggesting Mr. Lara was attempting to sell the gun. The officers confiscated the phone and later conducted a forensic analysis that revealed Global Positioning System ("GPS") location data attached to the photographs, which led the officers to Mr. Lara's parents' residence. A search of that location uncovered the firearm depicted in the photographs and some ammunition. At no time did the officers request a warrant.

The government charged Mr. Lara with being a felon in possession of a firearm and ammunition, and Mr. Lara moved to suppress all evidence discovered

as a result of the warrantless, suspicionless searches of his phone. He argued that, because of the huge quantity of sensitive data stored on a modern cell phone, the search was not comparable to a search of ordinary property.

The district court denied the motion, explaining, “No U.S. Supreme Court precedent mandates treating a cell phone any differently than a container.” (ER 15.) To the contrary, the district court found “[i]ncredibly important . . . the line of cases that permit the police to search cellular telephones incident to arrest as property.” (ER 5.)

Seven months later, in *Riley v. California*, \_\_ U.S. \_\_, 134 S. Ct. 2473 (2014), the U.S. Supreme Court unanimously held that the warrantless search of a cell phone incident to arrest is unconstitutional, abrogating the precedent on which the district court relied. The Court specifically held that “[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse.” *Id.* at 2488-89.

This case presents the first opportunity for a federal court to apply *Riley* in the context of a warrantless, suspicionless probation search of a cell phone.

### **III. STATEMENT OF PERTINENT AUTHORITIES**

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the

place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV.

#### **IV. STATEMENT OF JURISDICTION**

This appeal is from a final judgment rendered by the Honorable Beverly Reid O’Connell, United States District Judge, on March 3, 2014, sentencing Mr. Lara to thirty-seven months in prison followed by three years of supervised release for being a felon in possession of a firearm and ammunition, in violation of 18 U.S.C. § 922(g)(1). (ER 265.) Judgment was entered on March 5, 2014. (ER 281.) Mr. Lara filed a timely notice of appeal on March 12, 2014. (ER 269-73.) *See* Fed. R. App. P. 4(b)(1)(A)(i).

The district court had jurisdiction pursuant to 18 U.S.C. § 3231. This Court has jurisdiction pursuant to 28 U.S.C. § 1291.

#### **V. STATEMENT OF THE CASE**

##### **A. Bail Status**

Mr. Lara is in federal custody with a March 4, 2016, projected release date.

##### **B. Course of Proceedings**

On May 30, 2013, the government charged Mr. Lara with being a felon in possession of a firearm and ammunition, in violation of 18 U.S.C. § 922(g)(1). (ER 18-19.) Mr. Lara pleaded not guilty (ER 20), and moved to suppress evidence obtained as a result of the warrantless search of his cell phone (ER 21-39). An

opposition and reply were filed (ER 40-113), and on November 4, 2013, the district court held a hearing (ER 114-229). At the conclusion of the hearing, the court orally denied Mr. Lara's motion. (ER 2-10.) The court later issued a written order memorializing its ruling. (ER 11-17.)

Mr. Lara signed a conditional plea agreement, preserving his right to appeal the denial of his suppression motion. (ER 230-42.) On November 26, 2013, Mr. Lara pleaded guilty (ER 243-64), and on March 3, 2014, the district court sentenced him to thirty-seven months in prison followed by three years of supervised release (ER 265).

Mr. Lara appeals the denial of his suppression motion.<sup>1</sup>

### **C. Statement of Facts**

The relevant facts are not in dispute.

#### **1. Mr. Lara's State Probation**

On July 25, 2012, Mr. Lara pleaded guilty to possession for sale of a controlled substance and transportation of a controlled substance, both felonies, in violation of California Health and Safety Code sections 11378 and 11379(a), respectively. (ER 79-85.) He was sentenced to probation under terms and

---

<sup>1</sup> Mr. Lara filed a second suppression motion, challenging the warrantless search of his mother's residence as independently unlawful. (CR 30.) The district court found that the search was consensual and denied the motion. (ER 7-10, 16-17.) Mr. Lara does not appeal from that separate ruling.

conditions that included the following: “Submit your person and property including any residence, premises, container, or vehicle under your control, to search and seizure at any time of the day or night by any law enforcement officer, probation officer, or mandatory supervision officer with or without a warrant, probable cause or reasonable suspicion.” (ER 38, 71, 83.) When Mr. Lara accepted those terms and conditions, he did not believe they authorized the search of data on his cell phone, including GPS location information, without his consent. (ER 39.)

One month later, Mr. Lara met for the first time with his probation officer, Jennifer Fix. (ER 74.) Officer Fix reviewed Mr. Lara’s probation terms, including the search condition, “to ensure he understood them.” (ER 74-75.) This review involved simply reading the conditions and asking Mr. Lara whether he had any questions. With respect to the search condition, Officer Fix did not offer any advice on its scope or discuss the various ways in which Mr. Lara was subject to search. (ER 126-27.) Mr. Lara did not ask any questions. (ER 75, 128-29.)

## **2. The Warrantless Searches**

On October 1, 2012, Mr. Lara failed to report to probation, as scheduled. (ER 75.) Two days later, Officer Fix and fellow probation officer Joseph Ortiz conducted a routine, unannounced visit at Mr. Lara’s home. (ER 75, 130.) At the

time, the officers did not have any reason to suspect that Mr. Lara possessed a firearm. (ER 130.)

On arrival, the officers ordered Mr. Lara to sit on the couch. (ER 75, 130.) He was not free to move about and did not have access to a cell phone that was on the coffee table. (ER 4, 133.) Officer Ortiz asked Mr. Lara whether the phone belonged to him, and Mr. Lara replied that it did. (ER 4, 75.) Officer Ortiz picked up the phone and searched through the text messages. (ER 75-76.) He did not ask for or receive Mr. Lara's consent; Mr. Lara did not object. (ER 39, 76.) On the phone, Officer Ortiz discovered three pictures of a semiautomatic handgun in recent text messages. Mr. Lara had sent the pictures to someone identified as "Al," and the text conversation between the two suggested Al was interested in buying the gun from Mr. Lara. (ER 75-76.)

The officers handcuffed Mr. Lara and searched his home and vehicle, but did not find the gun. (ER 76.) Mr. Lara was arrested for violating the terms of his probation and detained. (ER 76-77.) Upon arrival at the county jail, Officers Fix and Ortiz took Mr. Lara's cell phone to the Orange County Computer Forensics Lab, where its data and a report analyzing that data were downloaded onto a disc. (ER 77, 133-34.)

The following day, Officers Fix and Ortiz reviewed the forensics report and determined, based on GPS data, that the photographs in question were taken on

October 2, at a specific address in Long Beach, California. (ER 77, 133-34.)

