

No.

IN THE SUPREME COURT OF THE UNITED STATES

OCTOBER TERM, 2017

CARLOS MARTINEZ,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Petition for Writ of Certiorari to the
United States Court of Appeals for the Ninth Circuit

PETITION FOR WRIT OF CERTIORARI

STEVEN G. KALAR
Federal Public Defender
GEOFFREY A. HANSEN
Chief Assistant Federal Public Defender
450 Golden Gate Avenue, 19th Floor
San Francisco, California 94102
(415) 436-7700

** Counsel of Record for Petitioner*

QUESTION PRESENTED

Whether an evidentiary hearing under *Frank v. Delaware*, 438 U.S. 154 (1978) is warranted where the search warrant affidavit suggested that the residence to be searched was assigned a certain IP address at the time it was used to offer child pornography for sharing and downloading, but failed to disclose that the IP address was *dynamic* and that the only available evidence showed that it was assigned to the targeted residence more than a month *after* the illegal Internet conduct.

PARTIES TO THE PROCEEDINGS

The parties to the proceedings are set forth in the caption to this Petition.

CONTENTS

QUESTION PRESENTED	I
PARTIES TO THE PROCEEDINGS.....	II
TABLE OF CONTENTS	III
TABLE OF AUTHORITIES	IIIV
PETITION FOR WRIT OF CERTIORARI	1
OPINION BELOW	1
JURISDICTION	1
RELEVANT CONSTITUTIONAL PROVISION	1
STATEMENT OF THE CASE.....	2
I. INVESTIGATION OF IP ADDRESS 76.126.194.166.....	2
II. OFFICER ICHIGE OBTAINS THE PENNY ROYAL SEARCH WARRANT – BUT FAILS TO INFORM THE MAGISTRATE THAT THE TARGETED IP ADDRESS IS DYNAMIC AND THAT COMCAST IDENTIFIED AN ASSIGNED SUBSCRIBER FOR A DATE MORE THAN A MONTH AFTER THE ILLEGAL CONDUCT BEING INVESTIGATED	5
III. THE EXECUTION OF THE PENNY ROYAL WARRANT AND INTERROGATION OF MR. MARTINEZ.....	7
IV. MR. MARTINEZ’S MOTION TO SUPPRESS	8
V. MR. MARTINEZ’S CONVICTION AND APPELLATE PROCEEDINGS.....	11
REASONS FOR GRANTING THE WRIT	11
A. <u>General Framework of <i>Franks</i>-Based Fourth Amendment Claims</u>	12
B. <u>Omission of the Fact That a Dynamic IP Address Was Assigned to a Certain User on a Date Other Than the Date of the Offending Child Pornography Offenses Is Material to the Probable Cause Determination.....</u>	14
C. <u>The Ninth Circuit Erred in Failing to Recognize that the Penny Royal Warrant Affidavit Deliberately or Recklessly Omitted Material Information That the Relevant IP Address Was Dynamic and Was Assigned to Ms. Botelho More Than a Month After the Illegal Online Activities.....</u>	20
CONCLUSION	22
CERTIFICATE OF COMPLIANCE	224

TABLE OF AUTHORITIES

Cases

<i>Brooks v. AM Resorts, L.L.C.</i> , 954 F. Supp. 2d 331 (E.D. Pa. 2013)	17-18
<i>Call of the Wild Movie, L.L.C. v. Does 1-1,062</i> , 770 F. Supp. 2d 332 (D.D.C. 2011)	16, 18
<i>Chism v. Washington</i> , 661 F.3d 380 (9th Cir. 2011)	14, 22
<i>Disney Enters. v. Rea</i> , 940 F. Supp. 2d 288 (E.D. Va. 2013)	18
<i>Franks v. Delaware</i> , 438 U.S. 154 (1978)	12, 13
<i>Illinois v. Gates</i> , 462 U.S. 213 (1983)	14
<i>Klimas v. Comcast Cable Commc'ns, Inc.</i> , 465 F.3d 271 (6th Cir. 2006)	17
<i>Liston v. County of Riverside</i> , 120 F.3d 965 (9th Cir. 1997)	13
<i>London-Sire Records, Inc. v. Doe 1</i> , 542 F. Supp. 2d 153 (D. Mass. 2008)	<i>passim</i>
<i>United States v. Christy</i> , 785 F. Supp. 2d 1004 (D.N.M. 2011)	18
<i>United States v. Craighead</i> , 539 F.3d 1073 (9th Cir. 2008)	15
<i>United States v. DeLeon</i> , 979 F.2d 761 (9th Cir. 1992)	13
<i>United States v. Hay</i> , 231 F.3d 630 (9th Cir. 2000)	5
<i>United States v. Jacobs</i> , 986 F.2d 1231 (8th Cir. 1993)....	14
<i>United States v. Kearney</i> , 672 F.3d 81 (1st Cir. 2012).....	19
<i>United States v. Perez</i> , 484 F.3d 735 (5th Cir. 2007)	15

