No. 16-10109

IN THE UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellant,

v.

ANTONIO GILTON, *et al.*,

Defendants-Appellees.

REDACTED OPENING BRIEF FOR THE UNITED STATES
*** **PUBLIC VERSION** ***

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
NO. 13-CR-00764-WHO-1

BRIAN J. STRETCH
United States Attorney

BARBARA J. VALLIERE
Chief, Appellate Division

ANNE M. VOIGTS
Assistant United States Attorney
450 Golden Gate Ave., 11th Floor
San Francisco, CA 94102
(408) 535-5588

Attorneys for Plaintiff-Appellant
UNITED STATES OF AMERICA

August 11, 2016

TABLE OF CONTENTS

TABLE OF AUTHORITIES iii

JURISDICTION, TIMELINESS, AND BAIL STATUS 3

ISSUES PRESENTED 3

STATEMENT OF THE CASE 3

A. Historical Cell-Site Information 3

B. Calvin Sneed's Murder 8

C. The Warrant 12

D. The Pending Charges 13

E. The Motion To Suppress 14

F. The District Court's Order 15

SUMMARY OF ARGUMENT 18

ARGUMENT 21

I. THE FOURTH AMENDMENT DOES NOT REQUIRE A WARRANT ESABLISHING PROBABLE CAUSE TO OBTAIN HISTORICAL CSLI 21

A. Standard Of Review 21

B. Under The Third-Party Doctrine, Individuals Do Not Have A Reasonable Expecation Of Privacy In Business Records Maintained by Their Cell Phone Carriers 21

1. The Third-Party Doctrine 21

2. Under The Third-Party Doctrine, Antonio Gilton Did Not Have A Reasonable Expectation Of Privacy In CSLI Maintained By His Cell Phone Carrier 27

C. No Fourth Amendment Precedent Supports A Contrary Result.....36

D. Even Assuming That Government Acquisition Of CSLI Is A Fourth Amendment Search, A Showing Of Reasonable Relevance To An Investigation, Rather Than Probable Cause, Would Satisfy The Fourth Amendment's Reasonableness Requirement 40

II. EVEN IF PROBABLE CAUSE WAS NECESSARY, THE WARRANT ESTABLISHED A REASONABLE NEXUS BETWEEN THE MURDER AND ANTONIO GILTON'S PHONE.....46

III. EVEN IF THE WARRANT DID NOT ESTABLISH PROBABLE CAUSE, THE OFFICERS RELIED ON IT IN GOOD FAITH.....51

CONCLUSION.....55

STATEMENT OF RELATED CASES.....56

CERTIFICATE OF COMPLIANCE.....57

CERTIFICATE OF SERVICE 58

TABLE OF AUTHORITIES

FEDERAL CASES

Brinegar v. United States, 338 U.S. 160 (1949) 47

Donaldson v. United States, 400 U.S. 517 (1971) 35

Ex Parte Jackson, 96 U.S. 727 (1878) 33, 34

Herring v. United States, 555 U.S. 135 (2009) 51, 52

Hoffa v. United States, 385 U.S. 293 (1966) 23

Illinois v. Gates, 462 U.S. 213 (1983) 47

Illinois v. Krull, 480 U.S. 340 (1987) 52, 54

In re Application for Tel. Info. Needed for a Criminal Investigation, No. 15-cr-90304-LHK, 119 F. Supp. 3d 1011 (N.D. Cal. 2015) 15, 16, 27

In re Application of the U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013) ..... *passim*

In re Application of U.S. for an Order Authorizing Release of Historical Cell-Site Info., 809 F. Supp. 2d 113 (E.D.N.Y. 2011) 28

In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304 (3d Cir. 2010) 30

In re Applications of U.S. for Orders Pursuant to Title 18, U.S. Code Section 2703(d), 509 F. Supp. 2d 76 (D. Mass. 2007) 27

In re Application of U.S., 405 F. Supp. 2d 435 (S.D.N.Y. 2005) 5

Katz v. United States, 389 U.S. 347 (1967) ..... *passim*

Kyllo v. United States, 533 U.S. 27 (2001) 35, 36, 37

Lopez v. United States, 373 U.S. 427 (1963) 23

Maryland v. King, 133 S. Ct. 1958 (2013) 40, 41, 44, 45

Maryland v. Macon, 472 U.S. 463 (1985) 21

Messerschmidt v. Millender, 132 S. Ct. 1235 (2012) 53

Navarette v. California, 134 S. Ct. 1683 (2014) 49

Oklahoma Press Pub. Co. v. Walling, 327 U.S. 186 (1946) 22, 43

Riley v. California, 134 S. Ct. 2473 (2014) 38, 39, 40

S.E.C. v. Jerry T. O'Brien, 467 U.S. 735 (1984) 33

Smith v. Maryland, 442 U.S. 735 (1979) ..... *passim*

United States v. Angulo-Lopez, 791 F.2d 1394 (9th Cir. 1986) 48

United States v. Banks, 52 F. Supp. 3d 1201 (D. Kan. 2014) 27

United States v. Benford, 2010 WL 1266507 (N.D. Ind. Mar. 26, 2010) 27

United States v. Booth, 669 F.2d 1231 (9th Cir. 1981) 21

United States v. Calandra, 414 U.S. 338 (1974) 51

United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016) ..... *passim*

United States v. Chavez, 2016 WL 740246 (D. Conn. Feb. 24, 2016) 27

United States v. Chavez-Miranda, 306 F.3d 973 (9th Cir. 2002) 47

United States v. Cooper, No. 13-cr-00693-SI, 2015 WL 881578 (N.D. Cal. Mar. 2, 2015) 15

United States v. Cormier, 220 F.3d 1103 (9th Cir. 2000) 26

United States v. Crews, 502 F.3d 1130 (9th Cir. 2007) 46

United States v. Davis, 785 F.3d 498 (11th Cir. 2015) (en banc)..... *passim*

United States v. Dorsey, 2015 WL 847395 (C.D. Cal. Feb. 23, 2015) 27, 54

United States v. Epstein, 2015 WL 1646838 (D.N.J. Apr. 14, 2015).....27

United States v. Evans, 892 F. Supp. 2d 949 (N.D. Ill. 2012).....5

United States v. Fernandez, 388 F.3d 1199 (9th Cir. 2004).....47

United States v. Forrester, 512 F.3d 500 (9th Cir. 2008)..... *passim*

United States v. Giddins, 57 F. Supp. 3d 481 (D. Md. 2014).....27

United States v. Golden Valley Electric Ass'n,
689 F.3d 1108 (9th Cir. 2012) 19, 26, 27

United States v. Gordon, 2012 WL 8499876 (D.D.C. Feb. 6, 2012) 27

United States v. Gourde, 440 F.3d 1065 (9th Cir. 2006) (en banc).....47

United States v. Graham, 2016 WL 3068018
(4th Cir. May 31, 2016) (en banc) 4, 5, 6, 27, 30

United States v. Grant, 682 F.3d 827 (9th Cir. 2012) 18, 50

United States v. Hamilton, 434 F. Supp. 2d 974 (D. Or. 2006).....26

United States v. Hernandez, 313 F.3d 1206 (9th Cir. 2002) 34

United States v. Hill, 749 F.3d 1250 (10th Cir. 2014).....4

United States v. Hill, 818 F.3d 289 (7th Cir. 2016).....4

United States v. Jacobsen, 466 U.S. 109 (1984).....34

United States v. Jones, 132 S. Ct. 945 (2012) 37, 38, 39, 44

United States v. Karo, 468 U.S. 705 (1984) 36, 37

United States v. Krupa, 658 F.3d 1174 (9th Cir. 2011).....46

United States v. Lang, 78 F. Supp. 3d 830 (N.D. Ill. Jan. 23, 2015).....27

United States v. Leon, 468 U.S. 897 (1984) 51, 52, 53

United States v. Luong, 470 F.3d 898 (9th Cir. 2006)..... 52, 53

United States v. Martinez, 2014 WL 5480686 (S.D. Cal. Oct. 28, 2014) 27

United States v. Miller, 425 U.S. 435 (1976) ..... *passim*

United States v. Moreno-Nevarez, 2013 WL 5631017 (S.D. Cal. Oct. 2, 2013) 27

United States v. Ocampo, 937 F.2d 485 (9th Cir. 1991) 47

United States v. Pitts, 6 F.3d 1366 (9th Cir. 1993).....47

United States v. Powell, 943 F. Supp. 2d 759 (E.D. Mich. 2013).....4

United States v. Reynolds, 626 F. App'x 610 (6th Cir. 2015).....4

United States v. Rigmaiden, 2013 WL 1932800 (D. Ariz. May 8, 2013) 27

United States v. Rodgers, 656 F.3d 1023 (9th Cir. 2011).....21

United States v. Rogers, 71 F. Supp. 3d 745 (N.D. Ill. 2014) 27

United States v. Salerno, 481 U.S. 739 (1987).....45

United States v. Serrano, 2014 WL 2696569 (S.D.N.Y. June 10, 2014).....27

United States v. Shah, 2015 WL 72118 (E.D.N.C. Jan. 6, 2015).....27

United States v. Underwood, 725 F.3d 1076 (9th Cir. 2013).....53

United States v. Van Leeuwen, 397 U.S. 249 (1970).....34

United States v. Watson, 423 U.S. 411 (1976) 42

United States v. Wheeler, -- F. Supp. 3d ---, 2016 WL 1048989 (E.D. Wis. Mar. 14, 2016) 27

United States v. White, 401 U.S. 745 (1971) 23

Utah v. Strieff, 136 S. Ct. 2056 (2016) 51, 52

Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646 (1995) 40

Zurcher v. Stanford Daily, 436 U.S. 547 (1978) 49, 50

CONSTITUTION AND FEDERAL STATUTES

U.S. Const. amend. IV ..... *passim*

12 U.S.C. § 1829b(b) 22

18 U.S.C. § 924(c) 13

18 U.S.C. § 924(j) 13

18 U.S.C. § 1959(a) 13

18 U.S.C. § 1962(d) 13

18 U.S.C. § 2701 .....7, 15

18 U.S.C. § 2703(c) ..... *passim*

18 U.S.C. § 2703(d) ..... *passim*

18 U.S.C. § 3231 3

18 U.S.C. § 3731 3

FEDERAL RULES

Fed. R. App. P. 4(b) 3

OTHER AUTHORITIES

Timothy Stapleton, *The Electronic Communications Privacy Act and Cell Location Data*, 73 Brook. L. Rev. 383 (2007).....5

No. 16-10109

IN THE UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellant,

v.

