MELINDA HAAG (CABN 132612)
United States Attorney

J. DOUGLAS WILSON (DCBN 412811)
Assistant United States Attorney
Chief, Criminal Division

DAMALI A. TAYLOR (CABN 262489)
Assistant United States Attorney

450 Golden Gate Avenue, Box 36055
San Francisco, California 94102-3495
Telephone: (415) 436-6401
FAX: (415) 436-7200
Damali.taylor@usdoj.gov

Attorneys for United States of America

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

IN RE TELEPHONE INFORMATION NEED FOR A CRIMINAL INVESTIGATION	NO. CR 14-xr-90532 NC UNITED STATES' REPLY MEMORANDUM

TABLE OF CONTENTS

TABLE OF AUTHORITIES

FEDERAL CASES

STATE CASES

U.S. CONSTITUTION AND FEDERAL STATUTES

MISCELLANEOUS

In *United States v. Miller*, 425 U.S. 435, 443 (1976), the Supreme Court held 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." Based on this principle, the Court held in *Smith v. Maryland*, 442 U.S. 735, 745 (1979), that a person has no reasonable expectation of privacy in dialed telephone numbers. The Supreme Court has never overruled those cases, and they remain governing law. Because a person voluntarily using a cell phone conveys the cell phone's approximate location to the cell phone service provider and the records created are business records of the provider, *Smith* and *Miller* make clear that a person has no reasonable expectation of privacy in the cell site records stored by a service provider. Probable cause is not required to obtain that information.

The Federal Public Defender (FPD) counters that *Smith* and *Miller* are inapplicable to historical cell site information for two reasons. First, the FPD asserts (at FPD Br. 13) that *Smith* and *Miller* do not apply "to an era where people routinely and unthinkingly disclose the most intimate details of their lives to their cell phone providers." But the rule of *Smith* and *Miller* was crafted in an era where people exposed the intimate details of their lives to banks and phone companies, and the privacy interest in the bank records at issue in *Miller* surpasses that of historical cell site records; yet, bank records are not protected from compulsory process by the Fourth Amendment. In addition, the information at issue in this case is not, as the FPD repeatedly asserts, the information contained in a cell phone; instead, it is the general location information that cell phone users voluntarily transmit to a cell phone provider through a cell tower when the cell phone user makes a call. It is not true that, as the FPD asserts (FPD Br. 17), historical cell site information "is more analogous to content of a communication than to an address." *See Smith*, 442 U.S. at 743 (noting that the numbers dialed do not constitute the contents of the call).

Second, the FPD claims (at FPD Br. 16), historical cell site information "is not knowingly and intentionally conveyed by the consumer to anyone but rather generated automatically by radio waves." *See also* American Civil Liberties Union (ACLU) Br. at 8-10 (arguing that cell phone users have an expectation of privacy because they do not voluntarily convey location information to cell phone companies). This statement relies on a misreading of *Smith*. In *Smith*, (as the FPD expresses its holding, Br. 15), the Court held "that there was no privacy interest in dialed numbers because the person using

the telephone intentionally conveyed the number to the telephone company for the express purpose of having the carrier connect him to that number." Historical cell site information does not differ in any constitutional sense from the telephone numbers gathered in *Smith* because the information used to construct historical cell site information comes from the signals conveyed to the cell phone provider to complete a telephone call. Moreover, contrary to the FPD's assertion, a cell phone user knowingly conveys the signal used to complete a cell phone call to the provider. Even the least sophisticated cell phone user knows that his or her cell phone has to send a signal to a cell phone tower to make a call. In fact, cell phone users often talk of being in or out of service range for their cell phones, by which they can only mean that their phone can or cannot send a signal to the cell phone provider. Nor does the FPD make any effort to explain (or even acknowledge) the policies from AT&T and T-Mobile that make it clear to users that those providers will gather location information conveyed by cell phones.[1] Finally, because the cell phone records are kept by the provider, the cell phone user cannot have an expectation of privacy in them. *See In re Grand Jury Proceeding*, 842 F.3d 1229, 1234 (11th Cir. 1988) ("an individual has no claim under the fourth amendment to resist the production of business records held by a third party").