Officer Fix entered that address into a law enforcement database, which revealed that Mr. Lara had listed it as his “home address” three-and-a-half years earlier, in conjunction with another case. (ER 77-78, 86.) Officer Fix reviewed Mr. Lara’s file and the contacts listed in his cell phone and learned that the residence belonged to Mr. Lara’s parents. An internet search revealed that Mr. Lara’s mother Rosa operated a day care on the premises. (ER 78.)

Later that day, Probation Officers Fix and Ortiz, accompanied by four to five Long Beach Police Department officers, searched Mr. Lara’s parents’ residence. In the search, the officers recovered a 9mm handgun and ten rounds of ammunition from a room with bedding that matched the background of the pictures on Mr. Lara’s phone. The gun resembled the one in the pictures and was wrapped in a towel that appeared to be the towel in the background of the pictures. (ER 78, 94-96, 142, 156.)

Without the GPS data, the probation officers would have had no reason to conduct a visit to Mr. Lara’s parents’ home. (ER 134.)

### **3. The Motion To Suppress**

Mr. Lara moved to suppress all evidence obtained as the fruit of the unlawful searches of his phone. (ER 21-39.) He argued that modern cell phones contain extensive, sensitive personal information that make them analogous to

computers and unlike traditional property. For this reason, California courts sometimes impose a more specific probation condition that authorizes searches of digital media. By contrast, no reasonable person would have understood the general property-search condition imposed on Mr. Lara to cover a search of his cell phone data. (ER 24-29, 180-85.)

Similarly, because of the sensitive nature of the data found on a modern cell phone, Mr. Lara had a reasonable expectation of privacy in that information. (ER 31-33, 187-88.) The GPS data, which essentially allowed the government to track Mr. Lara's movements, is particularly private, sensitive information. (ER 185-87.) The government's interests in investigating and preventing crime did not outweigh Mr. Lara's legitimate expectations. (ER 33, 188-89.) Thus, the warrantless, suspicionless searches of Mr. Lara's phone violated his Fourth Amendment right to be free from unreasonable searches and seizures. (ER 33-34.) Even if the initial search of Mr. Lara's phone was lawful, the subsequent warrantless search of GPS location information on his phone was unreasonable. (ER 29, 34-35.)

The government opposed the motion. (ER 40-96.) It claimed that Mr. Lara waived all of his Fourth Amendment rights when he pleaded guilty in state court and signed a document titled "Advisement and Waiver of Rights for a Felony Guilty Plea," which included the following language:

I understand under the Fourth and Fourteenth  
Amendments to the United States Constitution, I have a

right to be free from unreasonable searches and seizures. I waive and give up this right, and further agree that for the period during which I am on probation or mandatory supervision I will submit my person and property, including any residence, premises, container or vehicle under my control to search and seizure at any time of the day or night by any law enforcement officer, probation officer, post-release community supervision officer, or parole officer, with or without a warrant, probable cause, or reasonable suspicion.

(ER 80; *see* ER 52-53, 194-96.) The government also argued that the more specific search condition to which Mr. Lara consented covered the warrantless, suspicionless search of his cell phone because cell phones are no different from ordinary property. (ER 53-55, 196-97; *see* ER 60 (“[D]igital devices are entitled to no greater or lesser Fourth Amendment protection than other personal effects.”).)

According to the government, Mr. Lara’s status as a probationer and his consent to the search condition reduced his privacy interest in his cell phone data to almost nothing, and any remaining interest was outweighed by the government’s legitimate interests in ensuring that he completed probation and did not reoffend. (ER 55-63; 197-202.) With respect to the forensic search of the phone, the government claimed it was necessary because of the possibility that “probationers or their associates will remotely ‘wipe’ data from seized phones to prevent law enforcement from detecting their criminal activity.” (ER 62, 200.)

The government also argued that Mr. Lara subscribed to his cell phone using a false name, which further reduced his legitimate expectation of privacy. (ER 59,

198-99.) As evidence of this fact, the government submitted a computer printout titled “Sprint Requested Information,” which listed the subscriber to the phone number “714-XXX-XXXX” as “Peter Lara,” with an address that matched Mr. Lara’s home address. (ER 92.) According to Officer Fix, this document represented “[a] True [*sic*] and correct copy of relevant excerpts from the subscriber records.” (ER 75.) The government did not offer any additional information about the printout or Mr. Lara’s telephone number.

In response, Mr. Lara disputed having waived all of his Fourth Amendment rights or having consented to the search. (ER 101-03, 208-09.) He emphasized the absence of any evidence that he or someone else could have remotely wiped the phone after it was confiscated. (ER 212.) And he objected to the introduction of the Sprint computer printout as hearsay lacking foundation. (ER 209-10.) But even assuming the printout was properly before the court, there was no evidence on whether the incorrect first name was an alias or a mistake. Mr. Lara plainly provided his true last name and current address, which undercut the government’s theory that he was trying to conceal ownership. (ER 210-11.)

The court held a suppression hearing, at which Probation Officers Fix and Ortiz and Rosa Lara testified. (ER 116.) After hearing argument from the parties, the court denied Mr. Lara’s motion. (ER 179-226.)

The court found that Mr. Lara's status as a probationer, combined with his acceptance of the search condition, "significantly diminished" but did not eliminate his reasonable expectation of privacy in his cell phone. (ER 2-5.) The court was "not persuaded that Mr. Lara waived . . . all Fourth Amendment rights forever as to every place he was ever associated with" when he pleaded guilty in state court. (ER 209.) But the court believed Mr. Lara's probation condition covered warrantless, suspicionless cell phone searches. (ER 4.) Moreover, having rejected Mr. Lara's hearsay objection to the Sprint printout (ER 210), the court found that Mr. Lara's use of the name Peter Lara, although coupled with his correct address, "diminished . . . further" his reasonable expectation of privacy in the cell phone. (ER 5-6.)

The court recognized the government's legitimate interests in reducing crime and reintegrating probationers into society, noting in particular that probationers have an increased recidivism rate compared to the general population. (ER 6-7.) Regarding the GPS data specifically, the court found that the probation officers had "a legitimate fear that the information would be destroyed or somehow compromised," which justified downloading the data without a warrant. (ER 7.) Applying a balancing test, the court concluded that these government interests outweighed Mr. Lara's "small, significantly diminished Fourth Amendment interests." (*Id.*)

According to the court, had the officers searched Mr. Lara's desktop computer, that search would not have been reasonable "because there's no evidence that drug traffickers use the Internet" and Mr. Lara was convicted of a narcotics offense. (ER 4.) But the court believed that, because drug traffickers use cell phones to deal drugs, the search of Mr. Lara's cell phone did not present an analogous situation. (ER 4-5.)

