NINTH CIRCUIT MAGISTRATE JUDGES EDUCATION COMMITTEE

Ninth Circuit Judicial Conference

San Diego, California

July 2015

When Privacy is No Longer Private: A Judicial Primer on Cell Location Data

Moderator Judge Jacqueline Corley, U.S. Magistrate Judge for the Northern District of California

Panelists Judge William Cobb, U.S. Magistrate Judge for the District of Nevada

Richard Downing, Principal Deputy Chief, Computer Crime & Property Section, U.S. Department of Justice

Lisa Hay, Acting Federal Public Defender, District of Oregon

MATERIALS

1. The Fourth Amendment and Cell Site Location Information: What Should We Do While We Wait For The Supremes?, 8 FEDERAL COURTS LAW REVIEW 215 (2015)

2. *United States v. Dominic Dorsey*, 2:14-cr-00328-CAS, 2015 WL 847395 (Feb. 23, 2015, C.D. Cal.) (Snyder, J.)

3. *United States v. Elijah Cooper*, 3:13-cr-00693-SI, 2015 WL 881578 (March 2, 2015, N.D. Cal) (Illston, J.)

4. *In Re Application For Telephone Information Needed For A Criminal Investigation*, 15-CR-9030 (April 9, 2015, N.D. Cal) (Lloyd, M.J.)

5. *United States v. Davis*, 785 F.3d 498 (11th Cir. May 5, 2015) (*en banc*)

6. *In Re Telephone Information Needed For A Criminal Investigation*, Brief in Opposition to Government's Application Under 18 U.S.C. § 2703(d) For Cell Site Location Information, 14-xr-90532 (N.D. Cal, July 28, 2014)

7. *In the Matter of the Application of the United States of America for an Order Authorizing Prospective And Continuous Release Of Cell Site Location Records*, 31 F.Supp.3d 889 (2014) (Smith, M.J.)

8. *In The Matter Of The Application Of The United States Of America For An Order Pursuant To 18 U.S.C. §§ 2703(C) And 2703(D) Directing AT & T, Sprint/Nextel, T–Mobile, Metro PCS And Verizon Wireless To Disclose Cell Tower Log Information*, 42 F.Supp.3d 511 (S.D.N.Y. 2014) (Francis, M.J.)

9. *United States v. Rigmaiden*, 2:08-cr-00814-DGC, 2013 WL 1932800 (May 8, 2013, D. Ariz.) (Campbell, J.) (excerpts)

10. *In Re Application Of The United States of America For Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013)

11. List of Selected Cases Addressing Cell Site Location Information

12. Washington State Bill Limiting Use Of Stingray/Triggerfish Devices, House Bill 1440, 64th Leg. Regular Session (Wa. 2015)

13. Brian Owsley, *Triggerfish, Stingrays, and Fourth Amendment Fishing Expeditions*, 66 Hastings L.J. 183 (Dec. 2014)

THE FEDERAL COURTS LAW REVIEW

Volume 8, Issue 2 2015

The Fourth Amendment and Cell Site Location Information: What Should We Do While We Wait for the Supremes?

Patrick E. Corbett*

I. INTRODUCTION 215
II. WHAT IS CELL SITE LOCATION INFORMATION? 217
III. *IN RE APPLICATION*, *SKINNER*, AND OTHER FEDERAL COURTS 218
IV. CELL PHONE USERS HAVE ALTERNATIVES 226
V. CONCLUSION 230

I. INTRODUCTION

In *In re Application of the United States of America for Historical Cell Site Data*[1] (hereinafter *In re Application*), the United States Court of Appeals for the Fifth Circuit held, in a 2-1 opinion, that "court orders authorized by the Stored Communications Act to compel phone service providers to produce the historical cell site information of their subscribers [are not] per se unconstitutional."[2] Essentially, the opinion means that federal law enforcement officers (at least in the Fifth Circuit) can continue to obtain historical cell site information on a showing of less than probable cause. The officers need only provide "specific and articulable facts showing that there are reasonable grounds to believe" that the desired

---

*Professor of Criminal Law & Procedure, Thomas M. Cooley Law School, Lansing, Michigan. The author thanks the Federal Courts Law Review, Charleston School of Law, for inviting him to participate in the 2014 Federal Courts Law Review Symposium. The author also wishes to acknowledge the detailed, timely, and academic research of Cooley Law School librarian, Jamie Baker. This article is an expansion of an article originally published by JURIST, a publication of the University of Pittsburgh School of Law. *See* Patrick Corbett, *Fifth Circuit Makes Sound Decision on Cell Site Location Information*, JURIST – FORUM (Sept. 09, 2013), http://jurist.org/forum/2013/09/patrick-corbett-cel-tower-tracking.php.

1. 724 F.3d 600 (5th Cir. 2013).
2. *Id.* at 602.

information is "relevant and material to an ongoing criminal investigation" in order to get an order from a court.[3] In so ruling, the Fifth Circuit quoted a 2012 Sixth Circuit opinion, *United States v. Skinner* , noting that "[l]aw enforcement tactics must be allowed to advance with technological changes, in order to prevent criminals from circumventing the justice system."[4]

Did the Fifth Circuit get it right? Should law enforcement be able to get historical cell site location information on a showing of less than probable cause? How about real-time cell site location information? Should law enforcement be able to obtain that data on a showing of less than probable cause (as held in *Skinner*)? At present, it appears that the courts will have to answer these questions without the help of the U.S. Supreme Court. The Court denied certiorari in *Skinner*[5]and no review was sought in *In re Application*.

This article will provide a general overview of how various jurisdictions have handled these questions. Section I will provide a definition of cell site location information and briefly examine some relevant federal statutes.[6] Section II will discuss the *In re Application* and *Skinner* cases, noting how other federal courts have handled similar questions, and will also touch on a few recent United Supreme Court cases that may have an impact on the ability of law enforcement to access and use cell site location information. Section III will explore some alternatives arguably available to "cell phone users [who] may reasonably want their location information to remain private . . .."[7] The article will conclude with some practical reflections on how law enforcement will proceed while we wait for direction from the Supreme Court.[8]

---

3. *Id.* at 606 (quoting 18 U.S.C. § 2703(d) (2012)).

4. *Id.* at 614 (quoting *United States v. Skinner*, 690 F.3d 772, 778 (6th Cir. 2012), *cert. denied*, 133 S.Ct. 2851 (2013)).

5. 690 F.3d 772 (6th Cir. 2012), *cert. denied*, 133 S.Ct. 2851 (2013).

6. This article will briefly touch on the Stored Communications Act, Pub. L. No. 99-508, 100 Stat. 1848, 1860 (codified as amended at 18 U.S.C. §§ 2701-2712) and the Pen Register/Trap and Trace Statute, 18 U.S.C. §§ 3121-3127. A full discussion of these complex statutes is beyond the scope of this article.

7. 724 F.3d at 615.

8. Much has already been written on cell tower location information and the Fourth Amendment. *See, e.g.*, Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact,* 27 BERKELEY TECH. L.J. 117 (2012); Marc McAllister, *GPS and Cell Phone Tracking: A Constitutional and Empirical Analysis*, 82 U. CIN. L. REV. 207 (2013); Christopher R. Orr, *Your Digital Leash: The Interaction Between Cell Phone-Based GPS Technology and Privacy Rights in United States v. Skinner*, 45 U. TOL. L. REV. 377 (2014); Jacob T. Whitt, *Cell Phones as an Eye of the Government: In Re Application of the United States for Historical Cell Site Data*, 88 TUL. L. REV. 831 (2014); Kevin T. Crane, Jr., *Sixth Circuit Court of Appeals Creates New Categorical Exclusion from Warrant Requirement in U.S. v. Skinner*, 40 NEW ENG.

II. WHAT IS CELL SITE LOCATION INFORMATION?

What is "cell site location information"? What does this type of information involve? In a recent American Bar Association Journal article, writer Mark Hansen defined "cell tower records" as follows: "Cell tower records, also known as call detail records, are the billing records cell companies use to keep track of their customers' calls. They show the date and time of all calls made or received, the numbers called, the duration of each call, and the cell towers used to begin and end a call."[9] Such information has proved to be highly useful to law enforcement in a wide variety of cases, from "finding a missing person to tracking 911 hang-up(s) to tracking a suspect."[10] Some in law enforcement believe that requiring officers to get a search warrant would "cripple"[11] their investigations. Nevertheless, given the potentially extreme private nature of such records, the question arises[12] regarding what level of proof law enforcement should be required to show in order to get such information.