In short, historical cell site information is drawn from signaling information that a cell phone user voluntarily conveys to a cell phone provider. Because that information is voluntarily conveyed to the provider and because it simply allows the cell phone provider (and the government with a proper order) to obtain information concerning the general location of the cell phone, *Smith* and *Miller* apply. Accordingly, a person has no reasonable expectation of privacy in historical cell site information. For that reason, on August 1, 2014, the United States filed a petition for rehearing en banc in *United States v. Davis*, 754 F.3d 1205 (11th Cir. 2014), the decision recently finding that the government must obtain a warrant based on probable cause before seeking historical cell site information.

//

//

[1] The FPD also fails to acknowledge Judge Alsup's decision in *United States v. Velasquez*, No. CR 08-0730 WHA. 2010 WL 4286276 (N.D. Cal. Oct. 22, 2010), denying a motion to suppress historical cell site data.

I. There is no reasonable expectation of privacy in information conveyed by a cell phone.

To reiterate, the Supreme Court has squarely held that individuals have no expectation of privacy in information that they voluntarily share with third parties, and that principle forecloses any claim that individuals have a reasonable expectation of privacy in historical cell site information. The FPD argues (FPD Br. 7), however, that historical cell site information creates a reasonable expectation of privacy because it allows the government to "track individuals" and "provides the government with a comprehensive, intimate portrait of an individual's life." In addition, according to the FPD (at FPD Br. 7), the government can use historical cell site information "to track people inside buildings." For those reasons, the FPD concludes, individuals have a reasonable expectation of privacy in historical cell site information, and that information is protected by the Fourth Amendment.

Notably, the FPD does not cite any case in which the government used historical cell site information to "track individuals," obtain a "comprehensive, intimate portrait of an individual's life," or place an individual inside a home or other place in which the person has an expectation of privacy. Nor is the government aware of any such case. That is because, as the government explained in its opening letter brief to the Court, historical cell site information allows the government to obtain only historical and approximate location information. In particular, historical cell site information tells the provider and the government only where a cell phone is at the beginning and end of a call and in relation to the cell tower and (in some cases) 120-degree segment of the tower that the cell phone is using. In this District, the government uses historical cell site information to show that a person was near criminal activity (such as a drug deal or a bank robbery) when it occurred. The government is not aware of any other use to which historical cell site data has been put.

Contrary to the suggestion of the FPD, in this case, the government is not seeking to obtain real-time cell site information that would allow the government to obtain cell site information within a few seconds after the cell phone provider obtained it. Moreover, because the location information obtained is approximate and registers only at the beginning and end of a call, it does not reveal "intimate" details of a person's life. In other words, the government cannot discern from historical cell site information whether a person went to a mental health counselor or a doctor because the government is not using that information to track a person and instead can learn only the approximate location of the cell phone when

a call is being made or received.[2]

The FPD and its amicus Electronic Frontier Foundation (EFF) rely (FPD Br. 10-12; EFF Br. 6) on the Supreme Court's recent decision in *Riley v. California*, 134 S. Ct. 2473 (2014), for the proposition that "individuals have a reasonable expectation of privacy in cell phone location data." As set forth in the government's opening letter brief, however, *Riley* has no bearing on this case. In *Riley*, the question was whether the government must have probable cause and a warrant to search the *contents* of a cell phone, not historical cell site information. Although it may be true that, as the FPD argues, "*Riley*'s focus on the wealth of information revealed by an individual's cell phone . . . applies beyond the limited context of searches incident to arrest," nothing in *Riley* suggests that the Court's concern with a cell phone's contents has any bearing on historical cell site information or any other business record held by a third party. In fact, the examples cited from *Riley* by the FPD all involve information that can be obtained only by looking at the content of information contained in a cell phone. *See* FPD Br. at 11 (noting that *Riley* cited to or discussed "[d]ata on a cell phone" and photographs on a cell phone).