The court emphasized that it was ruling on an issue of first impression. (ER 2; *see* ER 184 (explaining that there was "no case that addresses this context that I found".)) The court thus found "incredibly important . . . the line of cases that permit the police to search cellular telephones incident to arrest as property." (ER 5.) And it found inapposite cases protecting an individual's privacy interest in electronic tracking data because, in Mr. Lara's case, "[t]here was no tracker attached to anything." (ER 7.)

In a subsequent written ruling memorializing the court's findings (ER 11-16), the Court reiterated that it was "unpersuaded by Defendant's argument that digital media is different" (ER 15). "Indeed," wrote the court,

courts have held that digital media is not different. For example, in *People v. Diaz*, 51 Cal. 4th 84 (2011), the California Supreme Court held that a cell phone could be searched as an item seized incident to arrest. No U.S. Supreme Court precedent mandates treating a cell phone any differently than a container.

(*Id.*)

## VI. SUMMARY OF ARGUMENT

There are limited exceptions to the general rule that warrantless searches violate the Fourth Amendment. The Supreme Court has held that warrantless searches of probationers are permissible when accompanied by reasonable suspicion and authorized by a clear and unambiguous condition of probation. This Court has extended that precedent to permit warrantless searches of violent-felon probationers, without reasonable suspicion, where authorized by clear and unambiguous search conditions. The warrantless, suspicionless search of a nonviolent felon's cell phone data, not specifically authorized by any probation condition, stretches this precedent to its breaking point.

The relevant test is a consideration of the totality of the circumstances, balancing the individual's reasonable expectation of privacy against the government's legitimate interests. Following the Supreme Court's decision in *Riley v. California*, there is no question that an individual's privacy interest in his cell phone data is profound. Mr. Lara's status as a probationer did not diminish this interest to the point where the government's interests in preventing recidivism and reintegrating probationers into society outweighed it. And because his probation search condition said nothing about digital media, it similarly did not diminish his reasonable expectation of privacy in his cell phone data. The government's evidence purporting to show that the cell phone was registered in the

name “Peter Lara” was not properly admitted and in any event is a red herring. Mr. Lara, who at minimum registered the phone in his true last name using his current address and exercised control over it, plainly had a reasonable expectation of privacy in its data.

Finally, even if the initial search of Mr. Lara’s cell phone was constitutional, the later forensic search, which revealed GPS location data, was not. The Supreme Court has recognized an individual’s heightened interest in this sort of information, and Mr. Lara’s terms of probation gave him no reason to believe that the government could access it without a warrant.

The district court therefore erred in denying Mr. Lara’s motion to suppress.

## **VII. ARGUMENT**

### **A. Standard of Review**

This Court reviews the district court’s ruling on the motion to suppress de novo and the factual findings in support of the decision for clear error. See *United States v. Song Ja Cha*, 597 F.3d 995, 999 (9th Cir. 2010).

### **B. The District Court Should Have Granted Mr. Lara’s Motion To Suppress**

Mr. Lara argued that the warrantless, suspicionless search of his cell phone violated his Fourth Amendment rights, and asked the district court to suppress evidence found during the search and any fruits thereof, i.e., the gun and ammunition. See *Wong Sun v. United States*, 371 U.S. 471 (1963) (holding the

Fourth Amendment requires the exclusion not only of all evidence directly obtained through its violation but also all “fruits” thereof). The government opposed the motion and the district court denied it, based largely on arguments and a line of cases that have since been rejected by the U.S. Supreme Court.

**1. The Fourth Amendment Protects Against Warrantless Searches, Except in Narrow Circumstances**

Although there does not appear to be any precedent on the legality of a warrantless, suspicionless probation search of a cell phone, the relevant constitutional principles are well settled. The Fourth Amendment to the United States Constitution states:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV. The amendment “incorporates a strong preference for search warrants.” *United States v. Carbajal*, 956 F.2d 924, 930 (9th Cir. 1992). “Warrantless searches are *per se* unreasonable.” *Id.* There are only limited exceptions to this rule, and those exceptions “are jealously and carefully drawn.” *Id.* (internal quotation marks omitted). The Government bears the burden of demonstrating that a warrantless search comes within one of these “narrow” exceptions and is reasonable. *Id.*

One exception is for probation searches that, although warrantless, nonetheless are reasonable under a totality of the circumstances test. In *United States v. Knights*, the Supreme Court held “that the warrantless search of [a probationer], supported by reasonable suspicion and authorized by a condition of probation, was reasonable within the meaning of the Fourth Amendment.” *United States v. Knights*, 534 U.S. 112, 122 (2001). To reach that conclusion, the Court considered “the totality of the circumstances, with the probation search condition being a salient circumstance.” *Id.* at 118 (citation and internal quotation marks omitted). As the Court explained, a “totality of the circumstances” examination is effectively a balancing test “assessing, on the one hand, the degree to which [a search] intrudes upon an individual’s privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.” *Id.* at 118-19 (internal quotation marks omitted). A defendant’s “status as a probationer subject to a search condition informs both sides of that balance.” *Id.* at 119.

In *United States v. King*, this Court took *Knights*’s holding one step further, upholding the *suspicionless* search of a violent felon-probationer who was given clear and unambiguous notice that he was subject to such a search. *United States v. King*, 736 F.3d 805 (9th Cir. 2013) (as amended) (hereafter “*King II*”). In doing so, this Court, like the Supreme Court, weighed the defendant’s reasonable expectation of privacy against the government’s legitimate interests, with the

defendant's status as a probationer and the clear and unambiguous text of the search condition informing that balance. *See id.* at 808-10.

**2. In *Riley v. California*, the Supreme Court Held That Law Enforcement Officers May Not Search an Arrestee's Cell Phone Without a Warrant**

In *Riley v. California*, 134 S. Ct. 2473 (2014), decided after the district court ruled on Mr. Lara's motion, the Supreme Court addressed a different exception to the warrant requirement: search incident to an arrest. Nonetheless, *Riley* is highly relevant to—and perhaps controlling on—the question presented in this case.

The first defendant in *Riley* was arrested and searched incident to that arrest after a police officer discovered illegal guns in his car. *Id.* at 2480. The officer found a “smart phone” in Riley's pocket, i.e., “a cell phone with a broad range of other functions based on advanced computing capability, large storage capacity, and Internet connectivity.” *Id.* The officer searched the data on the phone and discovered words in text messages or a contacts list that were associated with the Bloods gang. *See id.* Later, at the police station, a detective conducted a more thorough search of the phone and discovered photographs and videos that implicated Riley in a shooting. *See id.* at 2480-81. That evidence was admitted at trial, over Riley's objection that the warrantless searches violated the Fourth Amendment. *See id.* at 2481. The California Court of Appeal affirmed Riley's conviction, relying the same California Supreme Court decision cited by the

district court in this case, *People v. Diaz*, which had upheld warrantless cell phone searches incident to arrest. *See Riley*, 134 S. Ct. at 2481.