ANTONIO GILTON, *et al.*,

Defendants-Appellees.

REDACTED OPENING BRIEF FOR THE UNITED STATES
***** PUBLIC VERSION *****

L.G., a minor, was living in Los Angeles with her older brother, defendant Antonio Gilton, when she started a relationship with a pimp named Calvin Sneed. Eventually she advertised herself as a prostitute. In June 2012, L.G. and Sneed visited L.G.'s family in San Francisco. After L.G. and her mother had a late-night argument about whether L.G. should return to Los Angeles, L.G. asked Sneed to pick her up in his car. But as Sneed was about to do so, a silver SUV drove up next to his car, and a person in the SUV shot Sneed in the head, killing him. The police suspected the Gilton family. [redacted] officers

obtained a search warrant from a local magistrate judge for historical cell-site records of the phone numbers belonging to Barry Gilton and Antonio Gilton. (Those records indicate which cell towers a suspect's phone connected to over a given period of time.) The warrant obtained 37 days of call records and historical cell-site data for Antonio Gilton's number. Those records showed that Antonio Gilton was in the area of the murder shortly before it took place. In an indictment naming multiple other defendants involved in gang activity, Antonio and Barry Gilton were charged with four counts relating to the murder of Sneed.

After Antonio Gilton moved to suppress the evidence obtained through the state warrant, the district court suppressed the cell-site records for his phone. In so doing, the court erred for three reasons, any one of which independently warrants reversal. First, Antonio Gilton did not have a reasonable expectation of privacy in Sprint's business records. Second, the state search warrant was supported by probable cause, which is more than federal law requires for the acquisition of cell-site location information. And third, even if he had a reasonable expectation of privacy in the provider's records and the showing of probable cause in the warrant fell short, the records should nevertheless be admitted under the good faith exception to the exclusionary rule. Accordingly, this Court should reverse the district court's order granting his motion to suppress.

JURISDICTION, TIMELINESS, AND BAIL STATUS

The district court has jurisdiction under 18 U.S.C. § 3231. The court entered an order granting defendant's motion to suppress evidence on February 9, 2016. Excerpts of Record ("ER") 1-14. The government filed a timely notice of appeal on March 10, 2016. ER 189-90; *see* Fed. R. App. P. 4(b). This Court has jurisdiction under 18 U.S.C. § 3731. Antonio Gilton is currently being detained pending trial.

ISSUES PRESENTED

1. Whether the acquisition of historical cell-site records from a cellular-service provider, which the provider creates and maintains for business purposes, and which are generated by using a cell phone to make or receive calls, constitutes a Fourth Amendment search of the customer to whom the records pertain.

2. Whether the warrant for the cell-site data was supported by probable cause as to Antonio Gilton's phone.

3. If probable cause was lacking, whether the district court should have applied the good faith exception to the exclusionary rule.

STATEMENT OF THE CASE

A. Historical Cell-Site Information

Cell phones operate through the use of radio waves. *United States v. Carpenter*, 819 F.3d 880, 885 (6th Cir. 2016). A cell phone must send a signal to a

nearby cell tower in order to wirelessly connect a subscriber's call. *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d 600, 613 (5th Cir. 2013).

To facilitate cell phone use, cellular service providers maintain a network of radio base stations or cell towers throughout their coverage areas. *Id.* at 629. A cell site is a specific portion of the cell tower containing a wireless antenna, which detects the radio signal emanating from a cell phone and connects the cell phone to the local cellular network or Internet. *Id*. Cell towers may be divided into sectors (typically three) that each cover 120 degrees. *See United States v. Reynolds*, 626 F. App'x 610, 615 (6th Cir. 2015) (unpublished); *United States v. Hill*, 749 F.3d 1250, 1254 (10th Cir. 2014); *see also United States v. Graham*, 2016 WL 3068018, at *2, n.3 (4th Cir. May 31, 2016) (en banc); *United States v. Davis*, 785 F.3d 498, 503-04 (11th Cir.) (en banc), *cert. denied*, 136 S. Ct. 479 (2015). In urban areas, cell towers may be located relatively close together, while cell sites in rural areas may be farther apart. *United States v. Hill*, 818 F.3d 289, 295 (7th Cir. 2016).

A cellular phone automatically searches for a signal from nearby towers and "[o]nce the phone locates a tower, it submits a unique identifier – its 'registration' information – to the tower so that any outgoing and incoming calls can be routed through the correct tower." *United States v. Powell*, 943 F. Supp. 2d 759, 767 (E.D. Mich. 2013) (citing Timothy Stapleton, Note, *The Electronic*

Communications Privacy Act and Cell Location Data, 73 Brook. L. Rev. 383, 387 (2007)). "Nearby" is a relative term: it can range from a block (maybe less) to a couple miles (maybe more) depending on the tower density in the area. *See Davis*, 785 F.3d at 503; *In re Application of U.S.*, 405 F. Supp. 2d 435, 437 (S.D.N.Y. 2005). Although a cell phone often registers with its closest tower, "a variety of factors including physical obstructions and topography can determine which tower services a particular phone." *United States v. Evans*, 892 F. Supp. 2d 949, 952 (N.D. Ill. 2012).

"Cell-site location information" (CSLI) records from a cellular-service provider identify which cell towers the carrier used to route a user's calls and messages.[1] *United States v. Graham*, 2016 WL 3068018, at *2 (4th Cir. May 31, 2016) (en banc). In other words, CSLI identifies the equipment used to route calls and texts. *Graham*, 2016 WL 3068018, at *8. More specifically, wireless carriers typically log and store certain call-detail records of their customers' calls, including the date, time, and length of each call; the phone numbers engaged on the call; and the cell sites where the call began and ended. *Carpenter*, 819 F.3d at 885. CSLI records, however, do not include the content of personal

[1] The records at issue here are referred to as "historical" cell-site records because they were not generated in real time but were obtained from the provider's records for past calls.

communications, but only routing information that facilitates them. *Graham*, 2016 WL 3068018, at *8.

Cellular-service providers maintain these records not because they are obligated to do so by law (in fact they, are not), but because they serve legitimate business purposes. *Carpenter*, 819 F.3d at 887. "Carriers necessarily track their customers' phones across different cell-site sectors to connect and maintain their customers' calls," and keep CSLI records "to find weak spots in their network and to determine whether roaming charges apply, among other purposes." *Id.* at 887. The government does not require service providers to record this information or store it; instead, the providers control what they record and how long these records are retained. *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d at 611-12.

Before the provider can create such a record, though, it must receive information indicating that a cell phone user is relying on a particular cell tower. *Graham*, 2016 WL 3068018, at *5. The provider only receives that information when a cell phone user's phone exchanges signals with the nearest available cell tower. *Id.* A cell phone user therefore "conveys" location information to his provider by making use of the cell towers with which his phone connects with whenever he uses the provider's network. *Id.*

Although those records are kept by providers for business reasons, law enforcement officers can use those records to roughly approximate the suspect's location at a particular time. *Id.* at *1. However, historical cell tower location data does not identify the cell phone user's location with pinpoint precision – it simply identifies the cell tower that routed the user's call. *Davis*, 785 F.3d at 515. The range of a given cell tower will vary given the strength of its signal and the number of other towers in the area used by the same provider. *Id.* While the location of a user may be further defined by the sector of a given cell tower which relays the cell user's signal, the user may be anywhere in that sector. *Id.* This evidence still does not pinpoint the user's location. *Id.*

The Stored Communications Act (SCA or the Act), 18 U.S.C. § 2701 *et seq.*, provides procedures for obtaining information about telephone calls and subscribers from telephone providers. The procedures vary depending on the type of information sought. For the non-content records at issue here, the SCA raises the showing above that typically required to issue a subpoena and requires that a showing be made to a neutral magistrate, but it does not require that law enforcement officers seek a warrant to gain access to these non-content records. 18 U.S.C. § 2703(c), (d) (2012). Instead, the government may obtain "a record or other information pertaining to a subscriber to or customer of [an electronic communication service or a remote computing service] (not including the contents

of communications)" either through a warrant or "a court order." 18 U.S.C. § 2703(c)(1). To obtain a court order, the government must "offer[] specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought[] are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). The information that the government may obtain under such an order includes a subscriber's name and address, "telephone connection records," and "records of session times and durations." 18 U.S.C. § 2703(c)(2)(A)-(C).

B. Calvin Sneed's Murder

At approximately 2:00 a.m. on June 4, 2012, San Francisco Police Department officers responded to a report of shots fired in the Bayview, at Meade and Le Conte Avenues, and found Calvin Sneed slumped in the driver's seat of a Toyota Corolla. ER 414-15. Sneed had a gunshot wound to his head and was later pronounced dead. *Id.* His minor girlfriend, L.G., was screaming and crying next to the car. ER 414-15. She told the police that approximately eight months before the shooting, she had left San Francisco for Los Angeles to get a "new start," and that she had been staying with her "elder brother," Antonio Gilton, in Los Angeles. ER 415.

