1	MELINDA HAAG (CABN 132612) United States Attorney
2 3	DAVID R. CALLAWAY (CABN 121782) Chief, Criminal Division
4	J. DOUGLAS WILSON (DCBN 412811) JEFFREY SCHENK (CABN 234355)
5	Assistant United States Attorneys
6	150 Almaden Boulevard, Suite 900 San Jose, California 95113
7	Telephone: (408) 535-5061 FAX: (408) 535-5066
8	Jeffrey.b.schenk@usdoj.gov
9	Attorneys for United States of America
10	
11	UNITED STATES DISTRICT COURT
12	NORTHERN DISTRICT OF CALIFORNIA
13	SAN JOSE DIVISION
14	
15	IN RE: APPLICATION FOR TELEPHONE) No. CR 15-90304 HRL (LHK)
16	INFORMATION NEEDED FOR A) CRIMINAL INVESTIGATION)
17) UNITED STATES' REPLY MEMORANDUM
18))
19	
20	
21	
22	
23	
23 24	
2 4 25	
23 26	
27	
28	

REPLY BRIEF REGARDING APPEAL OF DENIAL OF APPLICATION TO OBTAIN CELL SITE INFORMATION NO. CR 15-90304 MISC LHK

TABLE OF CONTENTS 1 2 I. 3 A. The government does not obtain content in an order under 18 U.S.C. 4 Cell site information does not reveal the user's precise location......2 5 В. C. The Supreme Court and the courts of appeals have held that no privacy 6 7 8 D. The manner in which cell phone users provide information to cell phone providers and the cell phone providers' policy do not create an expectation of 9 privacy......5 Historical cell site information constitutes a business record of the provider......7 10 II. An application that meets the requirement in 18 U.S.C. § 2703(d) to present "specific 11 and articulable" facts must be granted. 12 13 IV. The SCA provides authority to issue an order requiring cell phone providers to furnish cell site location information. 14 V. The FPD incorrectly asserts that imposing a warrant requirement would not have 15 practical implications on government investigations......11 16 17 18 19 20 21 22 23 24 25 26 27 28

TABLE OF AUTHORITIES

2	FEDERAL CASES	
3	Alabama v. Bozeman, 533 U.S. 146 (2001)	8
4	Bond v. United States, 529 U.S. 334 (2000)	2
5	Donaldson v. United States, 400 U.S. 517 (1971)	7

In re Application of the United States for an Order Pursua	nt to 18 U.S.C.	
§ 2703(d),830 F. Supp. 2d 114 (E.D. Va. 2011))

In re Application of U.S. for Historical Cell Site Data, 724 F.3d 600 (5th				
Cir. 2013)	. 4,	5, ′	7,	8

of Electronic Communications Service to Disclose Records to the	
<i>Government</i> , 620 F.3d 304 (3d Cir. 2010)	. 1. 9
	, , -
POM Wandarful LLC v. Coca Cola Co. 134 S. Ct. 2228 (2014)	1(

In the Matter of Application of the U.S. for an Order Directing a Provider

	`	,	
Ouon v. Arch Wireless Operating Co.,	529 F.3d 892 (9th Cir	r. 2008)	. 2
	()	,	
D:1 C-1:1 124 C Ct 2472 (20	11.4		1

SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735 (1984)	8
Smith v. Maryland, 442 U.S. 735 (1979)	1, 6

19	United States v. Cooper, 2015 WL 881578 (N.D. Cal. Mar. 2, 2015)
20	United States v. Davis, 785 F.3d 498(11th Cir. 2015)

l	Consecution of the control of the co	abbii	.11
	United States v. Forrester, 512 F.3d 500 (9th Cir. 2008)	5,	6

22	United States v. Jones, 132 S. Ct. 945 (2012)	3, 4	4
22	United States v. Miller 125 U.S. 125 (1076)	1 .	7

	,	`	/		,
United States v	. <i>Taketa</i> , 923 F.2d	665 (9th (Cir. 1991)	 	 2
United States	Watson 123 IIS	411 (197	(6)		10

STATE CASES	

١		
١	People v. Blair, 25 Cal. 3d 640 (Cal.	1979)
١	1 copie v. Biair, 23 car. 3d 6 to (car.	17/7)

Case5:15-xr-90304-HRL Document22 Filed06/19/15 Page4 of 16

FEDERAL STATUTES

REPLY BRIEF REGARDING APPEAL OF DENIAL OF APPLICATION TO OBTAIN CELL SITE INFORMATION NO. CR 15-90304 MISC LHK iii

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

The Federal Public Defender's (FPD) argument that cell phone users have a reasonable expectation of privacy in historical cell site information relies primarily on two assertions: (1) by obtaining historical cell site information, the government can somehow obtain the contents of cell phone communications; and (2) cell site information reveals the exact location of the cell phone user.