A second defendant in *Riley*, Petitioner Wurie, was arrested after officers conducting routine surveillance saw him dealing drugs. *See id.* Upon arrival at the police station, officers confiscated two cell phones from Wurie. *See id.* “The one at issue here was a ‘flip phone,’ a kind of phone that is flipped open for use and that generally has a smaller range of features than a smart phone.” *Id.* After Wurie received repeated calls from a number listed as “my house,” officers opened the phone, accessed its call log to identify the number, and traced that number to a residence. *See id.* The officers then obtained a warrant to search the home, where they discovered drugs, guns, and cash. *See id.* That evidence was admitted at trial, over Wurie’s objection that it was the fruit of the unlawful search of his phone. *See id.* at 2482. The First Circuit reversed, holding “that cell phones are distinct from other physical possessions that may be searched incident to arrest without a warrant, because of the amount of personal data cell phones contain.” *Id.*

The U.S. Supreme Court unanimously ruled in favor of both petitioners. *See id.* at 2495. The Court held that law enforcement officers may not, “without a warrant, search digital information on a cell phone seized from an individual who has been arrested.” *Id.* at 2480. In reaching this conclusion, the Court made several relevant points.

First, the Court emphasized that “modern cell phones, which are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy,” are less telephones than miniature personal computers. *Id.* at 2484. Unlike ordinary “physical objects,” *id.*, “[c]ell phones . . . place vast quantities of personal information literally in the hands of individuals,” *id.* at 2485. “The term ‘cell phone’ is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone.” *Id.* at 2489.

For this reason, when it comes to warrantless searches, cell phones are different. “A search of the information on a cell phone bears little resemblance to” a search of an ordinary object. *Id.* at 2485. Saying the two are “materially indistinguishable . . . is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together.” *Id.* at 2488. Thus, although a “mechanical application” of the Court’s search incident to arrest precedent might have pointed to a different result, *id.* at 2484, the Court “decline[d] to extend [that precedent] to searches of data on cell phones, and h[e]ld instead that officers must generally secure a warrant before conducting such a search,” *id.* at 2485.

Second, although an arrestee has “reduced privacy interests upon being taken into police custody,” the Court emphasized that this fact “does not mean that the Fourth Amendment falls out of the picture entirely.” *Id.* at 2488. “To the contrary, when privacy-related concerns are weighty enough a search may require a warrant, notwithstanding the diminished expectations of privacy of the” individual. *Id.* (internal quotation marks omitted). And in the case of cell phone data, the Court held, privacy-related concerns are at their peak.

“Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse.” *Id.* at 2488-89. “[T]heir immense storage capacity” and “ability to store many different types of information” have “several interrelated consequences for privacy.” *Id.* at 2489. “First, a cell phone collects in one place many different types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record.” *Id.* “Second, a cell phone’s capacity allows even just one type of information to convey far more than previously possible. The sum of an individual’s private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions . . . .” Third, a cell phone records all of a person’s communications over a lengthy period of time. *See id.* “Finally, there is an element of pervasiveness that characterizes cell phones but not physical records.” *Id.* at 2490. “[T]he more than

90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate.”

*Id.* By contrast, individuals rarely possess such “a cache of sensitive personal information” in paper form. *Id.*

The data stored on a cell phone is not just quantitatively different from the data kept in physical records; it is “qualitatively different.” *Id.* Cell phone data can reveal “an individual’s private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD.” *Id.* It “can also reveal where a person has been . . . and can reconstruct someone’s specific movements down to the minute.” *Id.* In particular, the GPS data found on an individual’s cell phone “reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.” *Id.* (internal quotation marks omitted). In other words, the data stored on a cell phone, much like the data stored on a computer, “can form a revealing montage of the user’s life.” *Id.*

In addition to these concerns, there is the possibility that “the data a user views on many modern cell phones may not in fact be stored on the device itself,” but rather “on remote servers.” *Id.* at 2491. “Cell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference”; “officers searching a phone’s data would not

typically know whether the information they are viewing was stored locally at the time of the arrest or has been pulled from the cloud.” *Id.*

These multiple differences between cell phones and physical objects led the Court to conclude that “a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.” *Id.*

Third, the Court rejected the argument that because cell phones are “vulnerable to . . . evidence destruction” through “remote wiping and data encryption,” *id.* at 2486, warrantless searches may be necessary. There is “little reason to believe that either problem is prevalent.” *Id.* The Court distinguished between “seiz[ing] and secur[ing] [a] cell phone[] to prevent destruction of evidence while seeking a warrant,” which is lawful, and searching a cell phone without a warrant, which is not. *Id.*

Fourth, although the particular searches in *Riley* were conducted incident to arrest, the Court addressed the issue of cell phone searches more generally, concluding that while “the information on a cell phone is [not] immune from search[,] . . . a warrant is generally required before such a search.” *Id.* at 2493.

Fifth and finally, the Court recognized that “[c]ell phones have become important tools in facilitating coordination and communication among members of criminal enterprises,” and acknowledged that its decision in *Riley* would “have an impact on the ability of law enforcement to combat crime.” *Id.* at 2493. That was okay. “Privacy comes at a cost.” *Id.*

### **3. The Warrantless, Suspicionless Search of a Probationer’s Cell Phone Is Unconstitutional**

Almost four million adults—1 in 62 residents—are on probation in this country. Erinn J. Herberman and Thomas P. Bonczar, *Probation and Parole in the United States, 2013*, Bureau of Justice Statistics 1-3 (Oct. 2014), <http://www.bjs.gov/content/pub/pdf/ppus13.pdf>. In California alone, there are almost 300,000 adult probationers. *Id.* at 7. The decision in this case, therefore, will have far-reaching implications.

#### **a. A Cell Phone Search Implicates Heightened Privacy Concerns**

“Modern cell phones . . . hold for many Americans the privacies of life.” *Riley*, 134 S. Ct. at 2494-95 (internal quotation marks omitted). The *Riley* Court emphasized over and over the “weighty” privacy interest that individuals—even those with diminished privacy expectations—have in data stored on their cell phones. *See id.* at 2488-91; *see also id.* at 2497 (Alito, J., concurring) (“[B]ecause

of the role that these devices have come to play in contemporary life, searching their contents implicates very sensitive privacy interests.”).

Thus, although cases addressing warrantless searches of ordinary property are instructive on how to analyze a warrantless cell phone search (i.e., conduct a “totality of the circumstances” balancing test), they do not control the ultimate result. To the contrary, the unique concerns presented by warrantless cell phone searches “call[] for a new balancing of law enforcement and privacy interests.” *Id.* at 2496-97.