L.G. stated that she had met Sneed approximately four months before the shooting. *Id.* She subsequently learned that Sneed was pimping young women in

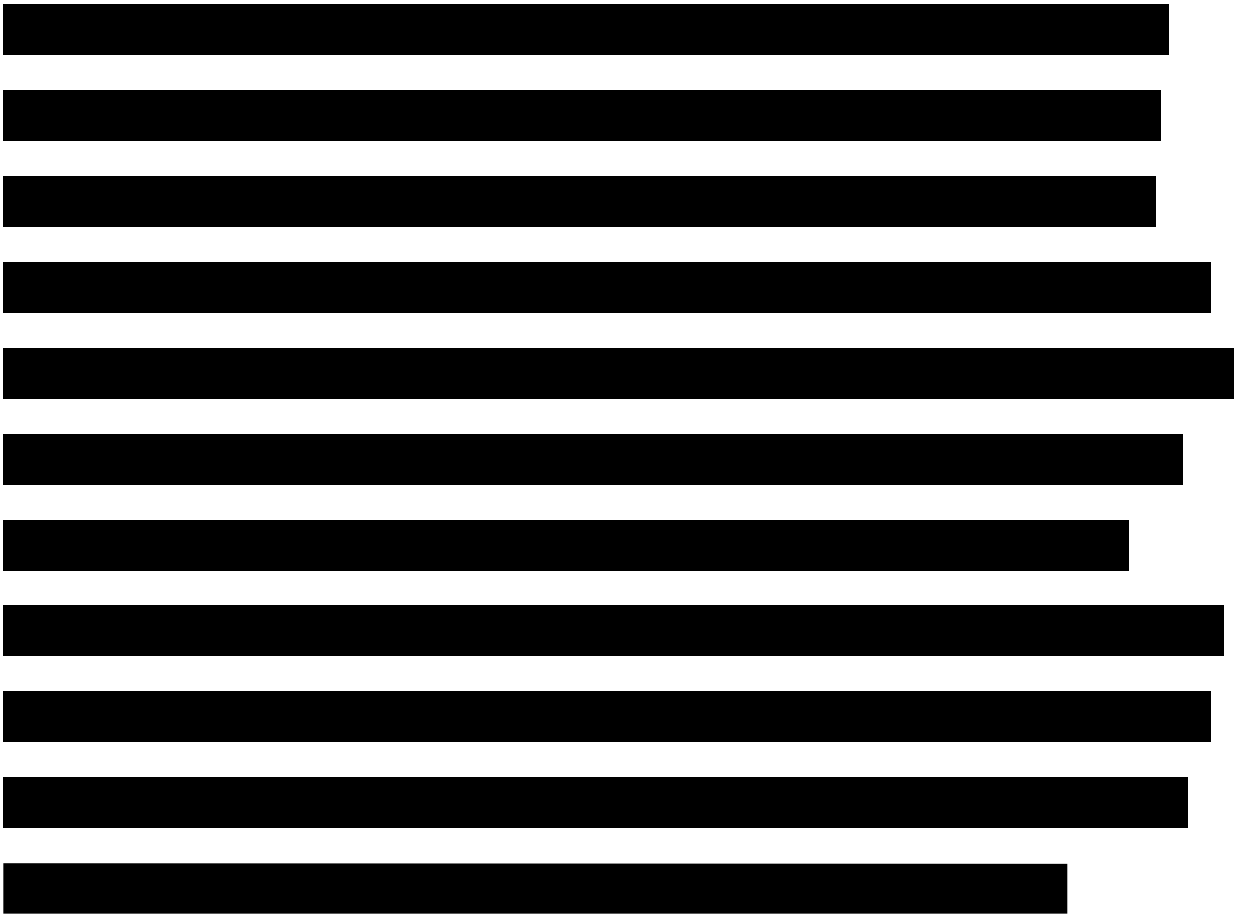
the Los Angeles area, and she began to advertise herself on various prostitution websites. *Id.* She said that after posting a picture of herself on a prostitution website, some of her girlfriends in San Francisco had found it, and that it was only a matter of time before her parents found out what she was doing in Los Angeles. *Id.* On May 31, 2012, her mother traveled to Los Angeles to try to persuade her to return to San Francisco. ER 415-16. A few days later, on June 3, 2012, L.G. and Sneed drove to San Francisco and arrived at her parents' home at approximately 4:00 p.m. ER 415-16.

At approximately 12:30 a.m. on June 4, 2012, L.G. had an argument with her mother about wanting to return to Los Angeles with Sneed. ER 416. She texted Sneed to pick her up from her parents' home and "used her brother's cell phone charger to charge her phone." *Id.* At approximately 1:49 a.m., she texted Sneed her parents' address. *Id.* A few minutes later, at approximately 1:56 a.m., he texted her to come outside. *Id.* Once outside, she noticed a silver SUV parked nearby with its lights on. *Id.* She saw Sneed's car arriving and called him to tell him to turn his headlights off. *Id.* The SUV then drove away. *Id.* As Sneed drove past where L.G. was standing, she saw the SUV reappear. *Id.* As the SUV accelerated up to Sneed's vehicle, L.G. heard gunshots and saw "muzzle flash" coming from the SUV. *Id.* She ran to Sneed's vehicle and found him slumped in the driver's seat with a gunshot wound to his head. *Id.*

After the murder, L.G. told police that she wanted to stay with her aunt, not her parents. ER 417. Later on June 4, 2012, at approximately 12:38 p.m., a police officer called her father, Barry Gilton, to tell him that his daughter wanted to stay with an aunt in Vallejo. ER 417. The father said that he would call back later to confirm an appointment to speak with the police. *Id.* At 2:32 p.m., the father called and left a message about confirming the time. *Id.* Roughly fifteen minutes later, an officer called back and Barry Gilton told him that he was coming to the police station as soon as possible. *Id.* At roughly 3:58 p.m., a lawyer left a message for the officer saying that Barry Gilton was with him. ER 418. After a subsequent call, the lawyer left a message for the officer saying that Barry Gilton would not speak with the police. *Id.*

L.G. allowed the police to search her cell phone. ER 419. During the search, the police identified cell phone numbers for her father (Barry Gilton), mother, older brother (Antonio Gilton), and younger brother, who was living at the parents' home at the time. *Id.* L.G. stated that the 424-XXX-XXXX number subsequently targeted in the Sprint warrant belonged to Antonio Gilton, her older brother. *Id.*

[redacted]



The SFPD also obtained historical CSLI for Barry Gilton's cell phone pursuant to an exigent request to T-Mobile on June 4, 2012. ER 419. According to those records, between 12:49 a.m. and 2:19 a.m. on June 4, 2012, Barry Gilton's cell phone was moving around San Francisco, from near his home to the Western Addition before returning to the vicinity of his home around the time of the murder, then traveling towards the northern area of the Mission after the shooting. ER 419. After the shooting, Barry Gilton told the police that he had returned to his house at approximately 12:15 a.m. and gone to his bedroom. *Id*. In fact, as the CSLI made clear, he had not. *Id.* The officers also reviewed video surveillance

from a camera near the site of the murder that appeared to identify the car used in the shooting. ER 418-19.

C. The Warrant

Based on all the information set forth above, San Francisco Police Department ("SFPD") Sergeant Gary Watts submitted an affidavit in support of a state search warrant, some portions of which were filed under seal. ER 414-20. The application sought CSLI for the cell phone number associated with Antonio Gilton, among other things. Watts averred that there was probable cause to believe that the cell phone numbers provided would tend to show "possible first-hand knowledge of those persons responsible for the shooting of . . . Calvin Sneed . . . and that the results of the subscriber identity information, all ingoing and outgoing calls, all text messages sent and received, . . . and the cell-site tower locations used on the date and times listed could possibly lead to the proper identity and the whereabouts of additional persons associated with this crime."[2] ER 419-20.

[2] The same Superior Court judge who issued the Sprint warrant also issued another warrant on June 6, 2012, this one to T-Mobile for the cell phone records of Barry Gilton (the "T-Mobile warrant"). The T-Mobile warrant identified the same three categories of information and the same date range for seizure as the Sprint warrant. Watts also wrote the affidavit submitted in support of the T-Mobile warrant. With limited exceptions, the affidavit was identical to the one submitted in support of the Sprint warrant. The district court did not suppress the information related to Barry Gilton's cell phone records.

On June 6, 2012, a judge of the Superior Court of California, County of San Francisco issued a warrant to Sprint for the seizure of cell phone records for the number 424-XXX-XXXX (the "Sprint warrant"). ER 412-13. The warrant identified three categories of information for seizure: (1) subscriber and billing information; (2) all incoming and outgoing calls and texts from May 1, 2012, to June 6, 2012; and (3) cell-site location information. ER 419-20. The only category at issue in this appeal is the third.

D. The Pending Charges

The Second Superseding Indictment charged Antonio and Barry Gilton in the following 4 of its 22 counts: (1) count one, conspiracy to conduct the affairs of an enterprise through a pattern of racketeering activity in violation of 18 U.S.C. § 1962(d); (2) count two, murder in aid of racketeering of Calvin Sneed in violation of 18 U.S.C. § 1959(a); (3) count three, use of a firearm in furtherance of a crime of violence in violation of 18 U.S.C. § 924(c)(1)(A); and (4) count four, use of a firearm in a murder in violation of 18 U.S.C. § 924(j). Clerk's Record ("CR") 139 ¶¶ 1-25; ER 260-70.

E. The Motion To Suppress

Antonio Gilton moved to suppress the evidence obtained pursuant to the Sprint warrant.[3] CR 570; ER 247-54. Antonio Gilton argued that the affidavit failed to establish probable cause to seize his cell phone data, and that it was so lacking in indicia of probable cause that the good faith exception did not apply. ER 251-54.

In its opposition, the government argued that: (1) Antonio Gilton had not established that the 424-XXX-XXX number belonged to him; (2) he had no reasonable expectation of privacy in the seized cell phone data; (3) the warrant was supported by probable cause; and (4) the police relied in good faith on the warrant. CR 677; ER 227-46. After Antonio Gilton filed his reply brief, ER 216-26, the government submitted a supplemental opposition brief arguing that the seizure of the cell phone data was also covered by the inevitable discovery doctrine.[4] ER 214-15.

---

[3] Although the record was not developed on this point, the government represents that that evidence was limited to records of calls made and received – that is, the numbers from and to which calls were made, the duration of those calls, and the historical CSLI. It did not include the contents of calls or text messages or any information about text messages. Although the information obtained through the warrant was not in the district court record, the government can supply it if the Court requests it.

[4] The government did not dispute that Antonio Gilton had a reasonable expectation of privacy in the contents of his incoming and outgoing text messages. ER 237 n.2, 245-46 n.6. Antonio Gilton did not dispute that he lacked a reasonable

F. The District Court's Order

The district court granted Antonio Gilton's motion to suppress. ER 1-14.

As an initial matter, the court concluded that there was "no serious dispute" that the cell phone number targeted by the Sprint warrant belonged to Antonio Gilton. ER 4. The court found that Antonio Gilton had a reasonable expectation of privacy in the historical CSLI he sought to suppress, relying on two decisions in the Northern District of California, *see In re Application for Tel. Info. Needed for a Criminal Investigation*, No. 15-cr-90304-LHK, 119 F. Supp. 3d 1011 (N.D. Cal. 2015); *United States v. Cooper*, No. 13-cr-00693-SI, 2015 WL 881578, at *6-*8 (N.D. Cal. Mar. 2, 2015). ER 4-5. Accordingly, the court concluded, probable cause was required to obtain that CSLI from Sprint. ER 5.