<i>United States v. Perrine</i> , 518 F.3d 1196 (10th Cir. 2008)	15
<i>United States v. Stanert</i> , 762 F.2d 775 (9th Cir.)	<i>passim</i>
<i>United States v. Stults</i> , 575 F.3d 834 (8th Cir. 2009)	15
<i>United States v. Vosburgh</i> , 602 F.3d 512 (3d Cir. 2010)	15, 17, 19
<i>United States v. Wagers</i> , 452 F.3d 534 (6th Cir. 2006)	15-16
<i>Wilson v. Russo</i> , 212 F.3d 781 (3rd Cir. 2000)	14

Statutes and Rules

18 U.S.C. § 2252(a)(4)(B)	8
28 U.S.C. § 1254	1
Fed. R. App. P. 30	<i>passim</i>
U.S. Const. amend. IV	1, 14

PETITION FOR WRIT OF CERTIORARI

Carlos MARTINEZ respectfully prays that a writ of certiorari issue to review the judgment of the United States Court of Appeals for the Ninth Circuit in this case.

OPINION BELOW

The Ninth Circuit's memorandum decision, *see* App. 1a-2a, is unpublished. The district court's oral ruling is also unpublished.

JURISDICTION

The Ninth Circuit issued its decision on September 18, 2017. App 1a. Mr. Martinez did not file a petition for rehearing. This Court has jurisdiction under 28 U.S.C. § 1254(1).

RELEVANT CONSTITUTIONAL PROVISION

The Fourth Amendment provides: "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.

STATEMENT OF THE CASE¹

This case concerns the unlawful search of a home on Penny Royal Lane in San Rafael, California on February 23, 2012. Although the search at issue was authorized by a warrant, that warrant (the “Penny Royal Warrant”) was obtained in violation of *Franks v. Delaware* and the Fourth Amendment.

I. Investigation of IP Address 76.126.194.166

On October 11, 2011, a detective from the Pleasant Hill Police Department, Steven Guidi, was using a software program called “E-Phex” to access the peer-to-peer file-sharing network Gnutella.² There, Detective Guidi established a direct connection with a computer at IP address **76.126.194.166** and obtained a list of files available for sharing and downloading from that computer. Of eleven files available for sharing, four matched suspected child pornography hash values contained in a local database compiled from previous investigations.³ Using E-Phex, Guidi downloaded one of those files, reviewed it, and determined that it was child pornography.

¹ The facts of this case were never addressed in the Ninth Circuit’s memorandum decision. As a result, they are set forth at some length here.

Where appropriate, Martinez will cite to the Appellant’s Excerpts of Record (“ER”), which Ninth Circuit Rule 30-1 directs parties to compile instead of the appendix contemplated by Federal Rule of Appellate Procedure 30. *See* Ninth Cir. R. 30-1(a)-(b).

² Peer-to-peer (“P2P”) file-sharing programs are typically free and publicly available; they are a standard method for transferring files from one computer to another while being connected to a network via the internet. ER 267. Peer-to-peer programs “typically require a user to place files in a share folder on their computer which allows access to other users using the same file sharing networks and protocols.” *Id.*

³ A “hash value” is a unique sequence of integers and characters that “is created any time a digital file is created, manipulated, or changed.” ER 268. Law enforcement knows the hash values of some files that have previously been identified as containing child pornography. *See id.* Those known hash values can then be compared to the hash values of files being offered on P2P networks for sharing/downloading. *Id.*

The following day, Guidi used E-Phex to determine that the IP address 76.126.194.166 was registered to Comcast Cable Communications, Inc.

On October 13, 2011, Guidi again used E-Phex to connect directly with a computer at IP address 76.126.194.166. This time, the list of files available for sharing and downloading included forty-six files, ten of which matched suspected child pornography hash values. Guidi used E-Phex to download four of the ten files, reviewed them, and determined that at least two of the files constituted child pornography.

Approximately one month later, Guidi applied for a search warrant authorizing him to obtain, from Comcast, information identifying the Comcast subscriber to whom IP address 76.126.194.166 was assigned on October 11, 2011. A magistrate granted the search warrant on November 10, 2011.

Comcast responded to the search warrant by letter dated November 16, 2011 (herein the “Comcast Letter”), an image of which is appended below. Comcast stated that the “subscriber information obtained” in response to the warrant showed that, “as of 11/16/2011,” the IP address 76.126.194.166 was assigned to Nicole Botelho of 820 Penny Royal Lane, San Rafael, California. ER 212. In other words, although the search warrant sought the identity of the Comcast subscriber assigned 76.126.194.166 on **October 11**, the Comcast Letter identified the subscriber whose “current” IP address was 76.126.194.166 on **November 16** – more than one month *after* the requested date:

Dear Detective Guidi:

The Search Warrant received on 11/10/2011 with respect to the above-referenced matter has been forwarded to the Legal Response Center for a reply. The Search Warrant requests Comcast to produce certain subscriber records pertaining to the following IP address: 76.126.194.166 assigned on 10/11/2011 at 23:58 UTC -07:00.