The *Riley* Court gave ample reasons for recognizing a substantial privacy interest in cell phone data. Yet there are also racial and socio-economic factors at work that caution against curtailing cell phone privacy rights. Disproportionate numbers of low-income, black, and Latino Americans rely on cell phones for tasks that wealthier and white Americans typically perform on traditional computers. According to a 2011 survey, “young adults, minorities, those with no college experience, and those with lower household income levels who owned smartphones were more likely to say that their phone was their main source of internet access.” Kathryn Zickuhr & Aaron Smith, *Digital Differences*, Pew Research Center 19 (Apr. 13, 2012), [http://www.pewinternet.org/files/old-media//Files/Reports/2012/PIP\\_Digital\\_differences\\_041312.pdf](http://www.pewinternet.org/files/old-media//Files/Reports/2012/PIP_Digital_differences_041312.pdf).

With respect to race, black Americans are less likely than white Americans to have broadband at home, but that “digital divide” starts to disappear when cell phones are taken into account. Black and white Americans own cell phones at identical rates. With those phones, ten percent of black adults are able to access the internet, despite lacking broadband connections at home. See Aaron Smith, *African Americans and Technology Use*, Pew Research Center 1, 5, 7, 8 (Jan. 6, 2014), <http://www.pewinternet.org/files/2014/01/African-Americans-and-Technology-Use.pdf>. Similarly, “Latino internet users are more likely than white internet users to say they go online using a mobile device . . . .” Mark Hugo Lopez, Ana Gonzalez-Barrera, & Eileen Patten, *Closing the Digital Divide: Latinos and Technology Adoption*, Pew Research Center 6 (Mar. 7, 2013), [http://www.pewhispanic.org/files/2013/03/Latinos\\_Social\\_Media\\_and\\_Mobile\\_Technology\\_Adoption\\_03-2013\\_final.pdf](http://www.pewhispanic.org/files/2013/03/Latinos_Social_Media_and_Mobile_Technology_Adoption_03-2013_final.pdf).

With respect to income, for many Americans, a cell phone is the only computer they can afford. See Gerry Smith, *Smartphones Bring Hope, Frustration as Substitute for Computers*, Huffington Post (June 6, 2012), [http://www.huffingtonpost.com/2012/05/25/smartphones-digital-divide\\_n\\_1546899.html](http://www.huffingtonpost.com/2012/05/25/smartphones-digital-divide_n_1546899.html). Only half of the adults in low-income households have broadband internet at home, but the vast majority own a cell phone. See Smith, *African Americans and Technology Use*, at 5, 7.

As the federal government, analyzing 2011 census data, put it, “smartphones appear to be leveling the Internet use disparities traditionally present for race and ethnicity groups.” Thom File, *Computer and Internet Use in the United States*, U.S. Census Bureau, 12 (May 2013), <http://www.census.gov/prod/2013pubs/p20-569.pdf>. Presumably that trend has continued since 2011, as the cost of smartphones has dropped. See Dan Rowinski, *Dropping Prices Are Driving Mass Smartphone Adoption Across the World*, readwrite (Nov. 27, 2013), <http://readwrite.com/2013/11/27/cheap-smartphones-drive-global-mobile-adoption>.

In sum, the modern reality is that traditionally disenfranchised groups increasingly rely on cell phones as de facto computers. The need to recognize a robust privacy interest in cell phone data, as the Supreme Court did in *Riley*, therefore takes on added social weight.

**b. Mr. Lara Retained a Reasonable Expectation of Privacy in the Data Stored on His Cell Phone, Despite His Status as a Probationer**

Mr. Lara concedes that, in this case, his privacy interest was somewhat diminished by his status as a probationer. The question is, by how much? The district court thought the diminution “significant,” resulting in a “small” residual privacy interest. (ER 7.) But this analysis was doubly flawed. First, because the court assumed that cell phones are ordinary objects and thus misunderstood the

privacy interest to begin with. And second, because probationers have greater protection against suspicionless searches than the court recognized.

The *Riley* Court’s treatment of arrestees’ privacy interests in their cell phone data is instructive. Similar to probationers, arrestees have “diminished” “expectations of privacy.” *Maryland v. King*, \_\_\_ U.S. \_\_\_, 133 S. Ct. 1958, 1978 (2013) (alteration and internal quotation marks omitted). In some ways, their expectations of privacy are less than those of probationers, for an arrestee is subject not only to a search of “the property in his immediate possession,” but also a search of his person that “may involve a relatively extensive exploration, including requiring at least some detainees to lift their genitals or cough in a squatting position.” *Id.* (alterations, citation, and internal quotation marks omitted). And yet, as *Riley* makes clear, arrestees maintain reasonable—indeed, substantial—expectations of privacy in their cell phone data. *See Riley*, 134 S. Ct. at 2488.

Even assuming that probationers’ reasonable expectations of privacy are less than those of arrestees, they are, as a matter of established precedent, greater than those of incarcerated inmates and parolees. *See Samson v. California*, 547 U.S. 843, 850 & n.2 (2006); *United States v. King*, 687 F.3d 1189 (9th Cir. 2012) (en banc). “Probation is . . . one point (or, more accurately, one set of points) on a continuum of possible punishments ranging from solitary confinement in a

maximum-security facility to a few hours of mandatory community service.”

*Griffin v. Wisconsin*, 483 U.S. 868, 874 (1987). In California, probation “is generally reserved for convicted criminals whose conditional release into society poses minimal risk to public safety and promotes rehabilitation.” *People v. Olguin*, 45 Cal. 4th 375, 379 (2008) (internal quotation marks omitted); *see King II*, 736 F.3d at 815 (Berzon, J., dissenting) (explaining that California probationers “may have been convicted of an infraction, misdemeanor, or felony” and have been found by a judge to present a minimal danger to society) (citing Cal. Penal Code § 1203). Thus, although probationers reasonably expect their rights to be somewhat curtailed, *see Griffin*, 483 U.S. at 874, they retain significantly greater rights than parolees and inmates.

But if officers have unfettered access to probationers’ cell phone data, probationers are treated like prisoners. Perhaps worse. While a prisoner expects the government to monitor his custodial communications, he surely does not expect that “all of his communications . . . for the past several months”—including those made prior to incarceration—are fair game. *Riley*, 134 S. Ct. at 2489. But in the case of cell phones, the data “can date back to the purchase of the phone, or even earlier”—including to a time before a probationer was charged or convicted. *Id.* at 2489. If officers are permitted to conduct warrantless, suspicionless searches

of probationers' cell phone data, probationers will, in this way, be subject to more profound intrusions into their private communications than even prisoners.