In so doing, the court incorporated by reference its reasoning from a separate order, in which it held that while a warrant was required, other defendants' CSLI should not be suppressed because it was obtained in good faith through applications under the Stored Communications Act, 18 U.S.C. § 2701 *et seq*. ER 191-95. In that other order, the court relied on "three principles: "'(1) an individual's expectation of privacy is at its pinnacle when government surveillance intrudes on the home; (2) long-term electronic surveillance by the government

---

expectation of privacy in his subscriber and billing information and the records of incoming and outgoing calls. ER 218 n.1.

implicates an individual's expectation of privacy; and (3) location data generated by cell phones, which are ubiquitous in this day and age, can reveal a wealth of private information about an individual.'" ER 195 (quoting 119 F. Supp. 3d at 1022-23). Applying these principles, the court concluded that individuals have a reasonable expectation of privacy in historical CSLI and that, as a result, probable cause was required to obtain it. *Id*.

Having reaffirmed its reasoning from its order denying the motions to suppress evidence obtained pursuant to a Section 2703(d) order, the court then turned in this order to the question whether the state search warrant affidavit established probable cause to search Antonio Gilton's phone and concluded it did not. ER 5. The court specifically held that "the affidavit submitted in support of the Sprint warrant plainly failed to provide a substantial basis for concluding that there was probable cause to search Antonio Gilton's cell phone records" because the affidavit "hardly mention[ed]" Antonio Gilton, and that "[t]hese passing, innocuous references to A[ntonio] Gilton constitute the only information about him in the affidavit." *Id.* The court further held that the affidavit "does not even assert, or provide a substantial basis for inferring, that Antonio Gilton was in the San Francisco area at the time of the shooting." *Id.* The district court discounted the fact that the girlfriend told the police that she "used her brother's cell phone charger to charge her phone," noting that there was "no indication" that she was

referring to Antonio Gilton's charger as opposed to her younger brother's, who, according to the affidavit, was then living at the parents' home. ER 5-6.

The district court did not reference the sealed material – [redacted] Instead, the court simply noted in passing that "[a]lthough the affidavit submitted in support of the Sprint warrant includes additional information beyond that described above, there are no other references to Antonio Gilton. Much of the additional information concerns the girlfriend's father, Barry Gilton." ER 2.

Accordingly, the district court concluded that it was "not convinced" that the facts set forth in the affidavit "pointed to the murder being a family-based attack." ER 6. Even assuming that the facts stated in the affidavit supported a reasonable inference of a "family-based attack," the court held, those facts pointed to one particular family member being involved in the attack: Barry Gilton, not Antonio. *Id.* Accordingly, the district court concluded, the notion that the affidavit supported a reasonable inference of a "family-based attack" did not create a

plausible connection between Antonio Gilton and the shooting given that there was no indication in the affidavit that any particular family member other than Barry Gilton had been involved, or that Antonio Gilton was in or around San Francisco on or around June 4, 2012. ER 8.

The court then turned to whether the good faith exception applied. ER 8. Acknowledging that the good faith exception applies unless the affidavit is "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable," *id.* (quoting *United States v. Grant*, 682 F.3d 827, 836 (9th Cir. 2012)), the court concluded that it was "entirely unreasonable" to believe that the affidavit's "passing, innocuous" references to Antonio Gilton established probable cause to obtain his cell phone data.[5] ER 8.

Accordingly, the court granted his motion to suppress the cell phone data obtained through the warrant. ER 13.

SUMMARY OF ARGUMENT

This Court should reverse the district court's order for any one of three reasons. First, law enforcement officers did not violate Antonio Gilton's Fourth Amendment rights by obtaining Sprint's business records pursuant to a state warrant because the CSLI did not belong to Antonio Gilton, was not maintained

[5] The court also concluded that the inevitable discovery doctrine did not apply. ER 10-11. The government does not contest that ruling on appeal.

for his benefit, and was not stored in a place in which he had a reasonable expectation of privacy. Although this Court has not decided the issue (and indeed need not if it concludes that the district court erred in holding the warrant insufficient or in finding the good faith exception inapplicable), every Court of Appeals to have considered the issue (namely, the Fourth, Fifth, Sixth, and Eleventh Circuits) has concluded that historical cell-site information is obtainable without a warrant and probable cause. Those holdings follow from settled Fourth Amendment principles set out by the Supreme Court in *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979), and are consistent with this Court's holdings in *United States v. Forrester*, 512 F.3d 500 (9th Cir. 2008), and *United States v. Golden Valley Electric Ass'n*, 689 F.3d 1108 (9th Cir. 2012). Moreover, even if the acquisition constituted a Fourth Amendment search, the search was reasonable because the Fourth Amendment requires no more than "reasonable grounds to believe that the records [were] relevant to an investigation" – the Stored Communications Act subpoena standard set forth in 18 U.S.C. § 2703(d).

Second, this Court should reverse the district court's order because the court erred in finding that the warrant was not supported by probable cause as to Antonio Gilton's cell phone. Specifically, the district court analyzed the sufficiency of the affidavit based on whether or not it established that Antonio Gilton was involved in

the murder. That was legal error. In fact, the court should have evaluated (but did not) the sufficiency of the affidavit based on whether or not it established probable cause that Antonio Gilton's cell phone records would contain evidence about the identities of the persons responsible for Calvin Sneed's murder. The affidavit did that because it set forth facts providing reason to believe that the murder was committed by L.G.'s family and that more than one person was involved.

Third, even if the warrant was not adequately supported by probable cause, the district court erred in finding that the officers could not have relied in good faith on it. [redacted] Given the facts of the case, an officer could reasonably have concluded that the murder was a family-based retaliation against Sneed for encouraging L.G. to get involved in prostitution [redacted]. At a minimum, therefore, officers could have formed an objectively reasonable belief that there existed a fair probability that evidence relevant to the murder would be found in Antonio Gilton's historical cell-site records.

ARGUMENT

I. THE FOURTH AMENDMENT DOES NOT REQUIRE A WARRANT ESABLISHING PROBABLE CAUSE TO OBTAIN HISTORICAL CSLI

A. Standard Of Review

Motions to suppress are reviewed de novo. *See United States v. Rodgers*, 656 F.3d 1023, 1026 (9th Cir. 2011); *Forrester*, 512 F.3d at 506 ("Conclusions of law underlying the denial of a motion to suppress evidence are also reviewed de novo."). The trial court's factual findings are reviewed for clear error. *See United States v. Booth*, 669 F.2d 1231, 1238 (9th Cir. 1981).

B. Under The Third-Party Doctrine, Individuals Do Not Have A Reasonable Expecation Of Privacy In Business Records Maintained by Their Cell Phone Carriers

1. The Third-Party Doctrine

As a general matter, "[a] search occurs when an expectation of privacy that society is prepared to consider reasonable is infringed." *Maryland v. Macon*, 472 U.S. 463, 469 (1985); *Katz v. United States*, 389 U.S. 347 (1967). Accordingly, whether the Fourth Amendment's protections are implicated normally embraces two discrete questions: first, whether the individual, by his conduct, has "exhibited an actual (subjective) expectation of privacy," *Katz*, 389 U.S. at 361 (Harlan, J., concurring); and second, whether the individual's subjective expectation of privacy is "one that society is prepared to recognize as 'reasonable,'" *id.* at 361. Even if an

individual has a subjective expectation of privacy, the Supreme Court has repeatedly held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith*, 442 U.S. at 743-44; *see also Forrester*, 512 F.3d at 509 (discussing third-party doctrine). This rule – the third-party doctrine – applies even when "the information is revealed" to a third party "on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Miller*, 425 U.S. at 443.

In *Miller*, the government had obtained by subpoena records of the defendant's checks and other records from his banks.[6] 425 U.S. at 436, 437-38. The banks were required to keep those records under the Bank Secrecy Act of 1970, 12 U.S.C. 1829b(b). 425 U.S. at 436, 440-41. The Court held that the government's acquisition of those records was not an "intrusion into any area in which [the defendant] had a protected Fourth Amendment interest." *Id.* at 440. The Court explained that "[o]n their face, the documents subpoenaed here are not [the defendant's] private papers." *Id.* (internal quotation marks omitted). He could "assert neither ownership nor possession" of the records; rather, they were "business records of the banks." *Ibid.*

[6] The Fourth Amendment also permits the government to obtain business records through a subpoena, without either a warrant or a showing of probable cause. *See Oklahoma Press Pub. Co. v. Walling*, 327 U.S. 186, 194-95 (1946); *see also Miller*, 425 U.S. at 445-46.

The defendant nevertheless argued that "he ha[d] a Fourth Amendment interest in the records kept by the banks because they [were] merely copies of personal records that were made available to the banks for a limited purpose and in which he ha[d] a reasonable expectation of privacy." 425 U.S. at 442. The Court rejected that argument, explaining that "[a]ll of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business." *Id.* "This Court," it continued, "has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose." *Id.* at 443 (citing *United States v. White*, 401 U.S. 745, 751-52 (1971); *Hoffa v. United States*, 385 U.S. 293, 302 (1966); and *Lopez v. United States*, 373 U.S. 427 (1963)). The Court added that, "even if the banks could be said to have been acting solely as Government agents" in light of the fact that the Bank Secrecy Act required the banks to maintain the records, that would not change the Fourth Amendment analysis. *Miller*, 425 U.S. at 443.

The Court applied the same principles in *Smith* to a record created by the telephone company. In *Smith*, the police requested that the defendant's telephone company install a pen register at its offices to record the numbers dialed from the

defendant's home phone. 442 U.S. at 737. The defendant argued that the government's acquisition of a record of his dialed numbers violated his reasonable expectation of privacy and therefore qualified as a Fourth Amendment search. *Id.* at 741-42. As in *Miller*, the Court rejected that argument. The Court explained that for the Fourth Amendment to apply to the government's acquisition of such information, two requirements must be met: (i) an individual must "by his conduct . . . exhibit[] an actual (subjective) expectation of privacy" in the information; and (ii) that "subjective expectation of privacy," when "viewed objectively," must be "one that society is prepared to recognize as reasonable." *Id.* at 740 (internal quotation marks omitted).