It is important to recognize that cell tower location information can be "historical" or "real-time"; that is, past connections of cell phones to cell towers or connections of cell phones to cell towers as they actually occur. Traditionally, historical non-content call records have required a court order

---

J. ON CRIM. & CIV. CONFINEMENT 275 (2014); Erik E. Hawkins, *No Warrants Shall Issue But Upon Probable Cause: The Impact of the Stored Communications Act on Privacy Expectations*, 4 WAKE FOREST J. L. & POL'Y 257 (2014); Charles E. MacLean, *Katz on a Hot Tin Roof: The Reasonable Expectation of Privacy Doctrine is Rudderless in the Digital Age, Unless Congress Continually Resets the Privacy Bar*, 24 ALB. L. J. SCI. & TECH. 47 (2014); *Fourth Amendment – Warrantless Searches – New Jersey Supreme Court Holds that State Constitution Requires Police to Obtain Warrant Before Accessing Cell-Site Location Information – State v. Earls, 70 A.3d 630 (N.J. 2013)*, 127 HARV. L. REV. 2164 (2014). As such, this article will only provide brief overviews of relevant background information and will focus instead on how the various jurisdictions have dealt with cell tower location information with no specific guidance from the United States Supreme Court.

9. Mark Hansen, *Prosecutors' Use of Mobile Phone Tracking is 'Junk Science,' Critics Say*, A.B.A. J. (June 1, 2013 3:50AM), http://www.abajournal.com/magazine/article/prosecutors_use_of_mobile_phone_tracking_is_junk_science_critics_say/.

10. Sheldon Gardner, *Latest Tool for Fighting Crime: Your Cellphone*, ST. AUGUSTINE REC. (July 7, 2013 12:02 AM), http://staugustine.com/news/local-news/2013-07-07-1#.UkKDq9K2NfZ.

11. Liz Klimas, *DOJ Official Says Requiring a Warrant to Track Cellphones Would 'Cripple' Criminal Investigations*, THE BLAZE (May 9, 2012, 12:55 AM), http://www.theblaze.com/stories/2012/05/09/doj-official-says-requiring-a-warrant-to-track-cellphones-would-cripple-criminal-investigations/#.

12. Liz Klimas, *Court: No Warrant Required for Cellphone Location Data Because It's 'Clearly a Business Record'*, THE BLAZE (July 31, 2013), http://www.theblaze.com/stories/2013/07/31/court-no-warrant-required-for-cellphone-location-data-because-its-clearly-a-business-record/.

under the Stored Communications Act (SCA)[13] which requires a showing by the government of "specific and articulable facts showing that there are reasonable grounds to believe that [the specified records] are relevant and material to an ongoing criminal investigation."[14] Importantly, the SCA also authorizes LE to obtain various other historical electronic records with a subpoena (generally based on a showing of relevance)[15] or a search warrant (based upon probable cause).[16] While subject to some debate, the SCA generally requires a lesser showing by the government when the data is not that private and a greater showing when the data is more private.

The Pen Register/Trap and Trace Statute,[17] on the other hand, addresses "real-time" cell tower location information. This prospective (as it actually happens) cell phone data can be obtained through a court order based upon a "certification by applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency."[18]

In either instance (historical or real-time), cell tower location information is generally not considered to be "content"; that is, it does not include the actual words communicated through the cell phone call.[19] Rather, cell tower location information deals with the numbers used to make calls, the duration of the calls, and what cell towers were used to make those calls.

What kind of showing should law enforcement be required to make in the context of cell site location information? Did Congress get it right? Or do the protections of the Fourth Amendment require a greater showing? The next section will explore how some federal courts have answered these questions.

III. *IN RE APPLICATION*, *SKINNER*, AND OTHER FEDERAL COURTS

In *In re Application*, federal authorities sought "historical cell site

---

13. 18 U.S.C. §§ 2701-2712 (2012).
14. 18 U.S.C. § 2703(d) (2012).
15. Under Michigan law, for example, a court will authorize a subpoena if the judge finds reasonable cause to believe the subpoenaed records, etc., are relevant to the investigation of a felony. MICH.COMP.LAWS. § 767A.3(1)(c)(ii) (2014).
16. 18 U.S.C. § 2703.
17. 18 U.S.C. §§ 3121-3127 (2012).
18. 18 U.S.C. §3122(b).
19. Real-time content-based communications are controlled by the Federal Wiretap Statute. *See* 18 U.S.C. §§ 2510-22; historical content-based communications are controlled by the Stored Communications Act, Pub. L. No. 99-508, 100 Stat. 1848, 1860 (codified as amended at 18 U.S.C. §§ 2701-2712).

information" in connection with "three separate criminal investigations."[20] The United States Magistrate Judge granted the request for subscriber information pertaining to the cell phone, but denied the request for other historical cell site information. The United States District Court agreed and the government appealed.

Characterizing the issue as "whether court orders authorized by the Stored Communications Act to compel cell phone service providers to produce the historical cell site information of their subscribers are per se unconstitutional", the court held "that they are not."[21] As already noted, the court justified the holding, in part, by noting that "[l]aw enforcement tactics must be allowed to advance with technological changes, in order to prevent criminals from circumventing the justice system."[22] This quote appears to sum up the likely motivation for *In re Application* – the government interest in obtaining the information (and thus enabling law enforcement to pursue criminal suspects by embracing the very technology criminals often use to avoid detection) outweighs the privacy interests presented by the facts of the case.

In its analysis, the court examined the recent U.S. Supreme Court decision of *United States v. Jones*.[23] In *Jones*, the Court held that law enforcement attaching a global positioning system (GPS) device to a car constituted a search under the Fourth Amendment so it would require probable cause and a warrant. A vital fact in reaching this decision was that "[t]he Government physically occupied private property for the purpose of obtaining information."[24] In *In re Application*, the court distinguished *Jones* by drawing "a line based on whether it is the Government collecting the information or requiring a third party to collect and store it, or whether it is a third party, of its own accord and for its own purposes, recording the information."[25] Law enforcement in *In re Application* did not physically occupy the private property of the suspects in order to obtain the information; as such, the Fifth Circuit distinguished *Jones*. As "third party's voluntarily created business records," federal law enforcement can obtain historical cell site information with a court order under the SCA.[26] Noting that the SCA "conforms to existing Supreme Court precedent" on the Fourth Amendment, the court "decline[d] to create a new rule to hold that

---

20. *In re Application*, 724 F.3d at 602.
21. *Id.*
22. *Id.* at 614 (quoting *Skinner*, 609 F.3d at 778).
23. *Jones*,132 S.Ct. 945 (2012).
24. *Id.* at 949.
25. 724 F.3d at 610.
26. 18 U.S.C. §§ 2701- 2712 (2012).

Congress's balancing of privacy and safety is unconstitutional."[27]

Citing *Jones*, however, the dissent in *In re Application* pointed out that "every member of the Court acknowledged last year that law enforcement's access to the location information generated by cell phones raises serious constitutional questions."[28] In support, the dissent quoted Justice Sotomayor's concurrence in *Jones*: "[In future cases] considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements[,] . . . it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[29]

In *United States v. Skinner*,[30] defendant Skinner was transporting large quantities of marijuana across state lines in a recreational vehicle. Through lawful conversation intercepts between other members of the drug conspiracy, officers determined what prepaid phone Skinner might have used to communicate with other members. Using both the SCA and the Pen Register/Trap and Trace statutes, the officers then obtained an order from a federal magistrate ordering the relevant phone company to release cell tower information, GPS real-time information, and other data to "ping" phone's location. Officers "pinged" the phone to track Skinner's progress to a truck stop, where local authorities arrested him with over 1100 pounds of marijuana.[31]

Defendant moved to suppress the cell site information, asserting a Fourth Amendment violation due to the fact that a court order (based on less than probable cause) was used to get this information and agents should have had probable cause and a warrant.[32] The U.S. District Court denied the motion, adopting the U.S. Magistrate Judge's opinion that, *inter alia*, "because the cell phone was utilized on public thoroughfares and was 'bought by a drug supplier and provided to . . . Skinner as part and parcel of

---

27. 724 F.3d at 614-15.

28. *Id.* at 622.

