MELINDA HAAG (CABN 132612)
United States Attorney

DAVID R. CALLAWAY (CABN 121782)
Chief, Criminal Division

J. DOUGLAS WILSON (DCBN 412811)
JEFFREY SCHENK (CABN 234355)
Assistant United States Attorneys

150 Almaden Boulevard, Suite 900
San Jose, California 95113
Telephone: (408) 535-5061
FAX: (408) 535-5066
Jeffrey.b.schenk@usdoj.gov

Attorneys for United States of America

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

IN RE: APPLICATION FOR TELEPHONE INFORMATION NEEDED FOR A CRIMINAL INVESTIGATION	No. CR 15-90304 MISC LHK APPEAL OF DENIAL OF APPLICATION FOR TELEPHONE INFORMATION NEEDED FOR A CRIMINAL INVESTIGATION

TABLE OF CONTENTS

TABLE OF AUTHORITIES

FEDERAL CASES

FEDERAL STATUTES

The government submitted, under seal, an application for an order under 18 U.S.C. §§ 3122 and 3123 and 18 U.S.C. § 2703(d) seeking, among other things, cell site information for several particular individuals. On April 9, 2015, Magistrate Judge Howard R. Lloyd denied the application in an order that found that "in order to get cell site information, prospective or historical, the government must obtain a search warrant under Rule 41 on a showing of probable cause." The government appeals Judge Lloyd's Order to this Court to the extent Judge Lloyd denied the government historical cell site information.

A. Background

1. Cell Site Information and Orders under Section 2703(d)

Cell site information consists of records of a provider of cell phone service as to the cell tower and segment a particular cell phone used when making a particular call at a specific time. Because the cell phone tower used by a cell phone is usually the closest tower to the cell phone, cell site information ordinarily gives an approximate location for a cell phone if the cell phone is in use. Cell site information does not provide a precise location for the cell phone at issue. As a general matter, cell phone providers compile cell site information for the beginning and end of a call, and, accordingly, if a cell phone relies on several cell towers during the course of a call, cell site information may not capture approximate location information for the cell phone throughout the call. Cell phone providers maintain cell site information for their own purposes, including billing and advertising, and not because the government mandates the compilation of such information; no federal law requires a company to create or keep cell site records. Cell site information can either be historical or prospective. Historical cell site information seeks records of calls that have already occurred; prospective cell site information seeks information about calls as they occur. Cell site information does not include the content of any communication.

Under 18 U.S.C. § 2703(c)(1), the United States may require a provider of electronic communication service to disclose "a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications)" when it obtains a § 2703(d) order. Under § 2703(d), a court may issue an order for "a record or other information pertaining to a subscriber to or customer" of "a provider of electronic communication service or remote computing company" if the government provides to the court "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."

For many years, the government in this District has submitted applications under § 2703(d), usually in combination with a request under § 3122 for a pen register/trap and trace authority, to obtain cell site information. Sometimes the applications seek only historical cell site information, and sometimes they seek both historical and prospective cell site information. The application in this case sought both historical and prospective cell site information.

Until Judge Lloyd declined to sign a request under § 2703(d), magistrate judges in this district have signed § 2703(d) orders authorizing a cell phone company to provide historical cell site information without requiring the government to show probable cause. In an order issued in *United States v. Cooper*, No. CR 13-00693 SI, however, Judge Illston found that a cell phone user has a right of privacy in historical cell site information, and that Congress could not have intended § 2703 to be used to gather that information absent a showing of probable cause. This Court has found Judge Illston's order "persuasive." *See United States v. Hitesman*, No. CR 14-00010 (Hearing on March 25, 2010).

2. Magistrate Judge Lloyd's Order

The government submitted to Judge Lloyd an application for a "hybrid" order. Under that order, the government seeks both pen register/trap and trace information under 18 U.S.C. §§ 3122 and 3123, and cell site information under 18 U.S.C. § 2703(d). As noted, the order sought both historical and prospective cell site information. The application sought historical cell site data for 60 days prior to the signing of the order, and prospective cell site date for 60 days from the signing of the order.

Judge Lloyd expressed skepticism that Section 2703(d) allowed the government to obtain prospective cell site information, but the court did not rest its argument on that ground. Instead, the court observed that "cell site location information implicates a person's constitutional right to privacy." Order at 4. Although Judge Lloyd noted that "[t]he interplay between the bounds of a person's expectation of privacy as it relates to his/her physical location and the government's ability to obtain cell phone-related information without a search warrant is not settled," Order at 4, he concluded that cell site information was sufficiently similar to information from a tracking device that it required a search warrant supported by probable cause. Order at 4-5. Judge Lloyd noted that he found Judge Illston's

analysis in *Cooper* "very persuasive." Order at 5.