Based on the information provided pursuant to the Search Warrant, the subscriber information obtained has been provided below:

Subscriber Name:	NICOLE BOTELHO
Service Address:	820 PENNY ROYAL LN SAN RAFAEL, CA 94903-2330
Telephone #:	[REDACTED]
Type of Service:	High Speed Internet Service
Account Number:	[REDACTED]
Account Status:	Active
Start of Service:	8/16/2006
Current IP:	76.126.194.166 as of 11/16/2011
IP Assignment:	Dynamically Assigned
E-mail User Ids:	nikibotelho (All Comcast user IDs end in @comcast.net)
Method of Payment:	Statement sent to above address (No credit card numbers or bank account numbers on file)

If you have any questions regarding this matter, please feel free to call 866-947-8572.

Very Truly Yours,

Comcast Legal Response Center

*Id.*⁴

Importantly, the Comcast Letter also noted that the IP address for the subscriber's account was "Dynamically Assigned." *Id.* Unlike a "static" IP address, which remains assigned to one specific user for an indefinite amount of time, a

⁴The Comcast Letter has been redacted here to protect personally identifying information.

“dynamic” IP address can change whenever a computer connects with the internet.

See discussion infra.

The day after receiving the Comcast Letter, Guidi forwarded the results of his investigation to San Jose Police Department Officer Daniel Ichige.

II. Officer Ichige Obtains the Penny Royal Search Warrant – But Fails to Inform the Magistrate That the Targeted IP Address Is Dynamic and That Comcast Identified an Assigned Subscriber for a Date More Than a Month After the Illegal Conduct Being Investigated

Officer Ichige reviewed the results of Detective Guidi’s investigation, including the Comcast Letter. Then, based largely on Guidi’s investigation, Ichige drafted his own search warrant affidavit seeking authorization to search the home at 820 Penny Royal Lane for evidence related to child pornography. In his warrant affidavit, Ichige included a general background on child pornography offenses committed over the internet. To help understand that discussion, Ichige also offered a comprehensive technological background, which included information about IP addresses, peer-to-peer networks, and hash values.

Regarding IP addresses, Ichige stated “[a]n Internet Protocol address (IP address) is a unique address that certain electronic devices use in order to communicate with each other on a computer network utilizing the Internet Protocol standard.” ER 268. Significantly, Ichige’s affidavit explained that there are two *different types* of IP addresses: “IP addresses can be static or dynamic. A static IP address remains assigned to a specific user for an indefinite amount of time where as [sic] a dynamic IP address may *change* according to available addresses *when a user computer connects with the internet.*” *Id.*

Ichige's affidavit also explained the critical role an IP address plays when law enforcement attempts to locate the actual physical location of a computer suspected of illegal activity:

I know from training and experience that Internet computers identify each other by an Internet Protocol or IP address. I know that these IP addresses can assist law enforcement in finding a particular computer on the Internet. These IP addresses lead the law enforcement officer to a particular Internet service provider or company (ISP). *Given the date and time the IP address was used*, an ISP can typically identify the account holder by name and physical address.

ER 271 (emphasis added).

Turning from his technological background to the specifics of the present case, Ichige's warrant affidavit related that Detective Guidi had contacted Ichige about his above-discussed child pornography investigation. Ichige next stated, "I reviewed the attached police report and search warrant to Comcast Cable Communications that Detective Guidi prepared and I found them to be accurate. I also concluded that the files that he was able to obtain from IP address **76.126.194.166** did indeed constitute child pornography." ER 272 (bold in original). Ichige's affidavit cited to Guidi's police report and his Comcast search warrant application, which were appended to his affidavit.

Although Ichige reviewed the Comcast Letter *before* drafting his search warrant affidavit, he did **not** provide the magistrate with a copy of that Letter. Nor did Ichige's affidavit otherwise alert the magistrate to the full contents of the Comcast Letter – *i.e.*, the identification of (1) a dynamic IP address and (2) a subscriber to whom it was assigned one month *after* the criminal activity at issue.

Rather than attach a copy of the Comcast Letter to his affidavit, or advise the magistrate of its full contents, Ichige instead asserted:

Detective Guidi served Comcast Cable Communications and received the following subscriber records associated to IP address **76.126.194.166** :

Nicole Botelho
820 Penny Royal Lane
San Rafael, CA 94903

Id. Ichige did **not** specify the dates the targeted IP address was associated with Ms. Botelho, or inform the magistrate that the targeted IP address was dynamic, rather than static. The police report that Ichige selected to attach to his warrant affidavit did **not** advise the magistrate of these facts either.