29. *Id.* at 623. There is considerable support within the legal community for reconsidering this third party doctrine. The American Bar Association Criminal Justice Standards Committee recently promulgated "Law Enforcement Access to Third Party Records," urging alternatives in lieu of the third party doctrine. A.B.A. STANDARDS FOR CRIM. JUST., LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS (3d ed. 2013), *available at* http://www.americanbar.org/content/dam/aba/publications/criminal_justice_standards/third_party_access.authcheckdam.pdf. In a recent law review article, Professor Stephen Henderson argues that the federal courts are already moving away from this doctrine. *See* Stephen Henderson, *After United States v. Jones, After the Fourth Amendment Third Party Doctrine*, 14 N.C.J. LAW & TECH. 431 (2013).

his drug trafficking enterprise,' Skinner did not have a legitimate expectation of privacy in the phone or in the motorhome that was driven on public roads."[33]

The Sixth Circuit affirmed, holding that "[t]here is no Fourth Amendment violation because Skinner did not have a reasonable expectation of privacy in the data given off by his voluntarily procured pay-as-you-go cell phone."[34] While the cell site location information aided officers in tracking Skinner's location, the same information would have been available through physically following him or visual surveillance.[35] The court went on to state that "[t]here is no inherent constitutional difference between trailing a defendant and tracking him via such technology."[36] The court distinguished *Jones* because the tracker in that case was physically installed on the defendant's car.[37] Here, there was no such physical intrusion.[38] The agents merely tracked a known cell number that was voluntarily used on public thoroughfares.[39]

How have other federal circuit courts handled similar concerns? The courts are clearly split, suggesting that it is only a matter of time before the U.S. Supreme Court intervenes. Like the Fifth Circuit in *In re Application* and the Sixth Circuit in *Skinner*, the Seventh Circuit has held that probable cause and a warrant are not required.[40] The Third Circuit has noted that courts have the option to require warrants based upon probable cause for historical cell tower data.[41] Going further, the Eleventh Circuit, recently held that "cell site location information is within the subscriber's reasonable expectation of privacy" and that "[t]he obtaining of that data without a warrant is a Fourth Amendment violation."[42]

---

33. *Id.* at 776-77.
34. *Id.* at 777.
35. *Id.* at 778.
36. *Id.*
37. *Id.* at 780.
38. *Id.*
39. *Id.* at 780-81.
40. United States v. Thousand, 558 F. App'x 666, 670 (7th Cir. 2014) ("We have not found any federal appellate decision accepting Thousand's premise that obtaining cell-site data from telecommunications companies – under any factual scenario – raises a concern under the Fourth Amendment. Like the district court, we would have no reason in this case to express an opinion about whether a probable-cause standard should govern 18 U.S.C. §2703(d) applications seeking cell-tower data that will disclose a subscriber's location at a particular time.").
41. 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) (court did not require the government to obtain a warrant).
42. United States v. Davis, 754 F.3d 1205, 1217 (11th Cir. 2014) (quoting the Third Circuit Court of Appeals, the court stated that "a cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way" and, hence, the third

United States District Courts are similarly divided. A U.S. District Court in the District of Columbia recently declined to rule on whether a warrant was required in the context of historical cell site location information without more evidence on the underlying technology.[43] Some courts have rejected arguments that probable cause and the Fourth Amendment must be applied to requests for cell site data.[44] Other courts

---

party doctrine does not require a finding that the defendant has no reasonable expectation of privacy). Not surprisingly, the court held that, even with the Fourth Amendment violation, the evidence was still admissible based on the good-faith exception to the warrant requirement. *Id.*

43. In Matter of United States, MC 14–286 (JMF), 2014 WL 1395082, at *3 (D.D.C.Apr. 17, 2014) ("These contrasting views about what the Fourth Amendment requires can only be answered with any reasonable certainty by taking evidence about how cell phones work and what subscribers reasonably understand about how their phones are tracked. For example, how frequently is CSLI generated and how closely can it track a person's location? Is it only generated when a phone call is made? If the government asks for only a narrow subset of CSLI, what does the provider *actually* give the government? What do the terms of service say about tracking a person's location? Does any location information appear on a person's bill? These are all of the types of factual questions that require this Court to develop a factual record. Taking the Third Circuit's hint, this Court will do so before making any determinations about whether the Fourth Amendment prohibits the issuance of an order requiring the disclosure of CSLI absent a showing of probable cause.").

44. *See, e.g.*, United States v. Carabello, 963 F. Supp. 2d 341 (D. Vt. 2013) (defendant had no reasonable expectation of privacy in his real time cell phone location information; exigent circumstances justified warrantless cell phone pinging); *In re* Smartphone Geolocation Data Application, 977 F. Supp. 2d 129 (E.D.N.Y. 2013) (no reasonable expectation of privacy in prospective cell-site data); United States v. Graham, 846 F. Supp. 2d 384, 402-05 (D. Md. 2012); *In re* Applications of U.S. for Orders Pursuant to Title 18, U.S. Code Section 2703(d), 509 F. Supp. 2d 76, 80-81 (D. Mass. 2007) (reversing Applications of United States for Orders Pursuant To Title 18, U.S. Code, Section 2703(d) to Disclose Subscriber Information and Historical Cell Site Information, 509 F. Supp. 2d 64 (D. Mass. 2007), in which a magistrate judge held that probable cause was required for the disclosure of historical cell site information). *See also* Fernandez v. Valenzuela, CV 12–9080–ODW SH, 2014 WL 293485 (C.D. Cal. Jan. 24, 2014) (court denied petition for habeas corpus for ineffective assistance of counsel when attorney did not file a motion to suppress evidence because it was not unreasonable in light of the law regarding the use of cell phone location information existing at the time of trial in 2009); United States v. Ruibal, No. 1:12–CR–132, 2014 WL 357298, at *2 (W.D. Mich. Jan. 31, 2014) ("In light of *Skinner*, Rios did not have an expectation of privacy in the location data from his cell phone, so the tracking of his cell phone [for a two-day period] does not qualify as a search under the Fourth Amendment. Because there was no Fourth Amendment search, no warrant was required...."); United States v. Carpenter, 12–20218, 2013 WL 6385838 (E.D. Mich. Dec. 6, 2013) (following *Skinner*); United States v. Moreno-Nevarez, 13–CR–0841–BEN, 2013 WL 5631017, at *2 (S.D. Cal. Oct. 2, 2013) ("'no reasonable expectation of privacy' in historical cell site data"); United States v. Booker, No. 1:11–CR–255–1–TWT, 2013 WL 2903562, at *9 (N.D. Ga. June 13, 2013) ("any expectation of privacy defendants assert in cell site location information contained in cell phone company records 'is not one that society is prepared to recognize as reasonable'"; found no real distinction with historical or prospective cell site location information); United States v. Rigmaiden, CR 08–814–PHX–DGC, 2013 WL 1932800 (D. Ariz. May 8, 2013) appeal dismissed (Nov. 19, 2013), reconsideration denied, CR-08-814-PHX-DGC, 2013 WL 4525252 (D. Ariz. Aug. 27, 2013) (one has no legitimate expectation of privacy in information he voluntarily turns over to third parties); United States v. Ruby, 12CR1073 WQH, 2013 WL 544888 (S.D. Cal. Feb. 12, 2013) (historical cell site location records are business records of the provider and not entitled

have determined that probable cause is necessary (or was actually present, whether or not it was needed) for such information.[45] Several courts have used the good faith exception to the exclusionary rule to allow the data to be admitted in spite of recent decisions.[46]

Lastly, some courts are delaying resolution of the questions presented by these cases pending further guidance by the U.S. Supreme Court. The District Court in *United States v. Graham*[47] heldthat the defendants did not have a legitimate expectation ofprivacy in historical cell site location records, and that, in any event, thegood-faith exception to the exclusionary rule applied. The defendants appealed to the Fourth Circuit Court of

---

to protection under Fourth Amendment); United States v. Gordon, 09–153–02 , 2012 WL 8499876 (D.D.C. Feb. 6, 2012) (cell-site information is not protected by the Fourth Amendment because *Smith v. Maryland*, 442 U.S. 735 (1979) is controlling); United States v. Benford, 2:09 CR 86, 2010 WL 1266507 (N.D. Ind. Mar. 26, 2010).

45. *See, e.g.*, *In re* Application of U.S. for an Order Pursuant to 18 USC 2703(d), 964 F. Supp. 2d 674 (S.D.Tex. 2013) (probable cause was required for search of cell site information and government should provide a protocol for addressing Fourth Amendment privacy rights of innocent cell phone subscribers); United States v. Espudo, 954 F. Supp. 2d 1029 (S.D. Cal. 2013) (need probable cause and a warrant to obtain real-time cell site location; even without warrant, real-time cell site location data admissible under good faith exception); United States v. Powell, 943 F. Supp. 2d 759, 776-77 (E.D. Mich. 2013) ("Court finds that when the government requests authorization to engage in long-term, real-time tracking of an individual's movements via his or her cell phone, the situation reaches past the law set forth in *Skinner*, and Fourth Amendment concerns are implicated."); In re U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 118–20 (E.D.N.Y. 2011); In re Application of U.S. for an Order Authorizing Release of Historical Cell-Site Information, 736 F. Supp. 2d 578, 579 (E.D.N.Y. 2010);.In the Application of the United States of America For and [sic] Order: (1) Authorizing the Use of a Pen Register and Trap and Trace Device; (2) Authorizing Release of Subscriber and Other Information; and (3) Authorizing the Disclosure of Location–Based Services, 727 F. Supp. 2d 571, 583–84 (W.D. Tex. 2010). *See also* United States v. Martinez-Rodriquez, No. 3:13–cr–00452–JO, 2014 WL 127072 (D. Or. Jan. 10, 2014) (upheld cell phone location tracking based on probable cause of warrant); United States v. Acosta, S1 12 Cr. 224, 2013 WL 1890337, at *7 (S.D.N.Y. May 6, 2013) ("It is not necessary for this Court to determine whether the Government is required to demonstrate probable cause for the issuance of a GPS tracking warrant [for GPS data associated with a cell phone]. Assuming *arguendo* that such a requirement exists, it was amply met here."); *In re* Application of U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), CR. C–12–755M, 2012 WL 3260215 (S.D. Tex. July 30, 2012).