B. Cell site orders under § 2703(d) do not violate the Fourth Amendment.

Judge Lloyd erred because a person has no right to privacy in historical cell site information.[1] That information is supplied to cell phone providers, which maintain it as a business record. Accordingly, the government may obtain cell site information using an order under § 2703(d).

The Fifth Circuit has directly held that the Fourth Amendment does not require the government to show probable cause before obtaining historical cell site information from a cell phone provider, because the cell phone user has no expectation of privacy in information that is conveyed when a call is made or received and kept by the cell phone provider for business reasons. *In re Application of U.S. for Historical Cell Site Data*, 724 F.3d 600, 608-15 (5th Cir. 2013) (*In re Application*). Instead, an order under § 2703(d) is sufficient. In addition, because a historical cell site record is a business record generated and stored by a cell phone company at the company's own discretion, it does not implicate the Fourth Amendment and instead is subject to only the reasonableness requirements applicable to compulsory process. No circuit court of appeals has held to the contrary, and the most recent court of appeals decision to address the issue, *United States v. Davis*, 754 F.3d 1205 (11th Cir. 2014), has been vacated and reheard by the court of appeals en banc. *See United States v. Davis*, 573 F. App'x. 925 (11th Cir. 2014). Davis is pending en banc review.

1. A cell phone customer has no reasonable expectation of privacy in cell site records

In *United States v. Miller*, 425 U.S. 443 (1976), the Supreme Court rejected a Fourth Amendment challenge to a third-party subpoena for bank records, explaining that the bank's records are business records of the bank, not private papers of the customer, and that the customer "can assert neither ownership nor possession" in the records. *Miller*, 425 U.S. at 440. In rejecting the challenge to

[1] The government submits that a person also has no right to privacy in prospective cell site information. In both cases, the government is simply asking the cell phone company to provide information that the cell phone user provides to the cell phone company and that the cell phone company gathers as a business record. Moreover, the government submits that Judge Lloyd is incorrect in stating that § 2703 applies only "to stored electronic information." Sections 2703(c) and 2703(d) make no reference to "stored" information and broadly apply to any "record or other information pertaining to a subscriber." As noted, however, the government is not appealing Judge Lloyd's order to the extent it denied the government prospective cell site information.

the subpoena, the Court held that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Governmental authorities, even if the information is revealed on the assumption that it will be used for a limited purpose and the confidence placed in the third party will not be betrayed." *Id*. at 443.

The reasoning of *Miller* applies to historical cell site records. First, historical cell site records are not a customer's private papers. Once a customer places a call, the customer has no control over cell site records relating to the customer's phone. Moreover, the customer knows that the call is going through one or more cell towers owned by a third party. Second, cell site records are business records of the provider. The choice to create and store cell site records is made by the provider, and the provider controls the format, content, and duration of the records it chooses to create and retain. By contrast, customers ordinarily do not create or retain records of cell phone calls. Third, cell site records pertain to transactions to which the cell phone provider was a party. It is not possible to make a call without a cell phone tower, and the cell phone company assigns the cell tower or towers to each call to facilitate the functioning of its network.

Smith v. Maryland, 442 U.S. 735 (1979), confirms the conclusion that cell phone users have no expectation of privacy in cell site records. In *Smith*, the telephone company installed a pen register at the request of the police to record numbers dialed from defendant's telephone. The Supreme Court held that telephone users had no expectation of privacy in dialed telephone numbers and that any such expectation of privacy is not one that society is prepared to recognize as reasonable. *Id*. at 742-44. The Court found that telephone users did not have an expectation of privacy even though the caller did not necessarily know what happened to a call after it was dialed. Similarly, cell phone users usually understand that they must send a signal and that it is received by a cell company's cell tower when the company routs the call to its intended recipient, but they may not know that the cell phone provider uses cell towers and compiles information about the calls made and received. Accordingly, like the dialer of a telephone in *Smith*, a cell phone user voluntarily transmits a signal to a cell tower.

In *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008), the Ninth Circuit applied this reasoning to the to/from addresses of e-mail messages and the IP addresses of websites visited. Relying on *Smith*, the court held that indivuals have no expectation of privacy in either e-mail to/from addresses

or the IP addresses of visited websites 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." *Id.*; *see also United States v. Velasquez*, 2010 WL 4286276, at *5 (N.D. Cal. Oct. 22, 2010) (denying motion to suppress historical cell site data). The Supreme Court has never overruled *Miller* and *Smith*, and the Ninth Circuit has never overruled *Forrester*, and they remain governing law.