Importantly, a probationer's reasonable expectation of privacy is greatest when there is *no* suspicion of wrongdoing. The Supreme Court has never upheld a warrantless, suspicionless search of a probationer qua probationer. In *Knights*, the Court found that a warrantless probation search "supported by reasonable suspicion and authorized by a condition of probation" was reasonable. *Knights*, 534 U.S. at 122. In *Griffin*, the Court approved of warrantless probation searches conducted pursuant to a regulation that required reasonable suspicion. *See Griffin*, 483 U.S. at 872-76. It is questionable whether the Supreme Court would uphold warrantless, suspicionless probation searches—of cell phones or otherwise—under any circumstances. *See Knights*, 534 U.S. at 120 n.6 (reserving the question); *King II*, 736 F.3d at 816-17 (Berzon, J., dissenting) (suggesting not); *United States v. Scott*, 450 F.3d 863, 866-68 (9th Cir. 2006) (recognizing limits on the extent of Fourth Amendment concessions the government may lawfully extract in exchange for a probation sentence). And it is notable that the district court in this case relied heavily on *Knights*, without apparent recognition that it is a "reasonable suspicion" case. (ER 2-4, 14-15.)

To be sure, this Court has extended the Supreme Court's jurisprudence to cover certain warrantless, suspicionless probation searches—but only once, and in

deliberately narrow circumstances. In *King II*, this Court upheld the suspicionless probation search of “a violent felon[,]” explicitly and repeatedly cabining the decision to similar individuals. *King II*, 736 F.3d at 810; *see id.* at 809 (relying on “the serious and intimate nature of [the] underlying conviction for the willful infliction of corporal injury on a cohabitant”). The *King II* panel pointedly did not address suspicionless probation searches of “lower level offenders.” *Id.* at 810.

It may be that, in certain circumstances, warrantless searches of probationers’ cell phones, *with reasonable suspicion*, are constitutional. That is not a question presented by this case. Here, the probation search was routine and suspicionless. In those circumstances, Mr. Lara reasonably expected that his cell phone data would remain private.

**c. Mr. Lara’s State Probation Condition Did Not Provide Notice That the Data on His Cell Phone Was Subject to Warrantless, Suspicionless Search**

What effect did Mr. Lara’s probation search condition have on his reasonable expectation of privacy? None. The condition required him to submit his “person and property[,] including any residence, premises, container, or vehicle under [his] control,” to a warrantless, suspicionless search at any time. (ER 38, 71, 83.) It did not mention cell phones or digital media at all. As the Supreme Court made pellucidly clear in *Riley*, cell phones are not ordinary property, nor are they

analogous to typical containers such as “a cigarette pack, a wallet, or a purse.”

*Riley*, 134 S. Ct. at 2489.

Because digital media are different from ordinary property, terms of supervision regularly distinguish between the two. For example, the statute setting forth standard conditions of federal probation includes a discretionary condition allowing officers to search the defendant’s “person, and any property, house, residence, vehicle, papers, computer, other electronic communication or data storage devices or media, and effects.” 18 U.S.C. § 3563(b)(23). Even without statutory guidance, when courts wish to include digital media in supervisory search conditions, they know how to do so. *See, e.g., United States v. King*, 608 F.3d 1122, 1125-26 (9th Cir. 2010) (discussing federal supervised release condition authorizing searches of defendant and “his property (including any computer ‘confined to his own use’)”); *People v. Realmuto*, 2010 WL 3221963, at \*5 (Cal. Ct. App. Aug. 17, 2010) (unpublished) (discussing probation conditions authorizing searches of defendant’s “person and property” as well as “computers and recordable media”); *People v. Lord*, 2009 WL 2244172, at \*1 (Cal. Ct. App. July 28, 2009) (unpublished) (discussing probation condition authorizing searches of defendant’s “person, vehicle, residence, property, personal effects, computers and recordable media”); *People v. Ramirez*, 2009 WL 2197070, at \* (Cal. Ct. App. July 24, 2009) (unpublished) (same). The absence of such terms from Mr. Lara’s

probation search condition is an indication of their exclusion. *Cf. Nijjar v. Holder*, 689 F.3d 1077, 1084 n.36 (9th Cir. 2014) (“The doctrine of *expressio unius est exclusio alterius* teaches that omissions are the equivalent of exclusions when a statute affirmatively designates certain persons, things, or manners of operation.” (alterations and internal quotation marks omitted)).

In a related context, this Court has held that a search warrant must specifically authorize the search of digital media; if it does not, digital media are outside its scope. *See United States v. Payton*, 573 F.3d 859, 861-64 (9th Cir. 2009). This rule, like the one set forth in *Riley*, is based in part on the recognition that digital media are different from “other containers.” *Id.* at 862. That distinction is important, because the language of a warrant “inform[s] the person subject to the search just what may be searched.” *Id.*

So too in the probation search context. A probationer’s search condition can diminish his reasonable expectation of privacy only to the extent that it provides “clear[]” and “unambiguous” notice of its scope. *Knights*, 534 U.S. at 119; *see Samson*, 547 U.S. at 852 (considering “the plain terms” of a search condition); *King II*, 736 F.3d at 808-09 (finding “clear and unambiguous” language of probation search condition is a “salient circumstance” in evaluating a probationer’s reasonable expectation of privacy (internal quotation marks omitted)). If the language of a probation condition is not clear and unambiguous, it does not

provide the requisite notice and cannot diminish a probationer's reasonable expectations.

Here, the district court specifically found that the “the plain language of the search condition itself, submit your person and property,” is subject to differing interpretations. (ER 5 (“Is it required to include cellular telephones? No. No, it's not. Does it by the fact that it is not mentioned mean it's entitled to different treatment . . . ? No.”).) That is the precise definition of ambiguity. Because the condition is neither clear nor unambiguous as to whether it covers cell phones, it has no effect on Mr. Lara's reasonable expectation of privacy.

In sum, it was reasonable for Mr. Lara to believe that his probation search condition, which said nothing about cell phones, did not cover the search of his phone. Because cell phones are unlike traditional property, and because courts explicitly refer to digital media when they wish to include it, his subjective belief on this point (ER 39), unchallenged by the government through cross-examination (ER 118), was objectively reasonable. *See United States v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. 2007) (“An individual has a reasonable expectation of privacy if he can demonstrate a subjective expectation that his activities would be private, and he can show that his expectation was one that society is prepared to recognize as reasonable.” (alteration and internal quotation marks omitted)).

**d. The Sprint Subscriber Record Was Not Properly Admitted and in Any Event Did Not Affect Mr. Lara's Reasonable Expectation of Privacy**

The district court believed that Mr. Lara's reasonable expectation of privacy in his cell phone was somewhat diminished because he subscribed to the phone in the name Peter Lara, using his correct address. (ER 5-6.) There was, however, no properly admitted evidence to support the court's conclusion.

Recall that the government submitted a one-page computer printout titled "Sprint Requested Information." (ER 92.) Probation Officer Fix stated in her declaration that the document was "[a] True [*sic*] and correct copy of relevant excerpts from the subscriber records." (ER 75.) Neither the record itself, nor Officer Fix's declaration, explain who created the document, when or how it was created, or how it came into Officer Fix's possession. It is not signed or authenticated in any way. In the form presented to the court, the record indicates that an unspecified phone number beginning with area code "714" was registered in the name "Peter Lara" at Mr. Lara's home address. The government did not present any evidence linking the record to the particular cell phone at issue. Nor was there any evidence showing how or why, if the Sprint record referred to Mr. Lara's cell phone, it contained the name "Peter."