On February 21, 2012, a state judge issued the Penny Royal Warrant.

III. The Execution of the Penny Royal Warrant and Interrogation of Mr. Martinez

On February 23, 2012, at about 9:30 a.m., seven San Rafael Police Department detectives and numerous officers from several other law enforcement agencies, including Detective Guidi, served the Penny Royal Warrant. The officers forced entry to 820 Penny Royal Lane after knocking and receiving no response. No one was at the residence. The police contacted Ms. Botelho, who said that she had not been at the house the night before, but her boyfriend Carlos Martinez had been.

During a search of the home, the officers located a Sony laptop computer. Guidi examined the computer, opened a “frostwire” file on the computer, and observed that the IP address listed in the search warrant matched the IP address in the frostwire file. His search then located suspected child pornography, which had been downloaded the night before.

Using a ruse, police enticed Mr. Martinez to go to the residence. He was interrogated and made incriminating statements. Most of those statements were suppressed by the the district court, and are not the subject of this petition.

IV. Mr. Martinez's Motion to Suppress

Mr. Martinez was charged in a one-count indictment with possessing child pornography in violation of 18 U.S.C § 2252(a)(4)(B). He subsequently moved the district court for an order suppressing all evidence and statements derived from the search of 820 Penny Royal Lane, the search of his person and effects, and his interrogation. As relevant here, the motion to suppress argued that Mr. Martinez was entitled to an evidentiary hearing under *Franks v. Delaware* because Officer Ichige intentionally or recklessly omitted from his search warrant affidavit the fact that (a) IP address 76.126.194.166 was a dynamic address and (b) the Comcast Letter identified a subscriber assigned that IP address on November 16 instead of October 11 (the date of the criminal activity at issue).

The government's opposition included a declaration from Officer Ichige. Therein, Ichige claimed that when he reviewed the Comcast Letter and its statement that the IP address was assigned to Ms. Botelho "as of 11/16/2011," his "experience as a police officer" nevertheless led him to "believe[] that to mean that Nicole Bothelo [sic] at 820 Penny Royal Lane was the subscriber for IP address 76.126.194.166 on *October 11, 2011.*" ER 216 (emphasis added). The government defended Ichige's "interpretation" of the Letter as reasonable and sincere; although the Comcast Letter's plain language provided subscriber information "as of

11/16/2011,” the government relied on the Letter’s acknowledgement that the search warrant requested subscriber records as “assigned on 10/11/2011.”

The government’s opposition to the suppression motion also produced a “clarifying” letter from Comcast, dated May 16, 2013 (one-and-one-half years after the events in question). The “clarifying” letter purported to “confirm” that the information provided in the original Comcast Letter actually identified Ms. Botelho as the subscriber associated with the IP address 76.126.194.166 “on 10/11/2011 at 23:58 UTC -07:00.” ER 211. Based on these facts, the government argued that the Penny Royal Warrant was supported by probable cause and that no *Franks* hearing was necessary because Officer Ichige’s statement in his warrant affidavit that the IP address was assigned to Botelho at the date and time in question was made in good faith.

On June 19, 2013, the district court held a particularly brief motion hearing. The court ruled orally from the bench, denying in part and granting in part the motion to suppress.

With respect to Mr. Martinez’s first two arguments – that the Penny Royal Warrant lacked probable cause, or alternatively, that Mr. Martinez was entitled to a *Franks* hearing – the entirety of the hearing proceeded as follows:

THE COURT: So, this is a motion to suppress.

MR. HANSEN: It is.

THE COURT: And I’ve reviewed the briefing in connection with this. It raises some interesting issues. So, let’s try to divide them a bit. We have the issue as to whether or not the warrant was adequate, essentially, right?

MR. HANSEN: Yes, sir.

THE COURT: Because the argument is that it didn't advise the magistrate that this was a dynamically assigned IP address.

MR. HANSEN: Yes, sir.

THE COURT: And whether that's a flaw such that, one, it should have been disclosed to the magistrate, and, two, whether it would have made a difference. That's one aspect. And from that flowed the search of the property. Okay.

And, after reviewing it, I conclude that it wasn't a flaw, but if it were and disclosed to the magistrate judge, it would not have made a difference. I don't think that – *it's my view that there isn't enough of a difference between dynamically assigned IP addresses and static IP addresses that would make the difference as to whether or not a particular premises can be subject to searches.* You take a different view. I appreciate that, but that's my view. So I'm not going to suppress the search of the house.

ER 169-70 (emphasis added).