Riley's discussion of *Smith* confirms that *Riley* did not expand the scope of what constitutes a Fourth Amendment search. The government in *Riley* argued that its authority to search phones incident to arrest should at least extend to a phone's call log, given the diminished expectation of privacy in such information under *Smith*. The Court distinguished *Smith*, explaining that *Smith* "concluded that the use of a pen register was not a 'search' at all under the Fourth Amendment. . . . There is no dispute here that the officers engaged in a search of [the defendant's] cell phone." *Riley*, 134 S. Ct. at 2492-93. Critically, the Court did not limit *Smith*; instead, it distinguished inspecting an arrestee's cell phone, which is a search, from obtaining information from the phone company, which under *Smith* is not.

Amicus ACLU adopts the view expressed by the majority in *United States v. Davis*, 754 F.3d 1205 (11th Cir. 2014), that a cell phone user does not voluntarily share his or her location information with the cell phone provider. *See* ACLU Br. 8-10. In particular, the ACLU argues that the privacy

[2] The FPD claims (Br. 3) that "there are 71 towers and 781 separate antennas" within one mile of the federal courthouse in San Francisco. The FPD's brief does not identify the significance of an antenna, as opposed to a tower. Moreover, according to the website cited by the FPD, those 71 towers have been erected by approximately 15 different companies.

policies adopted by the cell phone providers do not destroy a cell phone user's expectation of privacy because most cell phone users do not read the policies. As in many cases, however, publication is sufficient to put people on notice of the contents. For example, airline websites require a user to agree to certain terms and conditions before buying a ticket. Although few people read that small print, the terms and conditions are binding on a ticket buyer. Similarly, before obtaining a credit card, a person has to agree to pages of terms and conditions (on missed payments, interest rates, and arbitration, for example), and the credit card user cannot generally complain if those terms are enforced later. In *Smith* itself, the Court referred to the fact that telephone companies identify the uses to which phone numbers could be put in telephone books, which, even 35 years ago, few people read. To paraphrase the Court in *Smith*, even if the average user is not aware of all the uses to which cell phone signals may be put, he or she is aware that the cell phone is transmitting a signal to the provider. *See Smith*, 442 U.S. at 742-43. Finally, even assuming that a cell phone user is not subjectively aware that cell phone providers stored historical cell site data, that ignorance is not objectively reasonable; that is, it does not create an expectation of privacy that society is prepared to recognize. *See id.* at 743-44.

Nor is the ACLU correct that the cell phone providers' privacy policies fail to inform consumers that location information can be collected. *See* ACLU Br. at 11-13. As set forth in the government's opening letter brief, the AT&T policy specifically informs users that it will collect information on "where your wireless device is located." Similarly, the T-Mobile policy states that the provider will collect location information. That information is sufficient to put a user on notice that the use of the cell phone will result in the generation of records by the cell phone provider.

The FPD also relies (Br. 6-8) on the concurring opinions in *United States v. Jones*, 132 S. Ct. 945 (2012), to argue that "prolonged, electronic location monitoring by the government impinges upon a legitimate expectation of privacy." There are three short answers to this claim. First, *Jones* involved government surveillance; it did not purport to limit the government's ability to obtain information from a third party who had collected information at its own discretion. Second, as made clear above, historical cell site location information is not "prolonged, electronic location monitoring by the government." Instead, to reiterate, it provides only approximate information about the location of a cell phone when the cell phone makes or receives a call. Third, the concurring opinions in *Jones* do not