46. United States v. McCullough, 523 Fed.App'x. 82, 84 (2d Cir. 2013) (officers reasonably acted in reliance on SCA when they compelled cellular service provider to produce records that reflected location of defendant's cell phone, and thus records were admissible in defendant's prosecution pursuant to the good faith exception to the exclusionary rule where there was no "case law predating government's acquisition of records that rendered 18 U.S.C. § 2703(c) and (d) 'clearly unconstitutional' when applied to the acquisition of historic cell-site records"); United States v. Espudo, 954 F. Supp. 2d 1029 (S.D. Cal. 2013) (need probable cause and a warrant to obtain real-time cell site location; even without warrant, real-time cell site location data admissible under good faith exception); United States v. Jones, 908 F. Supp. 2d 203 (D.D.C. 2012); United States v. Graham, 846 F. Supp. 2d 384 (D. Md. 2012); United States v. Herron, 10–CR–0615 NGG, 2014 WL 824291 (E.D.N.Y. March 3, 2014) (court denied motion to suppress based on good faith exception).

47. 846 F. Supp. 2d 384, 406 (D. Md. 2012).

Appeals[48] but on January 23, 2014, the Fourth Circuit issued an order that read: "These cases were scheduled to be heard at oral argument on January 30, 2014. The court removes these cases from the oral argument calendar and places them in abeyance pending the Supreme Court's decision in *United States v. Wurie*, No. 13-212, (cert. granted January 17, 2014) and *Riley v. California*, No. 13-132 (cert. granted January 17, 2014). The parties shall immediately notify this court in writing of the Supreme Court's decision."[49]

On June 25, 2014, the Supreme Court issued its opinions in the *Wurie* and *Riley* cases.[50] Both cases involved the applicability of the search incident to arrest exception to the warrant requirement to searches of cell phones.[51] The Court unanimously ruled that police need a search warrant based upon probable cause to search the cell phones of arrested individuals.[52] The Court stated, *inter alia*, the following:

Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life[.]'. . . The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.[53]

Will the *Riley* decision empower lower courts to conclude that a warrant is necessary for cell site location information? Will it motivate the Supreme Court to grant certiorari in the next cell site location case?

In the recent past, the Court has demonstrated a desire to narrow the scope of its decisions because of the changing nature of technology. In *City of Ontario, California v. Quon*,[54] the Court considered whether a government employer violated the rights of an employee when the employer read text messages sent and received on a pager the employer issued to the employee.[55] The Court assumed, for argument's sake only, that the employee had a reasonable expectation of privacy over text

---

48. Graham, 846 F. Supp. 2d 384 (D.MD. 2012), appeal docketed, No. 12-4659 (4th Cir. Aug. 22, 2012).
49. *Id.*
50. Riley v. California, 134 S.Ct. 2473 (2014).
51. *Id.* at 2480-82.
52. *Id.* at 2495.
53. *Id.* at 2494-95.
54. 560 U.S. 746 (2010).
55. *Id.* at 750.

messages sent on the government-provided pager.[56] Nevertheless, the Court decided that the conduct of the employer, *under the circumstances*, was reasonable.[57] The *Quon* Court, however, refused to conclude that there is always a reasonable expectation of privacy over electronic communication devices:

The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear. . . .

Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior. . . A broad holding concerning employees' privacy expectations vis-à-vis employer-provided technological equipment might have implications for future cases that cannot be predicted. It is preferable to dispose of this case on narrower grounds.[58]

In his *Quon* concurrence, however, Justice Scalia challenges the Court to confront the difficult questions presented by changes in technology:

Applying the Fourth Amendment to new technologies may sometimes be difficult, but when it is necessary to decide a case we have no choice. The Court's implication. . . that where electronic privacy is concerned we should decide less than we otherwise would (that is, less than the principle of law necessary to resolve the case and guide private action)—or that we should hedge our bets by concocting case-specific standards or issuing opaque opinions—is in my view indefensible. The-times-they-are-a-changin' is a feeble excuse for disregard of duty.[59]

Riley certainly represents a step by the Court to take on the tough cases. Which Court will we see – *Quon* or *Riley* – if and when it decides to look at cell site location information?

Over the last several years, the Court has issued decisions that find ways to permit the jury to consider the evidence in Fourth Amendment suppression cases. In *Hudson v. Michigan*,[60] the Court declared that, because there are other remedies like a civil lawsuit and internal discipline of officers, suppression is not the proper remedy for a "knock and

---

56. *Id.* at 760.

57. *Id.* at 761-65.

58. *Id.* at 759-60. Notably, the Fifth Circuit in *In re Application* appeared to follow the lead of the U.S. Supreme Court: "Recognizing that technology is changing rapidly, we decide only the narrow issue before us. Section 2703(d) orders to obtain *historical* cell site information for specified cell phones at the points at which the user places and terminates a call are not categorically unconstitutional." 724 F.3d 600, 615 (5th Cir. 2013) (emphasis in original).

59. 560 U.S. at 768.

60. 547 U.S. 586 (2006).

announce" violation.[61] In *Herring v. United States*,[62] the Court held that "the jury should not be barred from considering all the evidence" obtained pursuant to a Fourth Amendment error – in this case, an arrest based on a warrant that wrongly appeared as active in a police department computer database – when the error "was the result of isolated negligence attenuated from the arrest."[63] Many lower courts have followed the lead of the Supreme Court – issuing "narrow" decisions and using exceptions to the exclusionary rule to permit the usage of cell tower information at trial.[64] Given this trend, it is likely the Court would follow a similar approach with cell site location information.

IV. CELL PHONE USERS HAVE ALTERNATIVES

In 2012, Congressman Ed Markey released a collection of letters he received from major phone carriers in response to a query he sent out requesting data on how often the carriers reveal phone users' data to the government.[65] According to an article in Forbes, "[t]he New York Times counts a total of 1.3 million requests for users' information in the last year based on Markey's data."[66] Without a doubt, the government is interested in how people use their phones.

What choices do cell phone users have when trying to maintain privacy? Some promote the virtues of using a "dumb phone" to find a way to get off the grid.[67] While not without shortcoming (e.g., my favorites apps don't work!), users can turn off the tracking features on their smart phones.[68] Or one could just turn the phone off – a viable option?[69] A user

---

61. *Id.* at 594.
62. 555 U.S. 135 (2009).
63. *Id.* at 137.
64. *See supra* notes 45-46, 58, and accompanying text.
65. Andy Greenberg, *Here's How Often AT&T, Sprint, and Verizon Each Hand Over Users' Data To the Government*, FORBES (July 9, 2012, 11:00 AM), http://www.forbes.com/sites/andygreenberg/2012/07/09/by-the-numbers-heres-how-often-att-sprint-and-verizon-hand-over-users-data-to-the-government/.
66. *Id. See also* Ms. Smith, *Cops Asked Wireless Carriers for Over 1.1 Million Customer Cellphone Records In 2012*, NETWORK WORLD (Dec. 9, 2013, 2:35 PM), http://www.networkworld.com/community/blog/cops-asked-wireless-carriers-over-11-million-customer-cellphone-records-2012.
67. Laura Newcomer, *Why I Still Use a Dumb Phone (and Have No Plan to Change)*, LIFEHACKER (July 18, 2013, 2:00 PM), http://lifehacker.com/why-i-still-use-a-dumb-phone-and-have-no-plan-to-chang-828910425.
68. *Disable tracking settings on phone: How your phone's operating system buries ad, tracking settings*, ABC15.COM (Nov. 27, 2013), http://www.abc15.com/news/science-tech/disable-tracking-settings-on-phone-how-your-phones-operating-system-buries-ad-tracking-settings (last updated Nov. 27, 2013).
69. Kim Komando, *Can You Spy On a Phone When It Is Turned Off?* USA TODAY (June

can attempt to anonymize one's actions, but some recent research suggests the net effect might not be the anonymity one seeks.[70] Given today's world – with the desire (and often need) to stay connected and informed – one's individual options are limited.

From a legal perspective, what should we do while we wait for the Supreme Court to give guidance? In *In re* Application, the Fifth Circuit pointed out that "cell phone users [who] may reasonably want their location information to remain private"[71] have alternatives. "[T]he recourse for these desires is in the market or in the political process: in demanding that service providers do away with such records (or anonymize them) or in lobbying elected representatives to enact statutory protections."[72] Some service providers may even choose to do this on their own – might that be an effective business strategy?

States like Indiana, Maine and Montana have already passed laws requiring state law enforcement officers to obtain a search warrant (based upon probable cause) in order to retrieve cell site information.[73] Other states – Wisconsin, Tennessee, Minnesota, Missouri, South Carolina, Illinois (and others) – are considering similar legislation.[74] It seems that many states are

---

20, 2014, 7:03 AM), http://www.usatoday.com/story/tech/columnist/komando/2014/06/20/smartphones-nsa-spying/10548601/.