Thus, the district court concluded (1) the Penny Royal Warrant was supported by probable cause, and (2) Officer Ichige's omission of the fact that IP address 76.126.194.166 was dynamically assigned to Ms. Botelho, rather than static, was not material to a finding of probable cause to search 820 Penny Royal Lane. The court's ruling on Mr. Martinez's *Franks* claim did not address, however, the fact that the Comcast Letter identified the subscriber assigned the targeted IP address on November 16 – not October 11, as requested by the warrant. Nor did the district court's ruling make any factual findings. The court made no finding as to whether Officer Ichige intentionally or recklessly omitted the full contents of the Comcast Letter from his warrant affidavit; the court similarly made no finding as to whether Ichige acted in "good faith" by doing so, as the government claimed he did.

The court did not issue a written order.

V. Mr. Martinez's Conviction and Appellate Proceedings

In order to preserve Martinez's right to appeal the district court's partial denial of his motion to suppress, the parties agreed to a stipulated-testimony bench trial before the district court. The district court held the bench trial on December 14, 2015 and found Mr. Martinez guilty. The court sentenced Mr. Martinez several months later.

Mr. Martinez appealed his conviction to the Court of Appeals for the Ninth Circuit. He argued that the district court erred in denying his motion for a *Franks* hearing. A panel of the Ninth Circuit affirmed Mr. Martinez's conviction in a memorandum disposition lacking any meaningful factual or legal analysis. *See* App. 1a-2a. Notwithstanding the fact that Martinez's argument was premised on Officer Ichige's dual omissions – of the IP address's dynamic nature and the Comcast Letter's identification of the subscriber "as of 11/16/2011," more than a month after the offending Internet activities, – the panel wrongly held that "Martinez failed to show that Officer Ichige's omission – that the IP address was dynamically assigned – was misleading or done in deliberate or reckless disregard of the truth." App. 1a. Then, utterly ignoring the Comcast Letter's plain language, the panel held that "had the affidavit included this fact, it would have still supported probable cause in light of the information that had been obtained from the internet service provider." App. 2a.

REASONS FOR GRANTING THE WRIT

Today, the vast majority of child pornography offenses are committed over the Internet. IP addresses play a critical role in investigating such crimes: by serving

as a unique identifier assigned to a specific computer at a certain point in time, IP addresses establish a nexus between Internet child pornography offenses and the physical location of those engaged in the offenses, which in turn can support a search warrant for those physical premises. This case presents an important question of federal law that has not been, but should be, settled by this Court: whether the fact that a *dynamic* IP address was assigned to the target of a search warrant at a time other than the time when it was used for Internet child pornography activities, is material to the probable cause determination under *Franks v. Delaware*, 438 U.S. 154 (1978).

The answer, as provided by the affiant police officer in this case himself and as corroborated by courts throughout the country, is yes. Unlike a static IP address, which remains assigned to a specific user for an indefinite amount of time, a dynamic IP address may change every time a computer connects to the Internet. Accordingly, the fact that a dynamic IP address was assigned to a certain user at a time other than the time of the illegal Internet activity fails to establish the requisite nexus between child pornography offenses and the physical location to be searched, and the information is material to the search warrant.

A. General Framework of *Franks*-Based Fourth Amendment Claims

In *Franks v. Delaware*, this Court held that evidence may be suppressed when obtained pursuant to a search warrant that issued based on an affidavit containing false statements with respect to probable cause. *Franks*, 438 U.S. at 155-56. Under *Franks*, a defendant is entitled to an evidentiary hearing where he makes a substantial preliminary showing that (1) a false statement was intentionally or

recklessly included in a search warrant application and (2) the false statement was material to the finding of probable cause; that is, it was “necessary to the finding of probable cause.” *Id.* at 156.

If, after a hearing, the defendant demonstrates the intentional or reckless falsity by a preponderance of the evidence, the reviewing court must set the false statements to one side and determine whether the remaining information is sufficient to establish probable cause. *See id.* at 156. If not, the warrant must be voided and the fruits of any search or seizure performed pursuant to the warrant must be suppressed. *See id.*

Franks applies equally to “deliberate or reckless **omissions** of fact which tend to mislead.” *United States v. Stanert*, 762 F.2d 775, 781, *amended* 769 F.2d 1410 (9th Cir. 1985) (bold added). In the case of such intentional or reckless omissions, the court must review the warrant application “with the omitted information included” and determine whether the application would still establish probable cause. *United States v. DeLeon*, 979 F.2d 761, 764 (9th Cir. 1992). If not, the warrant is invalid and any fruits obtained via the warrant must be suppressed.

To merit a *Franks* hearing, all that is required “is that the defendant make a substantial showing that the affiant intentionally or recklessly [misstated facts or] omitted facts required to prevent technically true statements in the affidavit from being misleading.” *Stanert*, 762 F.2d at 781; *see also Liston v. County of Riverside*, 120 F.3d 965, 973 (9th Cir. 1997).

Finally, where a *Franks* claim is based upon material omissions from a warrant affidavit, “[t]he most commonsense evidence that the officer acted with at least a

reckless disregard for the truth is that the omissions and false statements contained in the affidavit were all facts that were within [the officer's] personal knowledge.”