The Court determined that the defendant's asserted expectation of privacy in the numbers dialed from his phone satisfied neither the subjective nor the objective requirement. The Court first expressed "doubt that people in general entertain any actual expectation of privacy in the numbers they dial," 442 U.S. at 742, because "[t]elephone users . . . typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes," *id.* at 743. And the Court rejected the defendant's contention that he had an idiosyncratic expectation of privacy in the number he dialed. *Id.* The Court went on to explain that "even if [the defendant]

did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not one that society is prepared to recognize as reasonable." *Id.* (internal quotation marks omitted). That was because "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Id.* at 743-44 (citing, among other things, *Miller*, 425 U.S. at 442-44). "When he used his phone," the Court continued, the defendant "voluntarily conveyed numerical information to the telephone company and exposed that information to its equipment in the ordinary course of business." *Id.* at 744.

Smith and *Miller* stand for three basic principles: first, that an individual has no reasonable expectation of privacy in information voluntarily provided to a third party in a business transaction; second, an individual can therefore not object to the production of business records of a third party that that third party generates, even if based on information from a customer; and third, those principles apply fully to addressing or routing information obtained and recorded by communications providers.

Applying those principles, this Court has held that computer investigative techniques that reveal the to/from addresses of email messages, the IP addresses of websites visited and the total amount of data transmitted to or from an account are not Fourth Amendment searches. *Forrester*, 512 F.3d at 510-11. Instead, this Court concluded, the investigative techniques the government employed were

"constitutionally indistinguishable" from the use of a pen register approved in *Smith*. *Id.* Noting that *Smith* based its holding that telephone users have no expectation of privacy in the numbers they dial on the users' imputed knowledge that their calls are completed through telephone company switching equipment, 442 U.S. at 742, this Court held that email and Internet users "have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information." *Forrester*, 512 F.3d at 510. Like telephone numbers, "which provide instructions to the 'switching equipment that processed those numbers,'" email to/from addresses and IP addresses "are not merely passively conveyed through third party equipment, but rather are voluntarily turned over in order to direct the third party's servers." *Id.*

Similarly, this Court rejected a request to quash a subpoena for a power company's power consumption records for three customer residences, holding that "a customer ordinarily lacks 'a reasonable expectation of privacy in an item,' like a business record, 'in which he has no possessory or ownership interest.'" *Golden Valley Electric Ass'n*, 689 F.3d at 1116 (citing *United States v. Cormier*, 220 F.3d 1103, 1108 (9th Cir. 2000) (motel registration records); *Miller*, 425 U.S. at 440 (1976); *United States v. Hamilton*, 434 F. Supp. 2d 974, 979-80 (D. Or. 2006)

(electricity consumption records)). Because those records consisted of information voluntarily conveyed to the power company and exposed to their employees in the ordinary course of business by the company's customers, no warrant was necessary. *Golden Valley Elec. Ass'n*, 689 F.3d at 1116.

2. Under The Third-Party Doctrine, Antonio Gilton Did Not Have A Reasonable Expectation Of Privacy In CSLI Maintained By His Cell Phone Carrier

Applying the principles set forth in *Smith* and *Miller*, every Court of Appeals to have considered the issue (namely, the Fourth, Fifth, Sixth, and Eleventh Circuits) has concluded that historical cell-site information is obtainable without a warrant and probable cause.[7] *Graham*, 2016 WL 3068018 at *1 (obtaining

[7] The vast majority of district courts have reached the same conclusion. *See, e.g.*, *United States v. Wheeler*, -- F. Supp. 3d --, --, 2016 WL 1048989, at *11-*13 (E.D. Wis. Mar. 14, 2016); *United States v. Chavez*, 2016 WL 740246, at *2-*4 (D. Conn. Feb. 24, 2016); *United States v. Epstein*, 2015 WL 1646838, at *4 (D.N.J. Apr. 14, 2015); *United States v. Dorsey*, 2015 WL 847395, at *8 (C.D. Cal. Feb. 23, 2015); *United States v. Lang*, 78 F. Supp. 3d 830, 835-37 (N.D. Ill. Jan. 23, 2015); *United States v. Shah*, 2015 WL 72118, at *7-*9 (E.D.N.C. Jan. 6, 2015); *United States v. Martinez*, 2014 WL 5480686, at *3-*5 (S.D. Cal. Oct. 28, 2014); *United States v. Rogers*, 71 F. Supp. 3d 745, 748-50 (N.D. Ill. 2014); *United States v. Giddins*, 57 F. Supp. 3d 481, 491-94 (D. Md. 2014); *United States v. Banks*, 52 F. Supp. 3d 1201, 1204-06 (D. Kan. 2014); *United States v. Serrano*, 2014 WL 2696569, at *6-*7 (S.D.N.Y. June 10, 2014); *United States v. Moreno-Nevarez*, 2013 WL 5631017, at *1-*2 (S.D. Cal. Oct. 2, 2013); *United States v. Rigmaiden*, 2013 WL 1932800, at *14 (D. Ariz. May 8, 2013); *United States v. Gordon*, 2012 WL 8499876, at *2 (D.D.C. Feb. 6, 2012); *United States v. Benford*, 2010 WL 1266507, at *2-*3 (N.D. Ind. Mar. 26, 2010); *In re Applications of U.S. for Orders Pursuant to Title 18, U.S. Code Section 2703(d)*, 509 F. Supp. 2d 76, 79-82 (D. Mass. 2007). *But see In re Application for Tel. Info. Needed for a Criminal Investigation*, 119 F. Supp. 3d 1011, 1024 (N.D. Cal. 2015); *In re Application of*

historical cell-site location information from defendants' cell phone provider without a warrant to deduce defendants' approximate locations at times that crimes took place did not violate the Fourth Amendment; defendants had no reasonable expectation of privacy in that historical location information, as they voluntarily conveyed such information to cell phone provider by making and receiving calls and texts on their phones); *Carpenter*, 819 F.3d at 886-91 (government did not conduct a "search" for Fourth Amendment purposes when it obtained business records from defendants' wireless carriers for cell phone service, containing cell tower locational data); *Davis*, 785 F.3d at 511 (defendant had no subjective or objective reasonable expectation of privacy in carrier's business records showing the cell tower locations that wirelessly connected his calls at or near the time of six of seven robberies); *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d at 612 (cell-site data are business records and authorization of 18 U.S.C. § 2703(d) orders for historical cell-site information if an application meets the lesser "specific and articulable facts" standard, rather than the Fourth Amendment probable cause standard, is not per se unconstitutional). This Court should reach the same conclusion here.

U.S. for an Order Authorizing Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 120-27 (E.D.N.Y. 2011).

Here, the data obtained by the warrant consisted of two categories of data for a specific time period bracketing the murder: (1) the records of who Antonio Gilton called (and who called him) – that is, the phone numbers involved, the start and end time of the calls, and their duration; and (2) the historical cell-site information generated by those calls. Because Antonio Gilton has not demonstrated a subjective expectation of privacy, let alone "one that society is prepared to recognize as 'reasonable,'" *Katz*, 389 U.S. at 361, the district court erred in suppressing that information. This is so because Antonio Gilton voluntarily provided that information to Sprint in a business transaction, the CSLI at issue consists of Sprint's business records generated for its own purposes, even if based on information Antonio Gilton provided, and the data was limited to addressing or routing information obtained and recorded by Sprint in the ordinary course of business.

First, Antonio Gilton voluntarily conveyed CSLI when making or receiving a call. Here, as in *Smith*, 442 U.S. at 737, 744, Antonio Gilton unquestionably "exposed" the information at issue to the phone company's "equipment in the ordinary course of business." *Id.* Each time he made or received a call – activities well within the "ordinary course" of cell phone ownership – his cell phone carrier generated a record of the phone numbers involved and the cell towers used. The CSLI that the company recorded was necessary to route his cell phone calls, just as

the dialed numbers recorded by the pen register in *Smith* were necessary to route the defendant's landline calls. Having "exposed" the CSLI to the company, Antonio Gilton, like the defendant in *Smith*, "assumed the risk" that the phone company would disclose this information to the government.[8] *Smith*, 442 U.S. at 744; *see Graham*, 2016 WL 3068018, at *4; *Carpenter*, 819 F.3d at 887-89 (holding that "for the same reasons that Smith had no expectation of privacy in the numerical information at issue [in *Smith*], the defendants have no such expectation in the [CSLI] locational information here"); *Davis*, 785 F.3d at 511-13 (holding that defendant has no "objective[ly] reasonable expectation of privacy in MetroPCS's business records showing the cell tower locations that wirelessly connected his calls").

[8] The Third Circuit has held that that "[a] cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way," but nonetheless concluded that "CSLI from cell phone calls is obtainable under a § 2703(d) order," which "does not require the traditional probable cause determination" necessary for a warrant. *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304, 313, 317 (3d Cir. 2010). Although the court stated that "it is unlikely that cell phone customers are aware that their cell phone providers collect and store historical location information," *id.* at 317 (emphasis omitted), a factual premise the Fourth, Fifth, and Eleventh Circuits have rejected, the court did so only to note the possibility that the government's acquisition of such information could implicate the Fourth Amendment "if it would disclose location information about the interior of a home," *id.*; *see id.* at 320 (Tashima, J., concurring in the judgment).