According to the FPD and its amici, it follows from these premises that 18 U.S.C. § 2703(d) is unconstitutional to the extent that it does not require a warrant, and therefore the government must obtain a warrant based on probable cause to obtain historical cell site information. Both premises are faulty.

A. The government does not obtain content in an order under 18 U.S.C. § 2703(d)

First, the FPD's repeated citation (FPD Br. 1, 20-22; *see* Electronic Frontier Foundation (EFF) Br. 6-7) of *Riley v. California*, 134 S. Ct. 2473 (2014), cannot change the fact that *Riley* concerned the contents of a cell phone, and the government cannot and does not obtain the contents of a cell phone or cell phone communications in an order under Section 2703(d). *See 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, 306 (3d Cir. 2010) (*In the Matter of Application of the U.S.*) (orders under Section 2703(d) do not seek content). In particular, orders under Section 2703(d) do not reveal "vast amounts of personal information about their owners" that, according to *Riley*, cell phones contain. Although it may be true that, as the FPD argues (Br. 20), "*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 it created a privacy interest in historical cell site information or any other business record held by a third party. For this reason, the FPD is simply wrong in asserting (Br. 20) that "[a]fter *Riley*, there is no doubt that individuals have a reasonable expectation of privacy in cell phone location data." As the Eleventh Circuit recently noted in response to a defendant's effort to rely on *Riley*, "It is not helpful to lump together doctrinally unrelated cases that happen to involve

¹ Contrary to the FPD's suggestion, in this case the government is not seeking to appeal Judge Lloyd's order to the extent it denied the government 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.

similar modern technology." United States v. Davis, 785 F.3d 498, 516 n.19 (11th Cir. 2015) (en banc).

The government's inability to obtain content under Section 2703(d) also defeats the FPD's claim (FPD Br. 18) that "the Supreme Court and the Ninth Circuit have consistently held that exposing information to a third party does not automatically waive one's expectation of privacy." In the cases cited by the FPD, the government sought access to the content of an item. *See Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001) (patient has reasonable expectation of privacy in her urine); *Bond v. United States*, 529 U.S. 334 (2000) (person retains expectation of privacy in contents of opaque bag even after it is placed in overhead bin of bus); *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892 (9th Cir. 2008) (police officer had reasonable expectation of privacy in content of text messages).² Here, as the government has repeatedly made clear, it cannot obtain the content of a cell phone call through an order seeking historical cell site information.

B. Cell site information does not reveal the user's precise location

Second, the FPD is incorrect in arguing (FPD Br. 4, 7) that cell site location information may be used to calculate cell phone users' location with a precision that "approaches that of GPS," can "track individuals," "provides the government with a comprehensive, intimate portrait of an individual's life," or allows the government "to track people inside buildings." As the FPD acknowledges, historical cell site information allows the government to obtain information only about the cell tower a given call or data transmission is using to transmit or receive a call, text, or data transmission. In particular, historical cell site information ordinarily tells the provider and the government 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

² In *United States v. Taketa*, 923 F.2d 665 (9th Cir. 1991), the court found that a person has an expectation of privacy in not being secretly videotaped in another's office. That holding did not rest on the fact that a person conveyed his presence to a third party and has no bearing on whether cell phone users have an expectation of privacy.

³ The government has supported its assertions about cell site location information with a declaration from FBI Special Agent Hector M. Luna, who is currently assigned to the FBI's Cellular Analysis Survey Team. In addition to setting forth the means by which cell site location information is obtained and analyzed, Special Agent Luna's declaration state that "most modern smart cellular phones have applications that continually run in the background that send and receive datawithout a user having to interact with the cellular telephone." Luna Declaration ¶ 3.C. Even if such continually running background applications generate cell site location information, the government is not aware of any case in which it has introduced evidence based on information

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. 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 or the phone is otherwise engaged in data transmission.⁴

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 through a GPS device; it did not purport to limit the government's ability to obtain information from a third party that 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 is communicating with a cell tower. See Luna Declaration at ¶ 3. 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

25

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

obtained from these applications' interaction with a cell tower. Moreover, the fact that these applications may interact with a tower does not create an expectation of privacy in cell phone users.

27

28

⁴ The FPD claims (Br. 3) that "there are 199 towers and 652 separate antennas" within three miles of the federal courthouse in San Jose. 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 199 towers have been erected by many different companies.

Communications Act. See Jones, 132 S. Ct. at 964 (Alito, J., concurring).