Chism v. Washington, 661 F.3d 380, 388 (9th Cir. 2011); *see also Wilson v. Russo*, 212 F.3d 781, 788 (3d Cir. 2000) (an officer acts with reckless disregard for the truth when he “withholds a fact in his ken that ‘any reasonable person would have known that this was the kind of thing the judge would wish to know’” (quoting *United States v. Jacobs*, 986 F.2d 1231, 1235 (8th Cir. 1993))).

B. Omission of the Fact That a Dynamic IP Address Was Assigned to a Certain User on a Date Other Than the Date of the Offending Child Pornography Offenses Is Material to the Probable Cause Determination

For a search warrant to issue, the Fourth Amendment requires that there be “probable cause, supported by Oath or affirmation.” U.S. Const. amend. IV. Probable cause exists when, under the totality of the circumstances, “there is a fair probability that contraband or evidence of a crime will be found in a particular place.” *Illinois v. Gates*, 462 U.S. 213, 238 (1983).⁵ Probable cause, therefore, requires proof of a sufficient nexus between the evidence and the location to be searched. *See id.*

Evidence that an IP address was used in child pornography-related Internet activities plays a critical role in establishing probable cause to search the physical premises associated with that IP address for evidence of child pornography offenses. *See, e.g., Chism v. Washington*, 661 F.3d 380, 390 (9th Cir. 2011) (“We have explained that a computer that is connected to the internet can be uniquely

⁵ When reviewing a search warrant for probable cause, courts are limited to the information contained within the four corners of the affidavit supporting the warrant application. *Stanert*, 762 F.2d at 778.

identified by its IP number, much like a land-line phone can be uniquely identified by its phone number Moreover, we have repeatedly recognized the utility of using IP address information to investigate child pornography offenders. *See United States v. Craighead*, 539 F.3d 1073, 1080–81 (9th Cir. 2008) (holding that probable cause existed where the IP address from which child pornographic images were shared was traced to the defendant); *United States v. Hay*, 231 F.3d 630, 634–35 (9th Cir.2000) (holding that an affidavit demonstrated probable cause where the agent carefully detailed how the IP address associated with the child pornographic images was connected to the defendant).”); *United States v. Vosburgh*, 602 F.3d 512, 526-27 (3d Cir. 2010) (noting that “several Courts of Appeals have held that evidence that the user of a computer employing a particular IP address possessed or transmitted child pornography can support a search warrant for the physical premises linked to that IP address” and holding that probable cause supported warrant where officers used IP address to identify the physical location of the person who tried to access link posted on an Internet message board dedicated to child pornography); *United States v. Stults*, 575 F.3d 834, 843–44 (8th Cir. 2009) (holding that probable cause supported warrant where officers used IP address to identify possessor of child pornography on a file-sharing network); *United States v. Perrine*, 518 F.3d 1196, 1205–06 (10th Cir. 2008) (upholding probable cause where pornographic images were traced to defendant’s residence using IP address); *United States v. Perez*, 484 F.3d 735 (5th Cir. 2007) (upholding probable cause where email containing child pornography was traced to defendant’s residence using IP address); *United States v. Wagers*, 452 F.3d 534, 539 (6th Cir. 2006) (upholding probable

cause where suspect was identified as a member of child pornography websites through an IP address assigned to his residence).

As these cases make clear, the IP addresses' utility in child pornography investigations derives from their ability to *uniquely* identify a computer connected to the Internet *at a certain point in time*. Armed with the IP address of a suspect computer, law enforcement can identify the ISP, which they may subpoena to provide the identifying information for the subscriber to whom the IP address was assigned during the relevant dates. *See generally London-Sire Records, Inc. v. Doe 1*, 542 F. Supp. 2d 153, 160-161 (D. Mass. 2008). Officer Ichige's affidavit confirms this approach, noting that "IP addresses lead the law enforcement officer to a particular Internet service provider or company (ISP). *Given the date and time the IP address was used*, an ISP can typically identify the account holder by name and physical address."⁶ ER 271 (emphasis added).

Law enforcement must cabin their identifications requests to an ISP to a specific date (or dates) for two separate, but interconnected reasons. First, as discussed *supra*, a search warrant must be supported by probable cause that evidence of a crime will be found at the location to be searched, which in the case of Internet child pornography offenses requires a showing that the physical location was associated with an offending IP address at the time (or times) that IP address

⁶ The identification process described above "requires ISPs to maintain logs and other records, and to use commercially available or customized software tools, to correlate the IP address assigned to a computer at a specific moment with the subscriber's account information in order to identify a customer from the IP address, either for the ISPs own internal business purposes or to respond to subpoenas requesting identifying information about a customer." *Call of the Wild Movie, LLC v. Does*, 770 F. Supp. 2d 332, 357 (D. D.C. 2011).