constitute the opinion of the Court. A majority of the Court found that the physical trespass needed to install a GPS tracker on a vehicle intruded on the vehicle owner's legitimate expectation of privacy. Justice Sotomayor joined that opinion, but also wrote a concurring opinion to suggest that the Court should reconsider *Smith* and *Miller*; she did not join Justice Alito's concurring opinion arguing that placement of the GPS tracker for 30 days violated the vehicle owner's expectation of privacy under a traditional Fourth Amendment analysis. Put another way, Justice Sotomayor's argument that the Court should reconsider *Smith* and *Miller* shows that they continue to require the conclusion that a person has no expectation of privacy in voluntarily produced information. Finally, it is worth noting that Justice Alito, joined by three other Justices, encouraged the kind of legislative solution that Congress has advanced in the Stored Communications Act. *See Jones*, 132 S. Ct. at 964 (Alito, J., concurring).

Finally, the FPD argues (FPD Br. 13) that *Smith* and *Miller* are "inapplicable to an era where people routinely and unthinkingly disclose the most intimate details of their lives to their cell phone providers" and urges this Court to re-evaluate "the question of 'privacy' in the context of the Fourth Amendment." In support of that claim, the FPD and its amici stress that cell phones have become nearly ubiquitous. *See* FPD Br. 1-4; EFF Br. 1-6; ACLU Br. 1. As already stated, however, the Supreme Court has never overruled *Smith* or *Miller*, and neither this Court nor the Eleventh Circuit is free to disregard those cases. Nor were banks and telephone companies minor institutions in the 1970s. Accordingly, this Court may only find that the government is not entitled to historical cell site information if it concludes that cell phone users do not voluntarily convey that information to the cell phone provider. As set forth in the government's opening letter brief and above, this Court should reject that claim.[3]

II. Historical cell site information constitutes a business record of the provider.

As the Fifth Circuit held in *In re Application of U.S. for Historical Cell Site Data*, 724 F.3d 600, 612 (5th Cir. 2013), and the government argued in its opening letter brief, a historical cell site record is "clearly a business record." Instead of quarreling with this finding, the FPD argues that it is irrelevant

[3] Amicus EFF argues (EFF Br. 7-8) that this Court should recognize an expectation of privacy in historical cell site information and "reexamine the entire premise" of *Smith* because the California Supreme Court held in 1979 that state law enforcement officers had to show probable cause to obtain a pen register. *See People v. Blair*, 25 Cal. 3d 640 (Cal. 1979). The EFF does not explain how a 1979 California Supreme Court decision could trump the United States Supreme Court and give this Court the ability to reexamine the premise of *Smith*.

because cell phone users have a reasonable expectation of privacy in cell phone records. As set forth above, however, that premise is inaccurate. Moreover, as the Supreme Court has made clear, a person has no expectation of privacy in business records created and held by a third party. In *Donaldson v. United States*, 400 U.S. 517 (1971), the Court held that a taxpayer could not intervene in the enforcement of IRS summonses to his former employer for his employment records. The Court explained that the material sought "consists only of [the employer's] routine business records in which [Donaldson] has no proprietary interest of any kind." *Id*. at 530. The FPD's argument disregards *Donaldson*, and acceptance of its argument would represent an expansion of an individual's right to privacy into records that the individual has not created.

Because historical cell site records are business records created and stored at the discretion of the provider, the government could use a § 2703(d) order to compel their disclosure even if the FPD were correct that location information is not voluntarily conveyed to the telephone company. In *Miller*, the Supreme Court addressed whether bank records were voluntarily disclosed only because the bank was required by the Bank Secrecy Act to keep the targeted records. *See Miller*, 425 U.S. at 441-42. Prior to the Bank Secrecy Act, the Court upheld a subpoena for bank records in a short *per curiam* opinion without addressing voluntariness. *See First National Bank of Mobile v. United States*, 267 U.S. 576 (1925). An inquiry into voluntariness is called for only when the government has imposed upon the business a mandatory records retention requirement or is acting as a government agent in collecting and disclosing information prospectively, as in *Smith v. Maryland*. For example, the Supreme Court did not address voluntariness in *SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735 (1984), which held that the target of an investigation had no right to notice of subpoenas issued to third parties. *See id.* at 743 n.11 ("It should be noted 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.").