As noted above, a cell phone must send a signal to a nearby cell tower in order to wirelessly connect a subscriber's call. *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d at 613. Indeed, any cell phone user who has seen her phone's signal strength fluctuate must know that when she places or receives a call, her phone "exposes" its location to the nearest cell tower and thus to the company that operates the tower. *Carpenter*, 819 F.3d at 888-90; *accord Davis*, 785 F.3d at 511; *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d at 613-14. And, as most users also know, cell phones do not work when they are outside the range of the provider company's cell tower network. *Davis*, 785 F.3d at 511. That is why, for example, cell phones often cannot receive a signal in sparsely populated areas or underground. *Id.* Simply put, for his cell phone to make or receive calls, Antonio Gilton had to voluntarily transmit information to Sprint – information that included data about his approximate location.[9]

---

[9] Sprint expressly advised its subscribers (including Antonio Gilton) that location data was stored and shared with law enforcement. The Internet Archive, a non-profit digital library, copied Sprint's Privacy Policy on May 9 and August 29 of 2012. At these times, the Privacy Policy stated: "Information we collect when we provide you with Services includes when your wireless device is turned on, how your device is functioning, device signal strength, *where it is located*, what device you are using, what you have purchased with your device, how you are using it, and what sites you visit." (Emphasis added). *See* http://web.archive.org/web/20120509224057/http:/www.sprint.com/legal/privacy.html?INTNAV=ATG:FT:Privacy; http://web.archive.org/web/20120829032456/http:/www.sprint.com/legal/privacy.h

Second, as with the bank records in *Miller*, Antonio Gilton "can assert neither ownership nor possession" of the records at issue here. To the contrary, they are Sprint's own "business records" that Sprint created for its own purposes. *Miller*, 425 U.S. at 440; *Carpenter*, 819 F.3d at 887; *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d at 611-12. Indeed, unlike in *Miller*, the records at issue here are not even copies of documents that Antonio Gilton submitted to Sprint, and the government did not require Sprint to keep the records. *See Miller*, 425 U.S. at 442; *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d at 612. Instead, they are records that Sprint created for its own business purposes as part of the process of providing telephone service to customers. *Carpenter*, 819 F.3d at 887. As noted above, "[c]arriers necessarily track their customers' phones across different cell-site sectors to connect and maintain their customers' calls," and keep CSLI records "to find weak spots in their network and

---

tml?INTNAV=ATG:FT:Privacy. Similarly, the Internet Archive copied Sprint's Terms and Conditions on March 30 and July 5, 2012. At these times, the Terms and Conditions included provisions that stated: "As we provide telecommunications products and Services to you (the account holder), we develop information about the quantity, technical configuration, type, *location, and destination of telecommunications products and Services you use*" and "[o]*ur networks generally know the location of your Device when it is outdoors and/or turned on*." http://web.archive.org/web/20120330073913/http:/shop2.sprint.com/en/legal/legal_terms_privacy_popup.shtml?ECID=vanity:termsandconditions (Emphasis added); http://web.archive.org/web/20120705001309/http:/shop2.sprint.com/en/legal/legal_terms_privacy_popup.shtml?ECID=vanity:termsandconditions.

to determine whether roaming charges apply, among other purposes." *Id*. And, providers control what they record and how long these records are retained. *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d at 612; *see also S.E.C. v. Jerry T. O'Brien*, 467 U.S. 735, 743 n.11 (1984) (noting that any Fourth Amendment interests of investigative targets in certain third-party business records would be "substantially weaker than those of the bank customer in *Miller* because respondents, unlike the customer, cannot argue that the subpoena recipients were required by law to keep the records in question").

Third, the data was limited to addressing or routing information obtained and recorded by Sprint in the ordinary course of business. In determining whether a reasonable expectation of privacy exists, courts have consistently distinguished routing information from the contents of communications, according the former significantly less protection. *See, e.g.*, *Carpenter*, 819 F.3d at 886-90 (contrasting *Katz*, 389 U.S. at 361 (party has reasonable expectation of privacy in content of phone calls) with *Ex Parte Jackson*, 96 U.S. 727, 733 (1878) (no reasonable expectation of privacy in outward form and weight of mailings)); *Smith*, 442 U.S. at 740 (no reasonable expectation of privacy in numbers dialed). Thus, "although the content of personal communications is private, the information necessary to get

those communications from point A to point B is not."[10] *Carpenter*, 819 F.3d at 886-90 (citing *Ex parte Jackson*, 96 U.S. at 733 (holding that the "outward form and weight" of mailings, including the recipient's name and physical address was not constitutionally protected)).

Here, the records of calls and the cell-site information both "fall on the unprotected side of this line" because they "say nothing about the content of any calls." *Carpenter*, 819 F.3d at 887-90. The cell-site records – like mailing addresses, phone numbers, and IP addresses – are information that facilitates personal communications, rather than part of the content of those communications. *Id.* As such, the acquisition of cell-site records does not qualify as a Fourth

[10] In a line of cases dating back to the nineteenth century, the Supreme Court has held that the government cannot engage in a warrantless search of the contents of sealed mail, but can observe whatever information people put on the outside of mail, because that information is voluntarily transmitted to third parties. *See United States v. Jacobsen*, 466 U.S. 109, 114 (1984) (stating that warrantless searches of letters and sealed packages are "presumptively unreasonable"); *United States v. Van Leeuwen*, 397 U.S. 249, 251-52 (1970) (mail is "free from inspection . . . except in the manner provided by the Fourth Amendment," but postal authorities could nonetheless detain mail without warrant based on suspicious appearance and circumstances); *Ex parte Jackson*, 96 U.S. 727, 733 (1877) ("Letters and sealed packages of this kind in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles."); *see also United States v. Hernandez*, 313 F.3d 1206, 1209-10 (9th Cir. 2002) ("Although a person has a legitimate interest that a mailed package will not be opened and searched en route, there can be no reasonable expectation that postal service employees will not handle the package or that they will not view its exterior.").

Amendment search of the cellphone user. *See Forrester*, 512 F.3d at 511 (investigative techniques that revealed the to/from addresses of e-mail messages, the IP addresses of websites visited, and the total amount of data transmitted to or from an account not a Fourth Amendment search).

This remains true even though that cell-site records may allow investigators to draw inferences about the whereabouts of the user of the phone. "An inference is not a search." *Kyllo v. United States*, 533 U.S. 27, 36 n.4 (2001). Law-enforcement investigators regularly deduce facts about a person's movements or conduct from information gleaned from third parties. Indeed, that is a central feature of criminal investigations. *See Donaldson v. United States*, 400 U.S. 517, 522 (1971) (explaining that the lack of Fourth Amendment protection for third-party business records was "settled long ago"); *id.* at 537 (Douglas, J., concurring) ("There is no right to be free from incrimination by the records or testimony of others."). For example, law-enforcement officers can infer from an eyewitness statement that a suspect was in a particular location at a particular time, from a credit-card slip that she regularly dines at a particular restaurant, and from a key-card entry log his routine hours at a gym. But merely because facts about a person can be deduced from records or other information in the possession of third parties does not make the acquisition of that information a Fourth Amendment search of the person. *See Forrester*, 512 F.3d at 510 (noting that certain phone numbers may

strongly indicate the underlying contents of the communication, and that, when an individual dials a pre-recorded information or subject-specific line, such as sports scores or lottery results, the phone number may even show that the caller had access to specific content information). Indeed, the pen-register records in *Smith* allowed a far more specific inference about a caller's whereabouts – his presence in his home. Yet the third-party doctrine still applied.

For all of these reasons, Antonio Gilton did not have a reasonable expectation of privacy in the historical CSLI records that the government obtained from his cell phone service provider.

C. No Fourth Amendment Precedent Supports A Contrary Result

None of the Supreme Court cases dealing either with locational information or cell phones justifies a contrary result. In *United States v. Karo*, 468 U.S. 705 (1984), the Supreme Court concluded that police officers conducted a Fourth Amendment search when they used a beeper device to monitor the location of a container within a private residence. *Id.* at 714. Similarly, in *Kyllo*, this Court held that the use of a thermal imaging device "that is not in general public use[] to explore details of the home that would previously have been unknowable without physical intrusion" is a Fourth Amendment search. 533 U.S. at 40. But in each case, the use of the device in question permitted the authorities to obtain information from inside a house that had not already been exposed to the public.

See Kyllo, 533 U.S. at 34-40; *Karo*, 468 U.S. at 714-16. In this case, however, the government is not obtaining information about an individual's or object's presence in a home. Antonio Gilton had already exposed the information necessary to create the cell-site records to Sprint, and the SFPD obtained that information from Sprint through lawful process. Neither *Karo* nor *Kyllo* involved the acquisition of business records from a third party based on information voluntarily conveyed by a customer; this case – like *Miller* and *Smith* – involves exactly that situation.

Nor does *United States v. Jones*, 132 S. Ct. 945, 949 (2012), in which the Supreme Court held that the warrantless installation and use of a Global Positioning System (GPS) tracking device on a vehicle to continuously monitor its movements over 28 days constituted a Fourth Amendment "search," support the finding of a search here. *Jones* relied on the fact that the government had "physically intrud[ed] on a constitutionally protected area" – namely, the suspect's automobile – to attach the device. *Id.* at 950 n.3. Because the Court concluded that the attachment of the device constituted "a classic trespassory search," it did not even reach the *Katz* standard, let alone hold that tracking a person's vehicle on public streets violates a reasonable expectation of privacy. *See Jones*, 132 S. Ct. at 953-54. In this case, by contrast, no contention could be made that any such physical occupation occurred. And, while the concurring opinions in *Jones* would have found a search based on the *Katz* expectation-of-privacy test, *see id.* at 954-56

(Sotomayor, J., concurring); *id.* at 962-64 (Alito, J., concurring in the judgment), the Court did not (and, as discussed below, the analysis in the concurrences does not support the finding of a search here).

Similarly, in *Riley v. California*, 134 S. Ct. 2473 (2014), the Supreme Court held that a law-enforcement officer generally must obtain a warrant to search the contents of a cell phone found on an arrestee. *Id.* at 2485. But in *Riley*, there was no dispute that an officer's physical review of the contents of a cell phone constituted a Fourth Amendment search; the question was whether that search fell within the traditional search-incident-to-arrest exception to the warrant requirement. *See id.* at 2482, 2492-93 (distinguishing *Smith v. Maryland*, *supra*, for that reason). *Riley* casts no doubt on Supreme Court holdings that an individual has no Fourth Amendment interest in records pertaining to the individual that are created by third parties, or in information he voluntarily conveys to third parties.

Not only are the holdings of *Jones* and *Riley* inapplicable here, but the broader privacy concerns raised in those cases (and the concurrences by Justice Alito and Justice Sotomayor in *Jones*) do not justify finding a Fourth Amendment search when the government acquires historical CSLI from a provider. The GPS tracking device in *Jones* allowed law-enforcement officers to use "signals from multiple satellites" to continuously track the movements of the defendant's vehicle over the course of 28 days, accurate to "within 50 to 100 feet." 132 S. Ct. at 948.