70. Kim Zetter, *Anonymized Phone Location Data Not So Anonymous, Researchers Find*, WIRED (Mar. 27, 2013, 4:10 PM), http://www.wired.com/2013/03/anonymous-phone-location-data/ ("Anonymized mobile phone location data produces a GPS fingerprint that can be easily used to identify a user based on little more than tracking the pings a phone makes to cell towers, a new study shows.").

71. *In re* United States for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013).

72. *Id.*

73. Gauthum Nagesh, *States Not Waiting for Congress on GPS Tracking Laws*, ROLL CALL (July 17, 2013), http://www.rollcall.com/news/states_not_waiting_for_congress_on_gps_tracking_laws-226435-1.html. *See also* Mark Flatten, *EXography: States Passing Laws to Pull the Shades On High-Tech Police Snooping On Mobile Phones, Services*, WASH. EXAMINER (Apr. 1, 2014, 12:00 AM), http://washingtonexaminer.com/exography-states-passing-laws-to-pull-the-shades-on-high-tech-police-snooping-on-mobile-phones-devices/article/2546576.

74. Jason Stein, *Bill Would Require Warrants for Law Enforcement Tracking of Cellphones*, JOURNAL. SENTINEL (Dec. 8, 2013), http://www.jsonline.com/news/statepolitics/bill-would-require-warrants-for-law-enforcement-tracking-of-cellphones-b99158195z1-234978781.html; *State Lawmaker Wants to Block Police From Cell PhoneTtracking*, WBIR.COM (Dec. 16, 2013, 9:38 PM), http://www.wbir.com/story/tech/2013/12/16/cell-phone-tracking/4046579/; Michael Boldin, *To the Governor's Desk: Illinois Bill to Ban Warrantless Cellphone Tracking Passes Unanimously*, TENTH AMENDMENT CENTER (June 2, 2014), http://blog.tenthamendmentcenter.com/2014/06/to-the-governors-desk-illinois-bill-to-ban-warrantless-cellphone-tracking-passes-unanimously/; Michael Boldin, *To the Governor's Desk: Minnesota Legislature Bans Warrantless Cellphone Tracking*, TENTH AMENDMENT CENTER (May 14, 2014), http://blog.tenthamendmentcenter.com/2014/05/to-the-governors-desk-minnesota-legislature-bans-warrantless-cellphone-tracking/; Faith Braverman, *South Carolina*

not waiting for the Supreme Court or Congress to act.[75]

Moreover, states are always free to interpret their own laws, i.e., set the "ceiling" – even if the laws are worded similarly to the United States Constitution – in ways that provide their citizens with greater protection from searches by police than the "floor" as set by U.S. Supreme Court case law. A good example lies in the case of *Michigan Department of State Police v. Sitz.*[76] In *Sitz*, the U.S. Supreme Court ruled that a Michigan State Police sobriety checkpoint was constitutionally permissible under the Fourth Amendment to the U.S. Constitution.[77] On remand, however, the Michigan Supreme Court[78] ruled that such checkpoints were not constitutionally permissible under the Michigan Constitution.[79] Essentially, states are free to give their citizens greater "protection" from intrusive police conduct.

In *State v. Earls*,[80] the New Jersey Supreme Court also set a higher "ceiling," holding that under the New Jersey Constitution, police were required to obtain a search warrant supported by probable cause in order to obtain cell site information from the defendant's cellular service provider.[81] While several states are finding no reasonable expectation of privacy in cell site location information,[82] other states, such as Massachusetts and

---

House Votes to Ban Warrantless Cell Phone Tracking, THE LIBERTARIAN REPUBLIC (May 7, 2014), http://thelibertarianrepublic.com/south-carolina-house-votes-ban-warrantless-cell-phone-tracking/#axzz35DLeJkuH; Hayes Brown, *Missouri Moves to Ban Use Of Cellphone Tracking Without Warrants,* THINK PROGRESS (March 16, 2014), http://thinkprogress.org/justice/2014/03/16/3410441/missouri-moves-to-ban-use-of-cellphone-tracking-without-warrants/. *See also* Mark Flatten, EXography: States Passing Laws to Pull the Shades on High-Tech Police Snooping on Mobile Phones, Devices, WASH. EXAMINER (April 1, 2014), http://washingtonexaminer.com/exography-states-passing-laws-to-pull-the-shades-on-high-tech-police-snooping-on-mobile-phones-devices/article/2546576.

75. Several bills have been introduced in Congress over the last couple of years but none have been enacted into law. *See, e.g.*, Location Privacy Protection Act of 2014, S. 2171, 113th Cong. (2014) (this bill would require a "covered entity" (defined as "a nongovernmental individual or entity") to get consent before tracking an electronic device); American Privacy Protection Act, H.R. 3920, 113th Cong. (2014); Online Communications and Geolocation Protection Act, H.R. 983, 113th Cong. (2014); GPS Act, H.R. 1312, 113th Cong. (2014).

76. Michigan Department of State Police v. Sitz, 496 U.S. 444 (1990).

77. *Id.* at 447.

78. Sitz v. Dept. of State Police, 443 Mich. 744 (1993).

79. *Id.* at 747. Notably, the words of the relevant provision of the Michigan Constitution are very similar to those of the Fourth Amendment, but that makes no difference in a state's ability to set a higher ceiling.

80. State v. Earls, 70 A.3d 630 (N.J. 2013).

81. *Id.* at 632.

82. *See, e.g.*, State v. Taylor, No. 25764, 2014 WL 2700846 (Ohio Ct. App. 2014) (no legitimate expectation of privacy in the pings emitted from cell phone); McCowan v. State, 10 N.E.3d 522 (Ind. Ct. App. 2014) (no violation under Article I, Section 11, Indiana Constitution). *See also* Reynolds v. Commonwealth, No. 2179–12–4, 2014 WL 2187774 (Va. Ct. App. 2014)

Pennsylvania, are following the lead of New Jersey.[83]

Alternative remedies may even exist in the courtroom. In *United States v. Evans,*[84] the trial judge questioned – from a Federal Rules of Evidence perspective – the reliability of cell site evidence and analysis through the testimony of a federal agent. In *Evans*, the government proposed calling a special agent "to testify about the operation of cellular networks and how to use historical cell site data to determine the general location of a cell phone at the time of a particular call. Applying a theory called 'granulization,' [the agent] propose[d] to testify that calls placed from Evans's cell phone during the course of the conspiracy could have come from the building where the victim was held for ransom."[85]

After examining Federal Rule of Evidence 702 and *Daubert v. Merrell Dow Pharmaceuticals, Inc.*,[86] the court stated: "Given that multiple factors can affect the signal strength of a tower and that [the special agent's] chosen methodology has received no scrutiny outside the law enforcement community, the court concludes that the government has not demonstrated that testimony related to the granulization theory is reliable."[87] In the end, the court held the agent could not "testify concerning the theory of granulization, which the court finds to be unreliable."[88]

While more courts have been willing to admit testimony on cell phone tracking,[89] some authorities have called cell tower tracking a "'junk science'

(affirming "specific and articulable facts" basis for court order).

83. *See, e.g.,* Commonwealth v. Augustine, 4 N.E.3d 846 (Mass. 2014) (warrant required to track cell site location information covering a 2-week period); Commonwealth v. Rushing, 71 A.3d 939 (Pa. 2013) (defendant had legitimate expectation that government could not surreptitiously track his real time location via his cell phone signal, police were required to make a showing of probable cause in order to obtain real time cell site location data, exigent circumstances existed, as required to justify officers' obtaining real time cells site information data).

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

85. *Id.* at 951.

86. Daubert v. Merrell Dow Pharms., Inc., 509 U.S. 579 (1993).

87. Evans, 892 F.Supp.2d at 957.

88. *Id* at 954. The court did state that the agent could "provide lay opinion testimony concerning (1) the call data records obtained for Evans's phone and (2) the location of cell towers used by Evans's phone in relation to other locations relevant to the crime...."

89. *See, e.g.,* United States v. Machado-Erazo, 950 F.Supp.2d 49, 57 (D.D.C. 2013) ("the Court finds that S.A. Magnuson's proposed expert 'testimony is based on scientific knowledge' and is admissible under *Daubert.*"); United States v. Jones, 918 F.Supp.2d 1, 5-6 (D.D.C. 2013) ("Overall, the Court is persuaded that Agent Eicher's opinions relating to the location of the cell towers, the sectors used for each call, and the general location where the cell phones must have been when they connected to each tower, are the product of reliable principles and methods. Agent Eicher's reports demonstrate that he has reliably applied that methodology to the facts of this case, and thus his proffered testimony meets the reliability standards required under Rule 702 and *Daubert.*"); United States v. Davis, No. 11–60285–CR, 2013 WL 2156659 (S.D. Fla. May 17, 2013) (testimony allowed "concerning the areas most likely to have been contained in the sectors

that should never be admitted in any court for any reason."[90] " 'It's not really junk science, it's misinterpreted science,' [according to] forensic expert Larry Daniel of Raleigh, N.C., who has consulted and testified for the prosecution and the defense in numerous cases, including a capital murder case in Fayetteville, N.C., where police claimed the cell-tower data showed a man was at the crime scene. 'It is useful and can be used. But in the hands of a novice, this is dangerous science.' "[91] However it is labeled, it certainly gives the parties something to argue about at trial.[92]

V. CONCLUSION

Will the U.S. Supreme Court eventually reconsider – and reject – the third party doctrine? Might the Court find that, in some situations, the tracking is so comprehensive (essentially the WHOLE of one's movements) that it is unreasonable and, hence, unconstitutional, under the Fourth Amendment? Given the uncertainty, courts will likely continue to look for narrow ways to decide their cases. While we wait for the Court and/or Congress to provide direction, people have choices. Depending on one's state, some of the choices may be better than others.