Moreover, *Smith* evaluated the information voluntarily disclosed to the phone company from the standpoint of a knowledgeable telephone user. The Court reasoned that based on a telephone book statement that the phone company could help identify "the origin of unwelcome or troublesome calls," customers "typically know" many of the facts revealed by use of pen registers. *Smith*, 442 U.S. at 742-43. Today, cell phone companies provide far more explicit notice to customers that they collect customers' location information. All of the major cell phone companies inform cell phone customers that the cell phone company will collect location information from customers and provide it to law enforcement to comply with court orders. For example, the AT&T privacy policy informs customers, both in the policy and in frequently asked questions about the policy, that AT&T will collect location information about "where your wireless device is located." http://www.att.com/Common/about_us/privacy_policy/print.html; *see* http://www.att.com/gen/privacy-policy?pid+13692#menu (stating in frequently asked questions about its privacy policy that AT&T collects "the whereabouts of your wireless device"); *see also* http://www.t-mobile.com//company/website/privacypolicy.aspx (noting that T-Mobile may collect location information and share it with law enforcement in response to legal process). Under the reasoning of *Smith*, customers voluntarily disclose cell site records in light of these policies.

As the Fifth Circuit held, when an individual shares information with a third party, "'[h]e cannot expect that these activities are a private affair.'" *In re Application*, 724 F.3d at 610 (quoting *Reporters Comm. for Freedom of the Press v. Am. Tel. & Tel. Co.*, 593 F.2d 1030, 1043 (D.C. Cir. 1978)). Nor does a customer have a right to control the information after it is conveyed to the cell phone company; instead, that information becomes a record of the cell phone company. *Id.* at 611. Here, because customers know, or are on notice, that cell phone companies must obtain their location information to connect cell phone calls, they voluntarily convey location information to cell phone companies. *See In*

re Application, 724 F.3d at 614.

2. Cell site records constitute business records subject to compulsory process

A second reason that Judge Lloyd erred is that a historical cell site record "is clearly a business record" of the cell phone provider. *In re Application*, 724 F.3d at 612. As the Fifth Circuit explained, "[t]he cell service provider collects and stores historical cell site data for its own business purposes, perhaps to monitor or optimize service on its network or to accurately bill its customers for the segments of its network that they use." *Id*. at 611-12; *see United States v. Jones*, 132 S. Ct. at 961 (Alito J., concurring) (government has not "required or persuaded" providers to keep historical cell site records). In short, "these are the providers' own records of transactions to which it is a party." *In re Application*, 724 F.3d at 612; *see also United States v. Golden Valley Elec. Ass'n*, 689 F.3d 1108, 1116 (9th Cir. 2012) (upholding subpoena for power company records and stating 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'").

Business records ordinarily may be obtained by a subpoena. In fact, the Supreme Court has never held that the government must obtain a warrant to obtain information from a third party holding it as a business record. Like a subpoena, a § 2703(d) order compels the recipient to produce specific information; the recipient may move to quash, and the order remains at all times under the supervision of the issuing court. Therefore, a § 2703(d) order is, like a subpoena, a form of compulsory process.

The Fourth Amendment sets a reasonableness standard for compulsory process; it requires probable cause only for a warrant. As the Supreme Court has held, the Fourth Amendment, "if applicable [to a subpoena], at the most guards against abuse only by way of too much indefiniteness or breadth in the things required to be 'particularly described.'…The gist of the protection is the requirement, expressed in terms, that the disclosure shall not be unreasonable." *Oklahoma Press Publishing Co. v. Walling*, 327 U.S. 186, 208 (1946); *see Golden Valley Elec. Ass'n*, 689 F.3d at 1115-16. Because subpoenas are subject only to a reasonableness requirement, the Eleventh Circuit panel erred in imposing a probable cause requirement for compelled disclosure of historical cell site records.

Finally, the government's ability to subpoena business records collected by a business at its own discretion is not limited to records "voluntarily disclosed" to the business. The subpoena power is

grounded in the long-standing principle that the government has the right to every witness's non-privileged testimony. *See Branzburg v. Hayes*, 408 U.S. 665, 688 (1972). When a company acting on its own discretion chooses to store business records that later prove relevant to a criminal investigation, it essentially functions as a witness, and no warrant is required to obtain information from a witness.