C. The Supreme Court and the courts of appeals have held that no privacy interest exists in cell site information

As set forth in the government's opening brief, 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. *See Smith v. Maryland*, 442 U.S. 735 (1979); *United States v. Miller*, 425 U.S. 435 (1976). Moreover, the FPD acknowledges (FPD Br. 17) that the Fifth and, recently, the en banc Eleventh Circuit have followed the Supreme Court and held that a cell phone user does not have an expectation of privacy in cell phone records. *See United States v. Davis*, 785 F.3d 498 (11th Cir. 2015) (*en banc*); *In re Application of U.S. for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013) (*In re Application*). The FPD's response is simply that those courts got it wrong. But no court of appeals has ever accepted the FPD's and its amici's argument that a cell phone user has an expectation of privacy in historical cell site information. In fact, other than Judge Illston in *United States v. Cooper*, 2015 WL 881578 (N.D. Cal. Mar. 2, 2015), the government is not aware of any district court judge that has found that a cell phone user has an expectation of privacy in historical cell site location information, and the FPD does not cite one.

In addition to relying on the now-overturned, panel opinion in *Davis*, the FPD, the amici, and Judge Illston in *Cooper* cite society's expectation of privacy in light of rapidly evolving technology. *Davis* answers that concern. While the *en banc* court in *Davis* acknowledged the rapidly evolving landscape of technology, it concluded that does not undermine the Supreme Court's pronouncement in *Smith*:

Admittedly, the landscape of technology has changed in the years since these binding decisions in *Miller* and *Smith* were issued. But their holdings did not turn on assumptions about the absence of technological change. To the contrary, the dispute in *Smith*, for example, arose in large degree due to the technological advance from call connections by telephone operators to electronic switching, which enabled the electronic data collection of telephone numbers dialed from within a home. 442 U.S. at 744-45. The advent of mobile phones introduced calls wirelessly connected through identified cell towers. This cell tower method of call connecting does not require "a different constitutional result" just "because the telephone company has decided to automate" wirelessly and to collect the location of the company's own cell tower that connected the calls. *See id.* at 744-45. Further,

Davis, 785 F.3d at 512.

MetroPCS's cell tower location information was not continuous; it was generated only when Davis was making or receiving calls on his phone. The longstanding third-party doctrine plainly controls the disposition of this case.

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. The Supreme Court has never overruled *Smith* or *Miller*, however, and this Court is not free to disregard those cases.⁵

D. The manner in which cell phone users provide information to cell phone providers and the cell phone providers' policy do not create an expectation of privacy

The FPD and amicus ACLU argue that a cell phone user does not voluntarily share his or her location information with the cell phone provider. *See* FPD Br. 12-14; ACLU Br. 8-10. The FPD asserts that cell phone users only passively convey signals to cell site towers, and that they "do not affirmatively convey" cell site location information. FPD Br. 12-13. In *Davis* and *In re Application*, the courts of appeals rejected this argument, finding that "cell users know that they must transmit signals to cell towers within range [and] that users when making or receiving calls are necessarily conveying or exposing to their service provider their general location within that cell tower's range." *Davis*, 785 F.3d at 511; *see In re Application*, 724 F.3d at 613-14.

The FPD argues (Br. 13) that in *United States v. Forrester*, 512 F.3d 500 (9th Cir. 2008), the court "rejected the general theory that passive transmission of data to a third party waives a consumer's Fourth Amendment rights." In *Forrester*, the Ninth Circuit upheld pen register surveillance – obtained without a warrant – in which the government obtained the to/from addresses on the defendant's e-mail, the IP addresses of websites that the defendant visited, and the total volume of information sent to or

⁵ 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*.

REPLY BRIEF REGARDING APPEAL OF DENIAL OF APPLICATION TO OBTAIN CELL SITE INFORMATION NO. CR 15-90304 MISC LHK

fro
 sea
 cor
 of a

from his account. The Ninth Circuit held that "the surveillance did not constitute a Fourth Amendment search and thus was not unconstitutional." 512 F.3d at 509. The Ninth Circuit relied on the fact that a computer user relied on "third-party equipment in order to engage in communication," and the absence of an expectation of privacy because computer users "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.* at 510. In that respect, cell phone use is indistinguishable from computer use, and *Forrester* supports the government's argument that a cell phone user has no expectation of privacy.

The ACLU argues that the privacy 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 v. Maryland*, 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 store 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 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 use of the cell phone will result in the generation of records by the cell phone provider.

1 2

3

4 5

6

7

8

9 10

11

12

13 14

15

16

17 18

19

20

21

22

23

- 24
- 25
- 26 27
- 28

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

As the Fifth Circuit held in *In re Application*, 724 F.3d at 612, and the government argued in its opening brief, a historical cell site record is "clearly a business record." Likewise, in the recent *en banc* decision in *United States v. Davis*, the court held that cell tower location records were business records of the provider created for "legitimate business purposes." See 785 F.3d at 511. Instead of quarreling with this finding, the FPD argues that it is irrelevant because cell phone users have a reasonable expectation of privacy in cell phone records. But the FPD ignores the import of that finding: because the cell site location records are business records of the provider, the user has "no subjective or objective reasonable expectation of privacy." Davis, 785 F.3d at 511; see In re Application, 724 F.3d at 610 (finding that creation of business record means that cell phone user has no expectation of privacy).