In other words, the Sprint Subscriber Record was unauthenticated, irrelevant hearsay. Officer Fix had no personal knowledge of the information in the record.

*See* Fed. R. Evid. 602, 901. And the record was irrelevant because there was no evidence tying it to the phone at issue. *See* Fed. R. Evid. 401.

Even putting aside these evidentiary problems, the Peter Lara name is a red herring. No one disputes that the cell phone actually belonged to Mr. Lara. Neither the government nor the court explained why subscribing to a cell phone in the wrong first name, with the correct last name and address, opens the data on that phone up to public scrutiny. Absent fraud or identity theft, using a pseudonym to obtain property is not illegal. Assuming Mr. Lara intentionally subscribed to the phone in the name Peter, he had no reason to expect that the text messages, photographs, and location data stored on it were no longer private—especially given his use of his correct last name and current address.

The cases cited by the government in district court are inapposite. (ER 59.) In *Skinner*, the court found that Melvin Skinner did not have a privacy interest in a cell phone subscribed to in the name “Tim Johnson” at a fictitious address, purchased by someone else for the express purpose of using it in a marijuana trafficking conspiracy, and referred to by members of that conspiracy as one of the “super secret phones” that the group frequently discarded and replaced. *See United States v. Skinner*, 2007 WL 1556596, at \*2-4, 15, 17 (E.D. Tenn. May 24, 2007) (unpublished). In *Suarez-Blanca*, the court found that Jesus Rodriguez did not have a privacy interest in a cell phone subscribed to in the name “Felix Baby” at a

fictional address, where there was nothing linking Rodriguez to the name or address. See *United States v. Suarez-Blanca*, 2008 WL 4200156, at \*2-3, 5-7 (N.D. Ga. Apr. 21, 2008) (unpublished). And in *Davis*, the court found that Jefferson Davis did not have a privacy interest in a cell phone subscribed to in the name “Josh Smith,” where “Defendant’s true name and address were not attached to the telephone number in any manner,” and it was not clear whether Josh Smith was the actual subscriber or an alias. See *United States v. Davis*, 2011 WL 2036463, at \*3 (D. Or. May 24, 2011) (unpublished). In each case, the search at issue was the remote access of cell phone location or subscriber information, not the in-person search of data stored on a cell phone. These cases bear little resemblance to Mr. Lara’s.

Judge O’Scannlain’s concurrence in *United States v. Lozano*, cited by the district court (ER 15), is even farther afield. *United States v. Lozano*, 623 F.3d 1055, 1062-65 (9th Cir. 2010) (O’Scannlain, J., specially concurring). In the specific context of the delivery of mail, Judge O’Scannlain concluded that “a nonaddressee does not have standing [to assert a Fourth Amendment claim over a package] despite his association with the street address listed on the package.” *Id.* at 1064. Judge O’Scannlain distinguished *Lozano* from other cases holding “that a defendant has a legitimate expectation of privacy in mail addressed to his ‘alter ego,’” because “Lozano’s theory was that he was not the rightful recipient of the

package. He denied that Bill Cormer [the addressee] was his alias.” *Id.* Given these facts, *Lozano* has little relevance to Mr. Lara’s case. But perhaps most importantly, the *Lozano* majority did not adopt Judge O’Scannlain’s reasoning. Quite the opposite—the majority analyzed whether Lozano’s Fourth Amendment rights with respect to the package had been violated. *See id.* at 1060-61 (per curiam).

More relevant are the cases where “[c]ourts have determined that an individual may assert a reasonable expectation of privacy in [property] addressed to [him] under [a] fictitious name[,]” as well as property “for which he uses an alias to register” but over which he exercises exclusive control. *Suarez-Blanca*, 2008 WL 4200156, at \*6 n.6 (collecting cases). Where there is evidence to “link” the person asserting the privacy interest to the property, in addition to possession, that individual has an objective expectation of privacy in it. *Id.* at \*7.

Here, even accepting the government’s evidence and assuming the unproven fact that Mr. Lara intentionally registered his cell phone in the name Peter Lara, the use of his true last name and current address, combined with his possession over the phone, make Mr. Lara’s subjective expectation of privacy in the phone’s data objectively reasonable.

**e. The Government’s Interests Do Not Outweigh Mr. Lara’s Reasonable Expectation of Privacy**

The relevant government interests are well established. They flow from “the very assumption of the institution of probation . . . that the probationer is more likely than the ordinary citizen to violate the law.” *Knights*, 534 U.S. at 120 (internal quotation marks omitted). Because of this assumption, the State has a legitimate “dual interest in integrating probationers back into the community and combating recidivism.” *Samson*, 547 U.S. at 849; *see Knights*, 534 U.S. at 120 (referring to the “dual concern” of reintegration and recidivism).

In *King II*, this Court interpreted the Supreme Court’s “dual interest” cases as actually containing three interests: reintegration, preventing recidivism, and “discovering criminal activity and preventing destruction of evidence.” *King II*, 736 F.3d at 809. The district court similarly cited these government interests. (ER 6-7.) The Supreme Court, in contrast, has rejected as illegitimate general law enforcement goals of ferreting out criminal activity and collecting evidence, when proffered by the government in support of warrantless searches and seizures. *See, e.g., Ferguson v. City of Charleston*, 532 U.S. 67, 82-86 & nn.20-23 (2001); *City of Indianapolis v. Edmond*, 531 U.S. 32, 41-44 & n.1 (2000).

Whether two or three, Mr. Lara does not dispute that the government has “important interests” when it comes to supervising probationers. *King II*, 736 F.3d

at 809. Nonetheless, these interests are insufficient to outweigh Mr. Lara's privacy interest in this case for three reasons.

First and most importantly, Mr. Lara's reasonable expectation of privacy in his cell phone data is so great that it tips the balance in favor of suppression. *See Riley*, 134 S. Ct. at 2488 (explaining that "when privacy-related concerns are weighty enough," as they are in the case of cell phone searches, they outweigh the government's otherwise legitimate interests).

Second, the government's interests in probation search cases are forward-looking. "In the cell phone context, however, it is reasonable to expect that incriminating information will be found on a phone regardless of when the crime occurred." *Id.* at 2492. Government interests in preventing *future* crimes and reintegrating probationers into society provide no justification for reviewing the wealth of pre-offense data a probationer likely retains on his cell phone.