It is true that in *Miller* and *Smith*, the Supreme Court considered whether the information obtained by the government was voluntarily disclosed to the businesses, but both of those cases involved information collected or maintained at the behest of the government. In *Miller*, the government issued subpoenas for records that a third-party bank was required to keep pursuant to federal law. *See* 425 U.S. at 436, 441. Similarly, the phone company in *Smith* installed a pen register "at police request," and the resulting records generated information about local calls that would not ordinarily have been preserved under then-prevailing billing practices. *See* 442 U.S. at 745. In other business records cases in which the records were collected at the business's discretion, the Supreme Court has not considered whether the information was voluntarily disclosed. *See, e.g.*, *SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 744 n.11 (1984) (noting that "any Fourth Amendment claims that might be asserted by respondents are 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"); *Donaldson v. United States*, 400 U.S. 517, 522-23 (1971) (holding that taxpayer was not entitled to intervene in proceeding to enforce summons for his employment records and stating "what is sought here by the Internal Revenue Service . . . is the production of Acme's records and not the records of the taxpayer"). Because cell site records are collected and stored at the discretion of the cell phone company, their compelled disclosure is analyzed for Fourth Amendment purposes pursuant to the reasonableness standard applicable to subpoenas.

3. The concurrence in Jones does not bar issuance of a cell site order

In *United States v. Jones*, 132 S. Ct. 945 (2012), the Court held that the placement of a GPS tracking device on an automobile violated the Fourth Amendment because it constituted a trespass on the vehicle owner's effects. Justice Alito, joined by three other Justices, concurred in the judgment, but argued that the month-long monitoring of the defendant's location violated the Fourth Amendment because it constituted an improper invasion of privacy. *Jones*, 132 S. Ct. 957-64 (Alito, J., concurring).

Justice Alito's concurrence addresses monitoring by the government, however; nothing in it limits the scope of information the United States may obtain from a witness. In fact, the majority of courts that have ruled after *Jones* have likewise found that a cell phone user has no expectation of privacy in the cell phone's location. *See United States v. Dorsey*, 2015 WL 847395, at *7 (C.D. Cal. Feb. 23, 2015); *United States v. Moreno–Nevarez*, 2013 WL 5631017, at *2 (S.D. Cal. Oct. 2, 2013); *United States v. Salas*, 2013 WL 4459858, at *3 (E.D. Cal. Aug. 16, 2013); *In re Smartphone Geolocation Data Application*, 2013 WL 5583711, at *14 (E.D.N.Y. May 1, 2013); *United States v. Rigmaiden*, 2013 WL 1932800, at *8 (D. Ariz. May 8, 2013); *United States v. Ruby*, 2013 WL 544888, at *6 (S.D. Cal. Feb. 12, 2013); *United States v. Graham*, 846 F. Supp. 2d 384, 387 (D. Md. 2012); *In re Application of U.S.*, 849 F. Supp. 2d 177, 177-79 (D. Mass. 2012). But see *In re U.S. Application for the Release of Historical Cell-Site Information*, 809 F. Supp. 2d 113 (E.D.N.Y. 2011) (pre-Jones decision holding that a warrant is required to compel disclosure of historical cell site records).

Moreover, the majority held that the installation of the GPS was a trespass; it did not endorse Justice Alito's view that an improper invasion of privacy occurred. In any event, Justice Alito's concurring opinion actually supports the lawfulness of obtaining historical cell site records with a § 2703(d) order. The Alito concurrence favors deference to Congress in resolving privacy issues involving modern technology: "In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative.…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); *see also United States v. Watson*, 423 U.S. 411, 416 (1976) (recognizing "a strong presumption of constitutionality" to federal statutes challenged on Fourth Amendment grounds). In the Stored Communications Act, including § 2703(d), Congress has enacted legislation controlling government access to historical records of cell-phone providers. When the government seeks historical cell site records using a § 2703(d) order, it complies with this statute.

4. The Supreme Court's decision in Riley does not affect cell site information.

In *Riley v. California*, 134 S. Ct. 2473 (2014), the Supreme Court held that a warrant is ordinarily necessary before police officers search a cell phone incident to the cell phone user's arrest for the content on that cell phone. The Court made clear, however, that its decision did not address whether

a search subject to probable cause had occurred. To the contrary, the Court cited *Smith* and noted that it did not involve a search under the Fourth Amendment, and it did not suggest that *Smith* or *Miller* was no longer valid. Nor did the Court suggest that a cell phone provider's supplying of historical cell site information constitutes a search requiring a showing of probable cause. Accordingly, the Court's decision has no bearing on this case.

* * *

The government appeals Judge Lloyd's order only to the extent that it denied the government historical cell site information. Accordingly, the Court should remand to Judge Lloyd with instructions to issue an order allowing the government to obtain historical cell site information from the company that maintains the target's cell phone records.

DATED: April 29, 2015

Respectfully submitted,

MELINDA HAAG
United States Attorney

/s/
J. DOUGLAS WILSON
JEFFREY SCHENK
Assistant United States Attorneys