Meanwhile, law enforcement officers will persist in using cell site location data to pursue criminal defendants. Especially since courts don't suppress the defendant – even if other evidence is suppressed.

---

being serviced by the cell towers used by the cell phones that made calls during the events relevant to the allegations in this case"); United States v. Eady, No. 2:12–cr–00415–DCN–3, 2013 WL 4680527(D.S.C. Aug. 30, 2013) ("the court finds that his proposed testimony is the product of reliable principles and methods and that he has reliably applied those principles and methods to the facts of this case"); Commonwealth v. Collins, 31 Mass.L.Rptr. 437 (2013) (testimony reliable on "very general idea as to where the cell phone in question was located").

90. Mark Hansen, *Prosecutors' Use of Mobile Phone Tracking Is 'Junk Science,' Critics Say*, A.B.A. J. (June 1, 2013), http://www.abajournal.com/magazine/article/prosecutors_use_of_mobile_phone_tracking_is_junk_science_critics_say/.

91. Tom Jackman, *Experts Say Law Enforcement's Use of Cellphone Records Can Be Inaccurate*, WASH. POST (June 27, 2014), http://www.washingtonpost.com/local/experts-say-law-enforcements-use-of-cellphone-records-can-be-inaccurate/2014/06/27/028be93c-faf3-11e3-932c-0a55b81f48ce_story.html?tid=sm_fb.

92. Judge Herbert B. Dixon, Jr., *Scientific Fact or Junk Science? Tracking a Cell Phone without GPS*, 53 THE JUDGES' J. 1 (2014), *available at* http://www.americanbar.org/publications/judges_journal/2014/winter/scientific_fact_or_junk_science_tracking_a_cell_phone_without_gps.html. *See also* Aaron Blank, *The Limitations and Admissibility of Using Historical Cellular Site Data to Track to Track the Location of a Cellular Phone,* 18 RICH. J. L. & TECH. 3 (2011); U.S. DEP'T. OF JUSTICE, *Obtaining and Admitting Electronic Evidence*, 59 U.S. ATT'YS BULL. 6, (2011), *available at* http://www.justice.gov/usao/eousa/foia_reading_room/usab5906.pdf.

C

Only the Westlaw citation is currently available.

United States District Court,
C.D. California.
U.S.A.
v.
Dominic DORSEY, Reginald Bailey, Defendants.

No. CR 14–328–CAS.
Signed Feb. 23, 2015.

David Herzog, Justin Rhoades, for U.S.

Philip Deitch, for Defendant Dominic Dorsey.

Jay Lichtman, for Defendant Reginald Bailey.

Proceedings: VARIOUS DEFENSE MOTIONS
CHRISTINA A. SNYDER, Judge.

***1** Catherine Jeang, Deputy Clerk.

Lisa Gonzalez, Court Reporter/Recorder, Tape No.

I. INTRODUCTION AND BACKGROUND

Defendants Dominic Dorsey ("Dorsey") and Reginald Bailey ("Bailey") are charged with one count of conspiracy to interfere with interstate commerce by robbery, in violation of the Hobbs Act, 18 U.S.C. § 1951(a); five substantive Hobbs Act robbery counts; and five counts of possessing, using, carrying, and brandishing a firearm in furtherance of a crime of violence, in violation of 18 U.S.C. § 924(c)(1)(A)(ii). *See* Dkt. No. 1. Defendants are alleged to have robbed numerous gas stations, a pizza restaurant, and a bank as part of a series of "Cowboy Gun Bandit" robberies in the fall of 2013. *See generally id.* On February 23, 2015, the Court held a hearing on various defense motions. After considering the parties' arguments, the Court finds and concludes as follows.

II. DEFENDANTS' MOTIONS TO DISMISS INDICTMENT ON JURISDICTIONAL GROUNDS

On December 24, 2014, Bailey filed a motion to dismiss the indictment on the ground that the charged robberies did not have a sufficient effect on interstate commerce to satisfy the jurisdictional element of the Hobbs Act. Dkt. No. 42. On January 13, 2015, Dorsey joined in that motion, adding limited briefing of his own. Dkt. No. 51. The government filed a consolidated opposition on January 26, 2015. Dkt. No. 63. Bailey and Dorsey filed separate replies on February 9, 2015. Dkt. Nos. 67, 74. For the reasons that follow, the motions are **DENIED.**

A. Legal Standards

1. Pretrial Motion to Dismiss

On a pretrial motion to dismiss an indictment, a court "must presume the truth of the allegations in the charging instrument[ ]." *United States v. Jensen,* 93 F.3d 667, 669 (9th Cir.1996). "[T]he issue in judging the sufficiency of the indictment is whether the indictment adequately alleges the elements of the offense and fairly informs the defendant of the charge, not whether the Government can prove its case." *United States v. Buckley,* 689 F.2d 893, 897 (9th Cir.1982). The prosecution "need not allege ... supporting evidence, but only the 'essential facts necessary to apprise a defendants of the crime charged.' " *Id.* (quoting *United States v. Markee,* 425 F.2d 1043, 1047–48 (9th Cir.1970)). Morever, a defendant " 'may not properly challenge an indictment, sufficient on its face, on the ground that the allegations are not supported by adequate evidence.' " *Jensen,* 93 F.3d at 669 (quoting *United States v. Mann,* 517 F.2d 259, 267 (5th Cir.1975)). Accordingly, the court " 'should not consider evidence not appearing on the face of the indictment.' " *Id.* (quoting *United States v. Marra,* 481 F.2d 1196, 1199–1200 (6th Cir.1973)).

2. The Hobbs Act's Jurisdictional Element

The Hobbs Act provides in part:

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

> Whoever in any way or degree obstructs, delays, or affects commerce or the movement of any article or commodity in commerce, by robbery or extortion or attempts or conspires so to do, or commits or threatens physical violence to any person or property in furtherance of a plan or purpose to do anything in violation of this section shall be [punished] ....

***2** 18 U.S.C. § 1951(a). The statute defines "commerce" as commerce within the District of Columbia or other federal land, and "all commerce between any point in a State ... and any point outside thereof; all commerce between points within the same State through any place outside such State; and all other commerce over which the United States has jurisdiction." *Id.* § 1951(b)(3). Both the Supreme Court and the Ninth Circuit have "emphasized the broad reach of the 'affects commerce' language of the Act." *United States v. Lynch,* 437 F.3d 902, 909 (9th Cir.2006) (en banc) (per curiam); *see United States v. Culbert,* 435 U.S. 371, 373 (1978) ("These words do not lend themselves to restrictive interpretation; as we have recognized, they 'manifest ... a purpose to use all the constitutional power Congress has to punish interference with interstate commerce by extortion, robbery or physical violence.' " (quoting *Stirone v. United States,* 361 U.S. 212, 214 (1960))).

The Ninth Circuit has held that the government need only prove that a defendant's acts had "a *de minimis* effect on interstate commerce to support a Hobbs Act violation." [FN1] *United States v. Atcheson,* 94 F.3d 1237, 1241 (9th Cir.1996). "The interstate nexus requirement is satisfied 'by proof of a probable or potential impact' on interstate commerce." *Lynch,* 437 F.3d at 909 (quoting *United States v. Huynh,* 60 F.3d 1386, 1389 (9th Cir.1995)). Accordingly, convictions under the Hobbs Act have been "consistently upheld"

> FN1. Defendants submit that because "the commercial activities at issue were intrastate, the 'substantially affects' [commerce] test of [United *States v. Lopez,* 514 U.S. 549 (1995)] and not the de minimis test of Atcheson would be applicable." Dkt. No. 42 at 6. This question-begging argument is unpersuasive: the *de minimis* test is what determines whether a charged Hobbs Act violation involves interstate, rather than solely intrastate, activities. And the Ninth Circuit has clearly stated that *Lopez* "did not require a change in the *de minimis* standard" applied to the Hobbs Act's jurisdictional element. *Lynch,* 437 F.3d at 909; *accord United States v. Boyd,* 480 F.3d 1178, 1179 (9th Cir.2007) (per curiam).