The FPD also claims that the government mandates that cell phone providers keep historical cell site information by the Communications Assistance for Law Enforcement Act, Pub. L. 103-414, 108 Stat. 4279 (1994) (CALEA). In fact, CALEA requires only that providers must be capable of implementing specific court orders, such as a Title III order. Nothing in CALEA requires providers to

collect and store cell site records absent a specific court order pertaining to the specific phone. *See United States v. Graham*, 846 F. Supp. 2d 384, 398 (D. Md. 2012) ("Federal law does not mandate that cellular providers create or maintain" historical cell site records). Nor is the FPD correct in asserting (FPD Br. 19) that CALEA's requirement in 47 U.S.C. § 1002(a) that "all cell phone service providers [must] build into their networks equipment capable of 'expeditiously isolating and enabling the government . . . to access call-identifying information" requires cell phone providers to maintain historical cell site information. Again, that section does not require providers to store historic cell site information.[4]

III. This Court has the authority under the Stored Communications Act to issue an order requiring a cell phone provider to furnish historical cell site information.

Addressing an issue on which the Court did not seek briefing, the FPD appears to argue (Br. 21-25) that a court lacks authority under the Stored Communications Act to issue an order for historical cell site information. But a closer reading of that portion of the FPD's brief suggests that it actually asserts that the Stored Communications Act *should not* encompass orders directing the production of historical cell site information. In particular, the FPD argues that Congress did not consider historical cell site information either when it enacted the Stored Communications Act in 1986 or amended it in 1994, that cell site networks have experienced "explosive growth" over the last 28 years, and that law enforcement agencies "have taken advantage" of the availability of cell site information. Based on these assertions, the FPD concludes that the Court should engage in "at least a reassessment of the interests at stake in allowing the government to obtain [historical cell site information] without a warrant." FPD Br. 25.

As an initial matter, FPD is wrong regarding the legislative history. Congress was specifically concerned with location information when it enacted CALEA. In testifying in support of CALEA, FBI Direct Louis Freeh testified that "[s]ome cellular carriers do acquire information relating to the general

[4] The case on which the FPD relies for the conclusion that the "call-identifying information" that CALEA requires a cell phone provider to keep includes historical cell site information, *U.S. Telecomm. Assn. v. FCC*, 227 F.3d 450, 453 (D.C. Cir. 2000), does not contain the proposition for which it is cited. To the contrary, "even courts that have concluded that government acquisition of cumulative cell site location records can violate the Fourth Amendment generally acknowledge that these records are generated in the ordinary course of the provider's business." *United States v. Graham*, 846 F. Supp. 2d at 398.

location of a cellular telephone. . . . Even when such generalized location information, or any other type of 'transactional' information is obtained from communications service providers, court orders or subpoenas are required and obtained." Statement of Louis J. Freeh, Director, FBI, Before the Senate Judiciary Subcomm. on Tech. and the Law and the House Subcomm. on Civil and Constitutional Rights, 103rd Cong. (March 18, 1994), *available at* 1994 WL 223962. Subsequently, in enacting CALEA, Congress enhanced privacy protections for location information in two ways. First, it limited providers from disclosing location information "solely pursuant" to a pen/trap order. *See* CALEA § 103; 47 U.S.C. § 1002(a). Second, CALEA raised the standard for obtaining § 2703(d) orders, which are used to obtain cell-site records, from a "relevance" standard to the "specific and articulable facts" standard now in effect. *See* CALEA § 207; 18 U.S.C. § 2703(d). Especially in light of the "strong presumption of constitutionality" accorded to federal statutes challenged on Fourth Amendment grounds, *United States v. Watson*, 423 U.S. 411, 416 (1976), it is appropriate for this Court to respect the standard for cell site records established by the Congress.