By contrast, the information here consisted of records indicating which of the cellular-service provider's antennas communicated with petitioner's phone only when the phone was making or receiving calls, not continuously. And although these records contained historical cell-site information for a 37-day period, the information revealed only that Antonio was somewhere within the specified sector of a cell tower when he made or received calls. Moreover, not only is CSLI far less precise than GPS information, but the individuals who use cell phones are providing location-related information to the phone company to make or receive calls, and the phone company is making a record of that routing information for its own purposes. This case thus presents no occasion to consider the legal implications of government-installed or government–mandated technology capable of "secretly monitor[ing] and catalog[ing] every single movement" an individual makes continuously "for a very long period." *Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment); *see id.* at 955 (Sotomayor, J., concurring); *see also id.* at 957 (recognizing that prevailing law includes the third-party doctrine under *Smith* and *Miller* and noting that determining whether to alter that doctrine was not necessary in that case).

Likewise, this case does not implicate a central concern in *Riley*: that cell phones may contain "vast quantities of personal information" that could be used to discern "[t]he sum of an individual's private life," including information about the

user's health, family, religion, finances, political and sexual preferences, and shopping habits, as well as GPS records of the user's "specific movements down to the minute, not only around town but also within a particular building." 134 S. Ct. at 2485, 2489-90. As explained, the historical cell-site records obtained in this case would only reveal Antonio Gilton's approximate location, not the content of his calls. They could not reveal any information stored on his phone or permit law-enforcement officers to learn the sort of detailed personal facts that the Court identified in *Riley*.

D. Even Assuming That Government Acquisition Of CSLI Is A Fourth Amendment Search, A Showing Of Reasonable Relevance To An Investigation, Rather Than Probable Cause, Would Satisfy The Fourth Amendment's Reasonableness Requirement

Even if this Court were to hold (or assume) that the use of government process to acquire CSLI is a Fourth Amendment "search," the Fourth Amendment would not require a showing of probable cause to justify such process. Not all Fourth Amendment searches require probable cause. "As the text of the Fourth Amendment indicates, the ultimate measure of the constitutionality of a governmental search is 'reasonableness.'" *Maryland v. King*, 133 S. Ct. 1958, 1969 (2013) (internal quotation marks omitted). A "warrant is not required to establish the reasonableness of all government searches; and when a warrant is not required (and the Warrant Clause therefore not applicable), probable cause is not invariably required either." *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 653

(1995). In deciding the appropriate procedure required by the Fourth Amendment, courts "balance the privacy-related and law enforcement-related concerns to determine if the intrusion was reasonable." *King*, 133 S. Ct. at 1970 (internal quotation marks omitted).

In this context, Congress has balanced those concerns through the Stored Communications Act, which authorizes a phone company to disclose to law enforcement call records and historical cell-site information upon receipt of either a Rule 41 search warrant (18 U.S.C. § 2703(c)(1)(A)), or a Section 2703(d) court order supported by a finding that reasonable grounds exist to conclude that the records are relevant and material to an investigation (18 U.S.C. § 2703(c)(1)(B) & (d)). Pursuant to Section 2703(d), to obtain an order for a phone company's records, it is enough for the government to provide "specific and articulable facts showing that there are reasonable grounds to believe that the [records] are relevant and material to an ongoing criminal investigation." *See In re Application of United States for an Order Directing a Provider of Electronic Communication Serv. To Disclose Records*, 620 F.3d at 313 ("this standard is a lesser one than probable cause").

Although the Section 2703(d) standard is not directly at issue here because the officers sought a warrant, the district court's ruling that historical CSLI may only be obtained with a warrant and probable cause implies that the procedure (and

standard of proof) set forth by Congress in the Act is constitutionally deficient. But this Court applies a "strong presumption of constitutionality" to statutes, "especially when it turns on what is 'reasonable'" within the meaning of the Fourth Amendment. *United States v. Watson*, 423 U.S. 411, 416 (1976). In light of those principles, even if the acquisition of Sprint's CSLI records pertaining to Antonio Gilton qualified as a Fourth Amendment search, at a minimum, the affidavit in support of the warrant established reasonable grounds to believe that the records sought were relevant and material to an ongoing criminal investigation. Accordingly, this Court should find that the acquisition of the records was constitutionally reasonable (if Antonio Gilton could assert a reasonable expectation of privacy in such records) for two independent sufficient reasons.[11]

First, as discussed above, the Supreme Court has held that subpoenas for records do not require a warrant based on probable cause, even when challenged by the party to whom the records belong. *See Miller*, 425 U.S. at 446 (reaffirming the "traditional distinction between a search warrant and a subpoena"); *see also*

[11] The fact that the officers sought a warrant based on a showing of probable cause should not prevent this Court from concluding that, even if probable cause was lacking, no Fourth Amendment violation occurred because the judicial authorization the officers sought and the showing on which it was based were constitutionally reasonable. Because this Court can and should reverse the district court's order because the warrant was supported by probable cause and the officers relied on it in good faith, the Court should refrain from addressing the constitutionality of the Section 2703(d) standard, reserving that issue for a case in which the statute was applied.

Oklahoma Press Pub. Co., 327 U.S. at 209. Rather, as the *Miller* Court explained, the Fourth Amendment, "if applicable to subpoenas for the production of business records and papers, at most guards against" vagueness and overbreadth, so long as the agency is authorized by law to make the inquiry and the materials specified are relevant. 425 U.S. at 445-46. Given that, to the extent that a person who does not own or possess the records and did not create them has any Fourth Amendment interest in them at all, he could not be entitled to greater protection than the party that created and owns the records.

It follows that the SCA standard is constitutionally reasonable, because the SCA provides more substantial privacy protections than an ordinary judicial subpoena. In particular, the SCA "raises the bar" for obtaining historical cell-site records, by requiring the government to establish "specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought[ ] are relevant and material to an ongoing criminal investigation," 18 U.S.C. § 2703(c) and (d) (emphasis added). In contrast, an ordinary subpoena requires only a "court's determination that the investigation is authorized by Congress, is for a purpose Congress can order, and the documents sought are relevant to the inquiry," and that the "specification of the documents to be produced [is] adequate, but not excessive, for the purposes of the relevant inquiry." *Oklahoma Press Pub. Co.*, 327 U.S. at 209. Given that "[a] legislative

body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way," *Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment), Congress's considered effort to augment the privacy protections that this Court has found sufficient for judicial subpoenas complies with the Fourth Amendment.

Second, traditional standards of Fourth Amendment reasonableness independently confirm that a Section 2703(d) court order is a reasonable mechanism for obtaining a cellular-service provider's historical cell-site records. As discussed above, under traditional Fourth Amendment standards, Antonio Gilton had no legitimate expectation of privacy in the third-party business records at issue here. But even if this Court were to depart from that settled framework and hold that an individual can assert a Fourth Amendment interest in records created by a third party that pertain to a transaction he engaged in with the third party, Antonio Gilton could at most assert only a diminished expectation of privacy in those records. That is a factor that this Court has said "may render a warrantless search or seizure reasonable." *King*, 133 S. Ct. at 1969. And any invasion of Antonio Gilton's assumed privacy interest was minimal, given the imprecise nature of the location information that could be inferred from the historical cell-site records at issue here, which could not have enabled law-enforcement officers to

pinpoint Antonio Gilton's location and could not have revealed other personal facts about him.

On the other side of the reasonableness balance, the government has a compelling interest in obtaining historical cell-site records without having to meet the requirement of a warrant and probable cause, because, like other investigative techniques that involve seeking information from third parties about a crime, this evidence is "particularly valuable during the early stages of an investigation, when the police [may] lack probable cause and are confronted with multiple suspects." *See Davis*, 785 F.3d at 518. Society has a strong interest in both promptly apprehending criminals and exonerating innocent suspects as early as possible during an investigation. *See King*, 133 S. Ct. at 1974; *United States v. Salerno*, 481 U.S. 739, 750-51 (1987). In addition, the SCA ensures judicial scrutiny of the government's basis for obtaining an order, so the government may obtain such orders only in circumstances where the asserted governmental interest in acquiring the records has been examined by a neutral magistrate.

Thus, even if the affidavit did not establish probable cause, at a minimum, the warrant met the lesser Section 2703(d) standard, and that was sufficient to satisfy the Fourth Amendment. *See infra* Section II.

II. EVEN IF PROBABLE CAUSE WAS NECESSARY, THE WARRANT ESTABLISHED A REASONABLE NEXUS BETWEEN THE MURDER AND ANTONIO GILTON'S PHONE

This Court need not reach the question whether the Fourth Amendment requires a warrant and probable cause to obtain historical CSLI, because even if it does, the district court erred in concluding that the warrant here did not satisfy that requirement. In so doing, it failed to accord appropriate deference to the judge issuing the warrant, ignored the evidence [redacted], and applied the incorrect standard by asking whether the affidavit provided sufficient information to incriminate Antonio Gilton, as opposed to whether it provided sufficient information to create a reasonable nexus between the murder and the information sought (namely, Antonio Gilton's records from a cell phone provider).

While this Court reviews de novo a district court's denial of a motion to suppress based on alleged defects in a search warrant affidavit, it reviews for clear error the magistrate judge's finding that a search warrant was supported by probable cause and gives great deference to that finding. *United States v. Krupa*, 658 F.3d 1174, 1177 (9th Cir. 2011). If a case is a close call, "preference will be accorded to [a] warrant[ ] and to the decision of the magistrate issuing it." *United States v. Crews*, 502 F.3d 1130, 1135 (9th Cir. 2007). "The task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all

the circumstances set forth in the affidavit before him, . . . 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, 238-39 (1983). And "the duty of the reviewing Court is simply to ensure that the magistrate has a substantial basis for . . . conclud[ing] that probable cause existed." *Id.*

Probable cause exists when there is a "fair probability" that contraband or evidence of a crime will be found in a particular place. *Gates*, 462 U.S. at 236. And a "fair probability" does not mean "certainty or even a preponderance of the evidence." *United States v. Gourde*, 440 F.3d 1065, 1069 (9th Cir. 2006) (en banc). To the contrary, probable cause is a practical, nontechnical concept. *Brinegar v. United States*, 338 U.S. 160, 176 (1949). Accordingly, a warrant application must show "only a reasonable nexus between the activities supporting probable cause and the location to be searched." *United States v. Ocampo*, 937 F.2d 485, 490 (9th Cir. 1991). "A 'reasonable nexus' does not require direct evidence that the items listed as the objects of the search are on the premises to be searched. The magistrate must 'only conclude that it would be reasonable to seek the evidence in the place indicated in the affidavit.'" *United States v. Pitts*, 6 F.3d 1366, 1369 (9th Cir. 1993); *see also United States v. Fernandez*, 388 F.3d 1199, 1254 (9th Cir. 2004); *United States v. Chavez-Miranda*, 306 F.3d 973, 978-79 (9th Cir. 2002). In assessing nexus, a magistrate judge may "draw reasonable

inferences about where evidence is likely to be kept, based on the nature of the evidence and the type of offense." *United States v. Angulo-Lopez*, 791 F.2d 1394, 1399 (9th Cir. 1986).