The Supreme Court has also made clear that 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. See Davis, 785 F.3d at 511-512.

Because historical cell site records are business records created and stored at the discretion of the provider, the government could use a Section 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 REPLY BRIEF REGARDING APPEAL OF DENIAL OF APPLICATION TO OBTAIN CELL SITE INFORMATION

address voluntariness in SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735 (1984), which held that the target of 1 2 an investigation had no right to notice of subpoenas issued to third parties. See id. at 743 n.11 ("It should 3 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 4 5 argue that the subpoena recipients were required by law to keep the records in question.").

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

III. 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.*, the FPD argues (Br. 27-30) that under Section 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 Judge Lloyd did not suggest that he would decline to issue an order in response to an application that complies with Section 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 must issue an order under Section 2703(d) for historical cell site information if the government satisfies the statutory standard. 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) REPLY BRIEF REGARDING APPEAL OF DENIAL OF APPLICATION TO OBTAIN CELL SITE INFORMATION

(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 in this respect. *See In re Application of the U.S.* 620 F.3d at 319-21 (Tashima, J., concurring) (noting that panel majority's finding that magistrate judges have discretion to grant Section 2703(d) orders "is contrary to the spirit of the statute" and "vests magistrate judges with arbitrary and uncabined discretion"). ⁶

IV. The SCA provides authority to issue an order requiring cell phone providers to furnish cell site location information.

The FPD appears to argue (Br. 22-27) 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.

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 Director Louis Freeh testified that "[s]ome cellular carriers do acquire information relating to the general

⁶ 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 Section 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*.

REPLY BRIEF REGARDING APPEAL OF DENIAL OF APPLICATION TO OBTAIN CELL SITE INFORMATION NO. CR 15-90304 MISC LHK 9

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 Section 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

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 Section 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 Section 2703(d) allows the government to seek an order in this case. FPD Br. 27 (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."

27 ||

V. The FPD incorrectly asserts that imposing a warrant requirement would not have practical implications on government investigations

In the final section of its brief, the FPD asserts (Br. 31) that it is arguing "only" that law enforcement officers must obtain a warrant when seeking cell site location information. The FPD justifies this claim by asserting (Br. 31) that "there will rarely, if ever, be such an urgent need for [cell site location information] that officers would not have time to get a warrant." At the outset, that observation is irrelevant: Section 2703(d) is either constitutional or it is not. The circumstances under which officers use Section 2703(d) has no bearing on the legal question before the Court.

In any event, the FPD's assertion ignores the fact that the government does not always have probable cause when it seeks cell site location information and frequently uses orders under Section 2703(d) as an investigative tool. In particular, the government often seeks cell site location information at an early stage of an investigation. *See Davis*, 785 F.3d at 518 (information obtained through Section 2703(d) order "is particularly valuable during the early stages of an investigation when the police lack probable cause and are confronted with multiple suspects"). Under the FPD's view, Section 2703(d) orders would be limited to situations in which probable cause existed, and the government could not use cell site location information early in an investigation when probable cause may not exist. The FPD's approach would therefore foreclose the government from using a Section 2703(d) order in a situation in which Congress plainly intended it.

//

20 || .

21 || /

22 | //

 $_{25}$

26 | //

27 || .

Case5:15-xr-90304-HRL Document22 Filed06/19/15 Page16 of 16

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

As noted by the Eleventh Circuit in *Davis*, the SCA has a privacy-protecting function. The court noted that Section 2703(d) imposes a neutral magistrate between citizens and officers, that Section 2702 prohibits voluntary disclosure by providers, and that Section 2707 prohibits improper disclosure of records obtained under Section 2703(d). As the court explained, "[t]he SCA goes above and beyond the constitutional requirements regarding compulsory subpoena process." Davis, 785 F.3d at 506. Should this Court find that privacy-protecting function insufficient, it must find the SCA unconstitutional under the Fourth Amendment.⁷ DATED: June 19, 2015 Respectfully submitted, MELINDA HAAG United States Attorney J. DOUGLAS WILSON JEFFREY SCHENK

Assistant United States Attorneys

REPLY BRIEF REGARDING APPEAL OF DENIAL OF APPLICATION TO OBTAIN CELL SITE INFORMATION NO. CR 15-90304 MISC LHK 12

⁷ As the *Davis* court found, an order under Section 2703(d) is also "reasonable" and therefore does not violate the Fourth Amendment for that reason as well. See Davis, 785 F.3d at 516-18. That is because a cell phone user has at most a "diminished expectation of privacy" in cell phone records, a Section 2703(d) order causes only a "minimal" intrusion into that expectation of privacy, a judicial officer issues a Section 2703(d) order, and such an order serves compelling government interests.