And third, 73-percent of California probationers now successfully complete their terms of supervision without committing new offenses. *See* Chief Probation Offices of California, *CPOC Adult Probation Business Model*, at 9 (Dec. 2009), <http://www.cpoc.org/assets/positionpapers/cpoc%20adult%20prob%20business%20model.pdf>. Of course, that means that 27-percent do not, and Mr. Lara does not dispute that probationers commit crimes at higher rates than nonprobationers. But the data are important. In *Knights*, the Supreme Court specifically "assess[ed] the

governmental interest side of the balance” in light of a 43-percent recidivism rate. *Knights*, 534 U.S. at 120 (citing 1992 data). In *Samson*, a parole search case, the Court took particular note of “[t]he empirical evidence” that California parolees have “a 68- to 70-percent recidivism rate.” *Samson*, 547 U.S. at 853; *see also id.* at 854. Today, the evidence supports a weaker government interest.

For all of these reasons, the government’s legitimate interests did not outweigh Mr. Lara’s reasonable expectation of privacy in his cell phone data.

**f. Even if the Initial Search of Mr. Lara’s Phone Was Constitutional, the Warrantless Search of the GPS Data on His Phone Was Not**

The probation officers’ warrantless search of the GPS data on Mr. Lara’s cell phone was particularly intrusive, and the purported government reasons for the search especially feeble. Accordingly, even if the initial search of Mr. Lara’s cell phone was lawful, the later forensic search was not.

Like many modern cell phones, Mr. Lara’s phone was GPS-enabled, storing data on where the phone (and, by extension, he) had been. As the Supreme Court recently explained, this sort of “[h]istoric location information,” which “is a standard feature on many smart phones[,] . . . can reconstruct someone’s specific movements down to the minute, not only around town but also within a particular building.” *Riley*, 134 S. Ct. at 2490. Because searches for GPS data reveal “a precise, comprehensive record of a person’s public movements that reflects a

wealth of detail about her familial, political, professional, religious, and sexual associations,” they pose a unique concern. *Id.* (internal quotation marks omitted).

*Riley*’s recognition that searches for GPS data are particularly intrusive was not novel. Thirty years ago, the Supreme Court held that government monitoring of a person or article not in public view by means of an electronic tracking device presents “a serious threat to privacy interests.” *United States v. Karo*, 468 U.S. 705, 716 (1984); *see also United States v. Jones*, \_\_\_ U.S. \_\_\_, 132 S. Ct. 945, 954-57 & n.\* (2012) (Sotomayor, J., concurring) (discussing heightened privacy concerns accompanying government searches for GPS data). In light of this precedent, the government can hardly dispute that the search for GPS data on Mr. Lara’s phone implicated an exceptionally strong privacy interest.

Further, Mr. Lara had no reason to believe that his status as a probationer diminished his significant interest in this sensitive information. Nothing in Mr. Lara’s probation terms suggested that probation officers were authorized to access data tracking his every movement. Mr. Lara was not subject to a GPS monitoring condition, nor was he required to report his minute-by-minute location to the probation office. (ER 71-72.)

In contrast to Mr. Lara’s considerable expectation of privacy, the government’s interests in conducting a forensic search of his cell phone and reviewing its GPS data were exceedingly weak. The district court thought the

search supported by the probation officers’ “legitimate fear that the information would be destroyed or somehow compromised.” (ER 7.) But *Riley* rejects this purported interest wholesale, finding “little reason to believe that [an evidence destruction] problem is prevalent.” *Riley*, 134 S. Ct. at 2486; *see id.* at 2486-87.

No other legitimate government interests remain. Once Mr. Lara had been arrested and detained, the forensic search could do nothing to further the government’s interests in preventing him from committing further crimes or reintegrating him into society. And of course, it was not intended to. The search plainly was an effort to collect evidence of past criminal wrongdoing—which, as discussed above, is not a legitimate purpose for a *warrantless* search.

In this case, the district court did not adequately account for the intrusiveness of the forensic search, and gave undo weight to the government’s proffered interests. Correct application of the “totality of the circumstances” balancing test requires suppression of the fruits of the forensic search, even if the initial cell phone search was lawful.

### **VIII. CONCLUSION**

For the foregoing reasons, Mr. Lara respectfully requests that this Court reverse the district court’s denial of his motion to suppress the fruits of the unlawful searches of his cell phone, including the gun and ammunition found at his

parents' house, and remand with instructions to permit him to withdraw his conditional guilty plea.

Respectfully submitted,

HILARY POTASHNER  
Acting Federal Public Defender

DATED: November 3, 2014

By /s/ Alexandra W. Yates

ALEXANDRA W. YATES  
Deputy Federal Public Defender  
Attorneys for Defendant-Appellant

**CERTIFICATE OF RELATED CASES**

Counsel for appellant certifies that she is unaware of any pending case presenting an issue related to those raised in this brief.

DATED: November 3, 2014

/s Alexandra W. Yates  
ALEXANDRA W. YATES

## CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. 32(a)(7)(C) and Circuit Rule 32-1, I certify that this opening brief is proportionally spaced, has a typeface of 14 points or more, and contains approximately 9691 words.

DATED: November 3, 2014

/s Alexandra W. Yates  
ALEXANDRA W. YATES

## **CERTIFICATE OF SERVICE**

I hereby certify that on November 3, 2014, I electronically filed the foregoing **APPELLANT'S OPENING BRIEF** with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

*Lorena Macias*  
LORENA MACIAS

\*\*\*NOTE TO PUBLIC ACCESS USERS\*\*\* Judicial Conference of the United States policy permits attorneys of record and parties in a case (including pro se litigants) to receive one free electronic copy of all documents filed electronically, if receipt is required by law or directed by the filer. PACER access fees apply to all other users. To avoid later charges, download a copy of each document during this first viewing.

United States Court of Appeals for the Ninth Circuit

Notice of Docket Activity

The following transaction was entered on 11/03/2014 at 5:37:27 PM PST and filed on 11/03/2014

**Case Name:** USA v. Paulo Lara

**Case Number:** [14-50120](#)

**Document(s):** [Document\(s\)](#)

**Docket Text:**

Submitted (ECF) Opening Brief for review. Submitted by Appellant Paulo Lara. Date of service: 11/03/2014. [9300240] [14-50120] (AWY)

**Notice will be electronically mailed to:**

Mr. Jean-Claude Andre, Assistant U.S. Attorney  
Alexandra Wallace Yates, Federal Public Defender  
Mr. Ryan Weinstein, Assistant U.S. Attorney

The following document(s) are associated with this transaction:

**Document Description:** Main Document

**Original Filename:** Lara AOB FINAL wTables.pdf

**Electronic Document Stamp:**

[STAMP acecfStamp\_ID=1106763461 [Date=11/03/2014] [FileNumber=9300240-0]

[23b4d6075a699ee07d12390ff3dda236511c009ee2cbe671776fc115a67dab06e1efe702f5d4386414181f3252e2fb9e8fb1188683060df906aef977ddeb431]]