Here, the district court ignored the information in the affidavit that supported a nexus between Sneed's murder and Antonio Gilton's cell phone. [redacted] ER 428-29. Moreover, Barry Gilton told the police that he had returned to the house at 12:15 a.m. and gone to his bedroom, when in fact cell records showed that his phone was moving around San Francisco neighborhood, between 12:49 a.m. and 2:19 a.m. on the night of the murder – and near his house around the time of the murder. ER 419. [redacted]

[redacted] and the shooter's car arrived at around the same time as Sneed, suggesting that the shooter was tipped off by someone at the house about Sneed's arrival. Antonio Gilton was L.G.'s guardian in Los Angeles and was likely involved in the efforts to extricate her from Sneed. Antonio Gilton could have been involved in that murder in multiple ways. When the state sought the warrant, they did not know where the shooters got the car, or where they got the gun.

Moreover, the affidavit included information supporting the credibility of the informant. *Cf. Navarette v. California*, 134 S. Ct. 1683, 1688-89 (2014) (describing characteristics of an anonymous tip that will support reasonable suspicion). [redacted]

Instead of giving this information its proper weight, the district court appeared to conclude that absent information expressly and specifically incriminating Antonio Gilton, as opposed to members of the Gilton family more broadly, the search warrant was inadequate. That was legal error. *See Zurcher v.*

Stanford Daily, 436 U.S. 547, 556-57 (1978) ("The critical element in a reasonable search is not that the owner of the property is suspected of crime but that there is reasonable cause to believe that the specific 'things' to be searched for and seized are located on the property to which entry is sought."). The appropriate question was whether it would be reasonable to seek evidence related to the murder in those records. *Id.* Simply put, it was.

Based on the affidavit here, there was no doubt but that Sneed was murdered. And there was ample reason to believe that Sneed was targeted by the Gilton family because of his relationship with Antonio Gilton's minor sister, that the shooter did not act alone, and that family members' cell phone records might have useful information about the murder. (Indeed, as the affidavit set forth, Barry Gilton's records from that night established that his claims about his whereabouts at the time of the murder were a lie.) The information in the affidavit supported the conclusion that the murder was a family matter, [redacted][12] [redacted]

[12] Nor is *Grant*, 682 F.3d at 836, to the contrary. There, the police obtained a warrant to search the defendant's home for the purpose of recovering, among other evidence, a gun and ammunition used in a homicide that had occurred nearly nine months earlier, even though there was no evidence that his sons had brought the gun to the house. *Id.* at 828. Here, the information was sought from the cell phone

[redacted]

That was enough to establish both probable cause that a crime had been committed and a reasonable nexus between the murder and Antonio Gilton's phone records and CSLI. The district court's contrary conclusion was error.

III. EVEN IF THE WARRANT DID NOT ESTABLISH PROBABLE CAUSE, THE OFFICERS RELIED ON IT IN GOOD FAITH

Even if the district court did not err in concluding that the warrant was inadequate, it erred in holding that the officers did not act in good faith when they relied on the search warrants issued by a neutral and detached judge. *See United States v. Leon*, 468 U.S. 897, 926 (1984). The "prime purpose" of the exclusionary rule is "to deter future unlawful police conduct and thereby effectuate the guarantee of the Fourth Amendment against unreasonable searches and seizures." *United States v. Calandra*, 414 U.S. 338, 347 (1974); *see Utah v. Strieff*, 136 S. Ct. 2056, 2061 (2016) (noting that "[s]uppression of evidence . . . has always been our last resort, not our first impulse"); *Herring v. United States*, 555 U.S. 135, 140 (2009) (same). Where an "officer is acting as a reasonable officer would and should act in similar circumstances[,] [e]xcluding the evidence can in no way

provider within days of the murder, there was evidence that more than one individual was involved in the murder, that the Giltons were involved as a family in the murder, and that there was some coordination between someone in the family home and the shooter.

affect his future conduct unless it is to make him less willing to do his duty." *Leon*, 468 U.S. at 920.

Accordingly, there is a strong presumption that a law enforcement officer acting pursuant to a warrant is acting in good faith, and "[s]earches pursuant to a warrant will rarely require any deep inquiry into reasonableness." *Leon*, 468 U.S. at 922 (internal quotation omitted). "It is the judicial officer's responsibility to determine whether probable cause exists to issue a warrant, and, in the ordinary case, police officers cannot be expected to question that determination." *Illinois v. Krull*, 480 U.S. 340, 349 (1987).

However, if the affidavit upon which the warrant was based was so lacking in indicia of probable cause that an officer "could not have harbored an objectively reasonable belief in the existence of probable cause," the good faith exception does not apply. *Leon*, 468 U.S. at 923-26; *see also Herring*, 555 U.S. at 145 (the "good-faith inquiry is confined to the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal in light of all of the circumstances"). In other words, if there is no "colorable argument for probable cause," *Leon* does not apply. *United States v. Luong*, 470 F.3d 898, 903 (9th Cir. 2006). *Cf. Strieff*, 136 S. Ct. at 2063 (favoring exclusion "only when the police misconduct is most in need of deterrence – that is, when it is purposeful or flagrant"). *Leon*'s good faith exception does apply, however, if the

affidavit is "sufficient to create disagreement among thoughtful and competent judges as to the existence of probable cause." *Leon*, 468 U.S. at 926.

Here, the affidavit plainly described a murder that grew out of a family crisis and suggested that Antonio, the older brother who lived with L.G. while she developed a relationship with Sneed, a pimp, and began advertising her services on the Internet, would have information that would have been vital to the parents. It therefore would not have been "entirely unreasonable" for the officers to rely on the state judge's assessment that the affidavit established a fair probability that Antonio's call records and location data would provide evidence related to the crime. *Messerschmidt v. Millender*, 132 S. Ct. 1235, 1249 (2012). Put another way, the affidavit presented a "colorable argument" for probable cause. *See United States v. Underwood*, 725 F.3d 1076, 1085 (9th Cir. 2013); *Luong*, 470 F.3d at 903.

In addition, it was reasonable for the officers to assume that if the trial judge found probable cause, at a minimum the facts in the affidavit satisfied the Section 2703(d) standard ("specific and articulable facts showing that there are reasonable grounds to believe that the [records] are relevant and material to an ongoing criminal investigation") for a court order authorizing the collection of phone records. The affidavit establishes reasonable grounds to believe that the whereabouts of everyone in the immediate Gilton family on the night of the

murder, and especially Antonio Gilton, who was L.G.'s guardian in Los Angeles, was "relevant" and "material" to the offense under investigation, as were Antonio Gilton's call records. *See* 18 U.S.C. § 2703(d).

Thus, even if this Court were to hold that the Section 2703(d) standard does not satisfy the Fourth Amendment, police officers could reasonably rely on a court order based on evidence that meets the "reasonable grounds" standard, especially where the officers obtained the court order before any appellate court (or for that matter, any district judge in the Northern District of California) had struck Section 2703(d) as unconstitutional. *See Krull*, 480 U.S. at 349-50 (exclusionary rule did not apply where officers acted in "objectively reasonable reliance on statute," even if statute was "subsequently declared unconstitutional"); *United States v. Dorsey*, 2015 WL 847395, at *8 (C.D. Cal. 2015) (collecting cases applying *Krull* to the collection of historical cell-site information from a phone company).

CONCLUSION

For the reasons stated above, this Court should reverse the district court's order granting Antonio Gilton's motion to suppress.

Dated: August 11, 2016

Respectfully submitted,

BRIAN J. STRETCH
United States Attorney

BARBARA J. VALLIERE
Chief, Appellate Division

/s/ Anne M. Voigts
ANNE M. VOIGTS
Assistant United States Attorney

Attorneys for Plaintiff-Appellant
UNITED STATES OF AMERICA

STATEMENT OF RELATED CASES

Pursuant to Rule 28-2.6(a) of the United States Court of Appeals for the Ninth Circuit, counsel for Appellee aware of another interlocutory appeal from the same district court case, *United States v. Williams, et al.*, CA No. 15-10475, which was argued and submitted on March 16, 2016,

Dated: August 11, 2016

/s/ Anne M. Voigts
ANNE M. VOIGTS
Assistant United States Attorney

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(a)(7)(C) and Circuit Rule 32-1, I certify that, the attached answering brief for the United States is:

_X_ Proportionately spaced, has a typeface of 14 points or more and contains 13,420 words or less; or,

__ Monospaced, has 10.5 or fewer characters per inch, and contains words or _____ lines of text

Dated: August 11, 2016

/s/ Anne M. Voigts
ANNE M. VOIGTS
Assistant United States Attorney

CERTIFICATE OF SERVICE

I, Hui Chen, certify that I am an employee of the Office of the United States Attorney, Northern District of California, a person over 18 years of age and not a party to the within action. I certify that on August 11, 2016, I electronically submitted the

- **United States' Redacted Opening Brief**
- **Volumes I and II of the Excerpts of Record**

in the consolidated cases of *United States v. Alfonzo Williams, et al.*, No. 16-10109, with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system. All participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system for the above documents.

I further certify that I served **Volume III of the Excerpts of Record (Under Seal)** and **Motion to File Documents Under Seal and Documents Ex Parte, Under Seal** to all other parties in the case via USPS certified mail service.

Dated: August 11, 2016

/s/ Hui Chen
Hui Chen, Paralegal