Different ISPs may have different retention policies (i.e., the length of time they may retain their IP logs or other data). *See London-Sire*, 542 F.Supp.2d at 160-61.

was used for child pornography-related Internet activities. Second, identification requests must specify a date (or dates) because most IP addresses are **not** indefinitely assigned to a computer.

“[R]elatively few personal computer users have a specific, set IP address, called a ‘static’ address.” *London–Sire*, 542 F.Supp.2d at 161. “Instead, many use their computers to connect to a network provided by their ISP, which uses a certain range of IP addresses—say, all of the numbers between 168.122.1.x to 168.122.100.x. The ISP assigns an address within its range to the user’s computer for the user’s session, allocating the numbers within its range on an as-needed basis. This process is known as ‘dynamic’ addressing.” *Id.*

Officer Ichige himself explained the distinction between static and dynamic IP addresses in his affidavit: “A static IP address remains assigned to a specific user for an indefinite amount of time where as [sic] *a dynamic IP address may change according to available addresses when a user computer connects with the internet.*” ER 268 (emphasis added). Critically, a computer assigned a dynamic IP address is still uniquely identified by its IP address while connected to the internet because, even in that instance, “*no two devices have the same IP address at the same time.*” *Vosburgh*, 602 F.3d at 517 n.3 (emphasis added).

Courts throughout the country have also recognized the distinction between static and dynamic IP addresses. *See, e.g., id.; Klimas v. Comcast Cable Comm’ns, Inc.*, 465 F.3d 271, 273 (6th Cir. 2006) (“Any computer from which a person accesses the internet is assigned an IP address, which may be either ‘static’ (remain constant) or ‘dynamic’ (change periodically).”); *Brooks v. AM Resorts, LLC*, 954 F.

Supp. 2d 331, 334 (E.D. Pa. 2013) (“All experts agree that IP addresses can be static or dynamic. Static IP addresses are assigned by the Internet Service Provider (‘ISP’) to an individual or company for a certain period of time. Dynamic IP addresses can change at any time because they are not assigned by the ISP to an individual or company for any certain period of time.”); *Disney Enters., Inc. v. Rea*, 940 F. Supp. 2d 288, 297 (E.D. Va. 2013) (“IP addresses can be ‘static,’ such that a particular computer is assigned an IP address that does not change, or ‘dynamic,’ such that each time a particular computer connects to the Internet it receives a randomly assigned IP address from a pool of available IP addresses.”); *Call of the Wild*, 770 F. Supp. 2d at 356-57 (“Most consumer IP addresses are ‘dynamic’ as opposed to ‘static.’ *See generally London–Sire*, 542 F. Supp. 2d at 160. Static IP addresses are addresses which remain set for a specific user. *Id.* Dynamic IP addresses are randomly assigned to internet users and change frequently. *Id.* Consequently, for dynamic IP addresses, a single IP address may be re-assigned to many different computers in a short period of time. *Id.*”); *United States v. Christy*, 785 F. Supp. 2d 1004, 1010 n.4 (D.N.M. 2011) (“An IP address is an address specific to every computer attached to the internet -- anytime a computer logs onto the internet it has to have a unique IP address to transmit information and to receive information through the internet. . . . IP addresses can either be static or dynamic. A dynamic IP address means that, after a user logs off the internet, when the user logs back on the user is periodically assigned a new IP address from the service provider.”); *London–Sire*, 542 F. Supp. 2d at 160 (discussing static versus dynamic IP addressing).

The static-dynamic dichotomy has important consequences in Internet child pornography offenses cases. Because probable cause requires a nexus between evidence of child pornography and the physical location to be searched, when an offending IP address is dynamic, that nexus is provided by evidence that that IP address was assigned to that physical location *at the time of the suspect online activities*. *Cf. United States v. Kearney*, 672 F.3d 81, 89-91 (1st Cir. 2012) (upholding the denial of motion to suppress where, although assigned a dynamic IP address, the defendant was assigned the offending IP address at the time child pornography files were sent from that address); *Vosburgh*, 602 F.3d at 523, 527. The requisite nexus, however, does **not** exist when the evidence only establishes that the offending dynamic IP address was assigned to the physical location to be searched at some point in time other than the time of the illegal Internet conduct. *Cf. id.* The explanation is obvious: because a dynamic IP address may change every time when the computer connects to the Internet, assignment of that IP address to a certain physical location at a certain time does *not* allow an inference of assignment to same physical location at a different time, regardless how close that time might be. *Cf. London–Sire*, 542 F. Supp. 2d at 161.

Consequently, where the only available evidence shows that an offending IP address was assigned to the targeted physical location at a time other than the time of the illegal Internet conduct, the fact that that IP address is dynamically assigned destroys the nexus required to support probable cause to search the targeted physical location. Omission that a dynamic IP address was assigned to a certain

user on a date other than the date of the offending child pornography offenses is therefore material to the probable cause determination.