In any event, even if the FPD intends to argue that the Stored Communications Act does not authorize a court to order the provision of historical cell site information, it is incorrect. Section 2703(c) straightforwardly provides that "a governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or a customer of such service (not including the contents of communications)." Historical cell site records are "a record or other information pertaining to a subscriber to or a customer of" a cell phone provider. Accordingly, the language of § 2703 plainly reaches historical cell site information. The FPD does not mention this language or argue that it does not reach historical cell site information, but, as the FPD points out (but only in the next section of its brief), "[a]nalysis of the statutory text" provides the answer to the question whether § 2703(d) allows the government to seek an order in this case. FPD Br. 25 (quoting *POM Wonderful, LLC v. Coca-Cola Co.*, 134 S. Ct. 2228, 2236 (2014)). In short, nothing in CALEA leaves this Court free to engage in a "reassessment of the interests at stake."

IV. An application that meets the requirement in 18 U.S.C. § 2703(d) to present "specific and articulable" facts must be granted.

Relying on the Third Circuit's decision in *In the Matter of Application of the U.S. for an Order Directing a Provider of Electronic Communications Service to Disclose Records to the Government*, 620 F.3d 304 (3d Cir. 2010) (*In the Matter of Application of the U.S.*), the FPD argues (Br. 25-28) that under the Stored Communications Act, 18 U.S.C. § 2703(d), a magistrate judge has discretion to deny an application that contains the requisite "specific and articulable facts" supporting issuance of an order to supply historical cell site information. That is not the issue that the FPD was asked to brief, and this Court has not suggested that it would decline to issue an order in response to an application that complies with § 2703(d) if that section does not violate the Fourth Amendment.

In any event, the FPD's argument is incorrect. The Stored Communication Act's language and structure make clear that a court may issue an order under § 2703(d) for historical cell site information. Section 2703(d) specifies that an order "may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers 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." As The Fifth Circuit has explained, the Third Circuit is incorrect because the phrase "shall" signifies a lack of discretion: "The word 'shall' is ordinarily 'the language of command.'" *In re Application*, 724 F.3d at 607 (quoting *Alabama v. Bozeman*, 533 U.S. 146, 153 (2001) (internal quotation omitted)). The court explained that the "may be issued" language grants a court the authority to issue the order, but the "'shall issue' term directs the court to issue the order if all the necessary conditions are met." *In re Application*, 724 F.3d at 607. Put another way, the phrase "may be issued" is "enabling language that allows the government to seek an order in any court of competent jurisdiction"; it does not grant a court discretion to refuse to issue an order altogether. *In re Application of the United States for an Order Pursuant to 18 U.S.C. § 2703(d)*, 830 F. Supp. 2d 114, 146-146 (E.D. Va. 2011) (finding that court has no discretion to decline to issue an order that satisfies § 2703(d)). Likewise, the phrase "only if" in the statute does not undercut the word "shall." As the district court in Virginia explained, the phrase "'only if' creates a necessary but not sufficient condition" but it "does not automatically create a gap in the statute that should be filled with judicial discretion." *Id*. at 148. In short, as the Virginia district court held, "[t]he statute contemplates a

simple situation in which the government presents its application for review by a judicial officer, who either approves or denies it." *Id*. at 147. For these reasons, the Third Circuit decision finding that magistrate judges have discretion under § 2703(d) is wrongly decided.[5]

DATED: August 8, 2014

Respectfully submitted,
MELINDA HAAG
United States Attorney

/s/
J. DOUGLAS WILSON
DAMALI A. TAYLOR
Assistant United States Attorneys

[5] Amicus ACLU argues at length (ACLU Br. at 4-8) that because applications to obtain historical cell site information are *ex parte*, "[m]agistrate judges . . . have not only the first but often the only opportunity to evaluate the constitutionality of warrantless demands for sensitive location information." But either § 2703(d) violates the Fourth Amendment or it does not; it is irrelevant to the question posed by the Court that magistrate judges issue § 2703(d) questions *ex parte*.