> even where the connection to interstate commerce was slight. *See, e.g., United States v. Pascucci,* 943 F.2d 1032, 1035 (9th Cir.1991) (defendant threatened to deliver embarrassing audio tapes to his victim's employer, a corporation engaged in interstate commerce); *United States v. Hanigan,* 681 F.2d 1127, 1130–31 (9th Cir.1982) (defendant robbed three undocumented alien farm workers, affecting the movement of labor across borders); *United States v. Phillips,* 577 F.2d 495, 501 (9th Cir.1978) (defendant's extortion "threatened the depletion of resources from a business engaged in interstate commerce").
> *Lynch,* 437 F.3d at 909 (citation formatting altered) (quoting *Atcheson,* 94 F.3d at 1243).

B. Application

As noted above, the indictment charges robberies of three gas stations, a Papa John's pizza restaurant, and a Citibank branch, as well as a conspiracy to commit the aforementioned robberies and related gun crimes. The indictment alleges that defendants obtained approximately $600 from the Papa John's, between $55 and $1,200 each from several gas stations, and over $55,000 from the Citibank. Dkt. No. 42 Ex. A at 3–5. The indictment charges that defendants' acts "obstructed, delayed, and affected commerce and the movement of articles and commodities in commerce by robbery." *Id.* at 6. The indictment further alleges that the in-

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

ventories of Papa John's and the three gas stations "traveled in interstate commerce," and that Citibank is a "national banking chain that operates in interstate commerce." *Id.* at 6–10. Under the *de minimis* standard cited above, and on the limited review a court conducts on a pretrial motion to dismiss, these jurisdictional allegations are more than sufficient. FN2

FN2. The Court notes that "[t]here is no requirement that a Hobbs Act indictment allege specific facts establishing an impact on interstate commerce." *United States v. Bellamy,* 521 F. App'x 590, 592 (9th Cir.2013) (unpublished) (citing *United States v. Woodruff,* 50 F.3d 673, 676 (9th Cir.1995) ("Although the indictment contained no facts alleging how interstate commerce was interfered with, and did not state any theory of interstate impact, prior decisions of our court compel the conclusion that the indictment was sufficient.")). Accordingly, defendants' entire argument may simply be non-cognizable on a motion to dismiss an indictment. Out of an abundance of caution, the Court nevertheless addresses its substance.

***3** Defendants dispute that allegations that the robbed businesses bought and sold inventory from other states satisfy the jurisdictional element, arguing that this case "involves 'strictly intrastate robber[ies] which caused only a speculative indirect effect on a business engaged in interstate commerce.' " Dkt. No. 42 at 8 (quoting *Lynch,* 437 F.3d at 910). But defendants cite no case dismissing a Hobbs Act indictment under similar circumstances—or, indeed, under *any* circumstances. FN3 This is unsurprising because "[r]obbery of an interstate business ... typically constitutes sufficient evidence to satisfy the Hobbs Act's interstate commerce element." *United States v. Rodriguez,* 360 F.3d 949, 955 (9th Cir.2004). Cases abound in which appellate courts have upheld Hobbs Act convictions based on the sort of interstate commerce nexus defendants maintain is insufficient. *See United States v. Ridgley,* 511 F. App'x 654, 654–55 (9th Cir.2013) (unpublished) (conviction for robbery of two pizza deliveryman upheld where the restaurants "engaged in interstate commerce because their supplies and ingredients came from out of state"); *United States v. Sutton,* 337 F.3d 792, 796 n. 2 (7th Cir.2003) (jurisdictional requirement met by similar robberies because the "aggregate transactions of banks, restaurants and retail stores" have a substantial effect on interstate commerce, "even if the specific events prosecuted do not, themselves, have a substantial effect on interstate commerce"); *see also United States v. Dean,* 517 F.3d 1224, 1228 (11th Cir.2008) (evidence that defendants stole less than $4,000 from "a bank with interstate branches ... open to out of state customers was sufficient to establish an effect on commerce"); *United States v. Jiminez–Torres,* 435 F.3d 3, 9 (1st Cir.2006) (sufficient that gas station in Puerto Rico purchased gasoline from the Virgin Islands). Indeed, in an unpublished disposition, the Ninth Circuit recently reversed a district court's dismissal of a Hobbs Act indictment where the defendant had robbed only *one* convenience store, for $135. *United States v. Bellamy,* 521 F. App'x 590, 591 (9th Cir.2013). The court explained that the "fact that Bellamy robbed a convenience store that obtains its inventory from out of state sources establishes the requisite impact on interstate commerce." FN4 *Id.* Defendants' argument to the contrary is without merit.

FN3. At oral argument, Bailey's counsel contended that *United States v. Collins,* 40 F.3d 95 (5th Cir.1994), is such a case. But the *Collins* court did not hold that a Hobbs Act indictment should have been dismissed; rather, it determined that insufficient evidence of an interstate commerce nexus had been introduced at trial to support one of the two Hobbs Act robberies of which the defendant was convicted. *Id.* at 99–101. Notably, *Collins* only reversed the defendant's conviction for robbing an indi-

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

vidual in his home, and drew a number of distinctions between robberies of "business or similar entities engaged in interstate commerce" on the one hand, and individuals on the other hand. *Id.* at 99–100. It was in the context of a robbery of an individual that the *Collins* court articulated the "speculative indirect effect on a business engaged in interstate commerce" language on which Bailey relies. In fact, the *Collins* court *affirmed* the defendant's Hobbs Act conviction for robbing a single Denny's restaurant. *Id.* at 101. *Collins* weakens, not strengthens, defendants' motions to dismiss.

FN4. In reply briefing on this and other motions, Bailey argues that the government's citations to recent unpublished Ninth Circuit cases should be ignored as lacking in any authority, persuasive or otherwise. Bailey correctly points out that unpublished dispositions "are not precedent" except under circumstances not relevant here. Ninth Circuit R. 36–3(a). However, unpublished decisions issued on or after January 1, 2007 may be cited "as persuasive authority pursuant to Ninth Circuit Rule 36–3(b)." *Uche–Uwakwe v. Shinseki,* 972 F.Supp.2d 1159, 1189 n. 14 (C.D.Cal.2013); *Nuh Nhuoc Loi v. Scribner,* 671 F.Supp.2d 1189, 1201 n. 10 (S.D.Cal.2009) ("Although still not binding precedent, unpublished decisions [postdating 2006] have persuasive value and indicate how the Ninth Circuit applies binding authority."). Bailey's cited authority to the contrary, *Sorchini v. City of Covina,* 250 F.3d 706, 708–09 (9th Cir.2001) (per curiam), was decided in 2001, when Rule 36–3(b) only permitted unpublished dispositions to be cited for "factual purposes." After the rule was amended, the Ninth Circuit expressly held: "as of January 1, 2007, we must now allow parties to cite even unpublished dispositions and unpublished orders *as persuasive authority.*" *Animal Legal Def. Fund v. Veneman,* 490 F.3d 725, 733 (9th Cir.2007) (emphasis added). To the extent that the Court cites unpublished decisions in this order, it does so for their persuasive value.

Defendants also argue that "due to the anticipated absence of proof on the interstate commerce element of the Hobbs Act charges, those charges should be dismissed so that the case can be prosecuted in state court," and that the gun charges predicated on those Hobbs Act charges should be dismissed as well. Dkt. No. 42 at 8–9. But as noted above, a defendant "may not properly challenge an indictment, sufficient on its face, on the ground that the allegations are not supported by adequate evidence." *Jensen,* 94 F.3d at 669 (internal quotation marks omitted).[FN5]

FN5. Contrary to Dorsey's argument, Federal Rule of Criminal Procdure 12 does not suggest otherwise. Rule 12 states that a "party may raise by pretrial motion any defense ... that the court can determine without a trial on the merits." Fed.R.Crim.P. 12(b)(1). A court cannot determine the sufficiency of the evidence supporting the jurisdictional element of charged Hobbs Act violations without a trial. *See Jensen,* 93 F.3d at 669 (" 'There is no summary judgment procedure in criminal cases. Nor do the rules provide for a pre-trial determination of the evidence.' " (quoting *United States v. Critzer,* 951 F.2d 306, 307 (11th Cir.1992) (per curiam))).

***4** Because the indictment sufficiently alleges Hobbs Act violations and defendants' arguments for dismissal run counter to settled law, the Court **DENIES** both defendants' motion to dismiss the indictment.