C. The Ninth Circuit Erred in Failing to Recognize that the Penny Royal Warrant Affidavit Deliberately or Recklessly Omitted Material Information That the Relevant IP Address Was Dynamic and Was Assigned to Ms. Botelho More Than a Month After the Illegal Online Activities

Despite the fact that Officer Ichige himself explained the distinction between static and dynamic IP addresses in his affidavit and despite the fact that the Comcast Letter clearly stated that the relevant IP address was dynamic and was assigned to Ms. Botelho more than a month after the illegal online activities, the Ninth Circuit summarily held that omission of this information was not material and not done in deliberate or reckless disregard of the truth. The Ninth Circuit plainly erred.

As explained at length above, there is a critical difference between static and dynamic IP addresses. That difference was crucial in Mr. Martinez's case.

The Comcast Letter identified Ms. Botelho as the subscriber assigned the IP address 76.126.194.166 on November 16, 2011 – more than one month *after* the relevant date of October 11, 2011, when that IP address was used to offer child pornography for sharing and downloading. The Comcast Letter also identified the IP address 76.126.194.166 as being dynamically assigned. Nonetheless, Officer Ichige failed to disclose these facts to the magistrate. He also failed to attach the Comcast Letter to his affidavit, which would have alerted the magistrate judge to the lack of a connection between the IP address 76.126.194.166 and Ms. Botelho's residence on October 11, 2011. Instead, he falsely suggested that Comcast had

identified Ms. Botelho as the subscriber assigned the IP address 76.126.194.166 on October 11, 2011.⁷ “By reporting less than the total story,” Officer Ichige “manipulate[d] the inferences” that the magistrate judge could draw, therefore bringing the case solidly under *Franks*’ purview. *Stanert*, 762 F.2d at 781.

Notably, Officer Ichige’s misrepresentations were the only evidence available to the magistrate judge from which he could infer a physical link between the child pornography files offered for sharing and downloading from the IP address 76.126.194.166 on October 11, 2011 and Ms. Botelho’s residence. Had Officer Ichige disclosed the fact that Comcast Letter had identified Ms. Botelho as the subscriber assigned the IP address 76.126.194.166 on November 16, 2011 and the fact that that IP address was dynamically assigned, the existence of that physical link would have been completely undermined. On these facts, no reasonable magistrate judge would have issued the search warrant for Ms. Botelho’s residence had he or she been apprised of the omitted information. Contrary to the Ninth Circuit’s decision, then, Mr. Martinez made a substantial showing, as required by *Franks*, that the omitted information was material to the probable cause determination for the Penny Royal Lane search warrant.

Mr. Martinez also made a substantial showing that Officer Ichige intentionally or recklessly omitted that material information. The very fact “that the affidavit

⁷ Officer Ichige did not explicitly state that Comcast had identified Ms. Botelho as the subscriber assigned the IP address 76.126.194.166 on October 11, 2011. Rather, he referenced and attached to his affidavit the Comcast search warrant, which sought the subscriber information for the IP address 76.126.194.166 as of October 11, 2011. He then noted that, in its response, Comcast had identified Ms. Botelho as the subscriber assigned that IP address. The only reasonable reading of Officer Ichige’s affidavit is that Comcast identified Ms. Botelho as the subscriber assigned the IP address 76.126.194.166 on October 11, 2011.

did not report important factual information that was within the officers' knowledge at the time [Officer Ichige] prepared [his] affidavit would allow a reasonable factfinder to conclude that the officers acted with at least a reckless disregard for the truth." *Chism*, 661 F.3d at 388.

The district court could also find that Officer Ichige acted intentionally or recklessly because he not only omitted remarkably important facts about the IP address, but he also failed to attach the Comcast Letter itself. By contrast, he did attach the Comcast search warrant and Guidi's police report, which also offered an incomplete and misleading picture of Comcast's response. From these facts, the district court could infer that Officer Ichige did not attach the Comcast Letter in order to deprive the magistrate judge of the opportunity to get an accurate understanding of the Comcast's response, which would have undermined the requisite nexus between the offending child pornography and Ms. Botelho's residence as of October 11, 2011.

To get an evidentiary hearing under *Franks*, Mr. Martinez only had to make a *substantial showing* that Officer Ichige intentionally or recklessly omitted material information from his affidavit. *See Stanert*, 762 F.2d at 781. For the reasons explained above, Mr. Martinez met his burden. Accordingly, this Court should reverse the Ninth Circuit and remand the case with instructions that the district court hold a *Franks* evidentiary hearing.

CONCLUSION

For the aforementioned reasons, this Court should grant this petition for a writ of certiorari and reverse the Ninth Circuit.

Respectfully submitted,

STEVEN G. KALAR
Federal Public Defender

December 13, 2017

s/ Geoffrey A. Hansen

GEOFFREY A. HANSEN

Chief Assistant Federal Public Defender