III. DEFENDANTS' MOTION TO SUPPRESS PHONE AND CELL SITE RECORDS FROM

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

STATE SEARCH WARRANT

On December 24, 2014, Bailey filed a motion to suppress phone and cell site records obtained pursuant to state court orders issued on or about November 6 and November 14, 2013. Dkt. No. 43. Dorsey joined in the motion on February 9, 2015. Dkt. No. 54. The government filed a consolidated opposition on January 26, 2015, and Bailey replied on February 9, 2015. Dkt. Nos. 59, 72. For the reasons that follow, the motion is **DENIED.**

A. Background

On November 6, 2013, Los Angeles Superior Court Judge Cathryn Brougham issued a court order concerning certain records related to a cellular telephone account associated with the number (213) 503–5495 (the "503" number). Dkt. No. 43 Ex. A. The order approved an application by the Los Angeles County Sheriff's Department ("LASD") made "pursuant to Title 18, United States Code Sections 2703(c), 2703(d), 3122, and 3123," and was issued pursuant to 18 U.S.C. §§ 2703(c)(1)(B) and 2703(d). *Id.* at 1–2. The Superior Court ordered Verizon Wireless (as well as any other telecommunications carrier that provides service to the 503 number due to roaming agreements or changes in service) to provide certain information for a time period beginning September 1, 2013, and continuing for thirty days after issuance of the order. *Id.* at 1. Specifically, the order covered:

> • **Subscriber/Account Information,** including but not limited to: Name, address, driver's license number, social security number, alternate telephone numbers, payment method, account notes, application information, billing statements, activation/suspension dates, make/model of handset ... [and various forms of] equipment identifying information.
>
> • **Call Detail Records with Cell site Location** for the aforementioned time period. The Call Detail Records should include all inbound and outbound calls, direct dispatched number(s), whether published or non-published, blocked or unblocked, including SMS and MMS text messages on the Target Telephone(s). The cell site information requested includes, but is not limited to, the location of cell site/sector, beginning and ending location of the Target Telephone(s), Location Area Code (LAC), Cellular ID (CID), switch information, latitude, longitude, tower orientation, azimuth, direction and strength of signal.

Id. The order also provided that, upon request from law enforcement, "any and all telecommunications carriers subject to regulation by the Federal Communications Commission ... shall provide" similar information or "initate a signal ... to determine the location of the subject's mobile device ... at five (5) minute intervals for a thirty (30) day period from the date this order was signed by the Court." *Id.* at 2. The order prohibited law enforcement agencies acting under authority of the order from intercepting the contents of any communications. *Id.* at 3.

***5** The aforementioned order was supported by an LASD detective's affidavit representing that she and her partner had been investigating a series of robberies that occurred between November 18, 2012 and October 26, 2013. [FN6] *Id.* at 5. She averred that "the robberies appear to be committed by the same individuals" because of similarities in involved clothing, weapon, style of robbery, and a getaway vehicle. She described the two suspects as (1) "Male Black, mid 30's, approximately 6'00", 200 pounds" and (2) "Male Black, 5' 05–5'08", 160 pounds," and noted that in each robbery the suspects "covered their face[s] with bandanas." The detective identified a vehicle used in the robberies as belonging to Jacqueline Martin ("Martin"), who she indicated was "believed to be the driver of the suspect vehicle in some of the robberies" and who "has a child with [Dorsey], who matches the first suspect's description." *Id.*

> FN6. The Court has excised from its discussion and consideration of this and other affidavits supporting search warrants certain evidence obtained from a July 2011 traffic stop, which is the subject of a separ-

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

ate suppression motion that, for reasons discussed in Section VII below, the Court does not rule on at this time.

The affidavit states that the detective had located a cellular telephone number for Martin through "public records and ... a contact number ... Martin had previously provided." The detective further averred that Bailey "matche[d] the description of the second robbery suspect involved in the series." She also noted that "Bailey's criminal history includes bank robberies." The affidavit states that a detective had observed Dorsey with Bailey on November 5, 2013. The affiant then stated that using "Sheriff's Resources, [she had] located a cell phone number" for Bailey-the 503 number-and had confirmed that the number corresponded to an active Verizon Wireless account. Based on these facts, the affiant requested "a court order to obtain records for" the 503 number and two other numbers not at issue in this motion "to identify any possible further suspects, locations of the persons believed to be involved in the crimes, and identify the persons['] whereabouts." The affiant explained that the requested record would "assist in determining if [the suspects were] involved in the robbery series based on their whereabouts during the time of the robberies." *Id* .

On November 14, 2013, LASD sought and obtained a similar § 2703 order for telephone number (310) 947–7057 (the "947 number"), linked to a Sprint–Nextel account. The application for this order included the same information provided in support of the 503 number order, as well as some additional details, including the license plate number of Martin's car. Dkt. No. 43 Ex. B at 5. The affidavit stated that a Los Angeles Police Department ("LAPD") detective had viewed surveillance video of Dorsey retrieving something from a vehicle at an impound lot while wearing "what appeared to be the same shoes as the larger suspect in the robbery series." He was accompanied an older black male who matched the second suspect's description in that he (1) appeared to be the same height and weight, (2) wore eyeglasses, (3) had a gray beard (as compared to a "salt and pepper mustache" described in one of the robberies), and (4) "walked exactly like the suspect seen by [the LAPD detective] in the robbery surveillance videos." The affiant stated that the 503 number belonged to Bailey and that records of that account showed "numerous phone calls" to the 947 number. *Id.*

B. Analysis

***6** Defendants characterize the court orders at issue as "search warrants," and cite cases involving the Fourth Amendment standard of probable cause. The government points out, however, that the orders were issued pursuant to 18 U.S.C. § 2703(d), part of the federal Stored Communications Act ("SCA"). *See* Dkt. No. 43 Exs. A, B. That statute provides in part:

> 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 customer of such service (not including the contents of communications) only when the governmental entity—
>
> (A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, using State warrant procedures) by a court of competent jurisdiction; [or]
>
> (B) obtains a court order under subsection (d) of this section ....

18 U.S.C. § 2703(c)(1).[FN7] Subsection (d), referenced above, provides in relevant part:

FN7. "Each option in § 2703(c)(1) is an independently authorized procedure." *In re Application of United States for Order Directing Provider of Elec. Commc'n Serv. to Disclose Records to Gov't,* 620 F.3d 304, 313 (3d Cir.2010) [hereinafter *In re Order Directing Provider].* That is, a govern-

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

> mental entity may either seek a warrant pursuant to subsection (A), apply for a court order pursuant to subsection (B) and § 2703(d), or pursue one of three other procedures authorized in subsections (C) through (E).

A court order for disclosure under subsection (b) or (c) 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.
18 U.S.C. § 2703(d). As noted above, the Superior Court issued the two orders pursuant to § 2703(c)(1)(B) and (d). Moreover, Verizon Wireless and Sprint–Nextel are "provider[s] of electronic communication service" within the meaning of § 2703(c), the information sought was "record[s] or other information pertaining to a subscriber or customer of" such a provider, and the information did not include the "contents of communications." FN8 Therefore, the relevant issues are (1) what standard applies to court orders issued pursuant to § 2703(d), (2) whether the orders in question met that standard, and (3) if the standard was not met, what remedies are available.

> FN8. "[E]lectronic communication service" is defined to mean "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15); *see id.* § 2711(1) (applying the definitions in § 2510 to the provisions of the SCA). "There is no dispute that historical CLSI [cell site location information] is a 'record or other information pertaining to a subscriber ... or customer,' and therefore falls within the scope of § 2703(c)(1)." *In re Order Directing Provider,* 620 F.3d at 307–08; *accord United States v. Martinez,* No. 13CR3560–WQH, 2014 WL 5480686, at *4 (S.D.Cal. Oct. 28, 2014); *United States v. Rigmalden,* No. CR 08–814–PHX–DGC, 2013 WL 1932800, at *10 (D.Ariz. May 8, 2013) ("Verizon clearly is a 'provider of electronic communication service' within the meaning of the SCA, and the historical cell site information ... clearly constitute 'a record or other information pertaining to a subscriber or customer of such service.' "). With regard to wire, oral, or electronic communications, "contents ... includes any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8).

As stated above, the statute pursuant to which the orders were issued requires that law enforcement support an application with "*specific and articulable facts* showing that there are *reasonable grounds* to believe that ... the records sought, are *relevant and material* to an ongoing criminal investigation." 18 U.S.C. § 2703(d) (emphasis added). Below, the Court first explains that the Fourth Amendment does not apply to the orders at issue (and that even if it did, the subscriber information and historical cell site data would likely be admissible under the good faith exception). Second, the Court concludes that the orders at issue met the applicable SCA standard for historical cell site data—and even if they did not, that statute would not permit the Court to suppress any evidence on that basis.

1. The Fourth Amendment Does Not Apply.

Although the Ninth Circuit has not yet ruled on the issue, the vast majority of courts to have done so—including every district court within this circuit—have held that § 2703(d) does not require the government to show probable cause to obtain historical cell site data pursuant to the SCA, and that this lower standard does not violate the Constitution.

***7** The Fifth Circuit recently examined § 2703(d) in the case of *In re Application of United*

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

States for Historical Cell Site Data, 724 F.3d 600 (5th Cir.2013). The court explained that the " 'specific and articulable facts' standard is a lesser showing than the probable cause standard that is required by the Fourth Amendment to obtain a warrant." FN9 *Id.* at 606. The court then held that this lower standard does not violate the Fourth Amendment because a search and seizure does not occur "[w]here a third party collects information in the first instance for its own purposes," and the government later obtains that information through a § 2703(d) order." *Id.* at 610. The court reasoned that when a person " 'communicates information to a third party *even on the understanding that the communication is confidential,* he cannot object if the third party conveys that information or records thereof to law enforcement authorities.' " *Id.* (emphasis in original) (quoting *SEC v. Jerry T. O'Brien, Inc.,* 467 U.S. 735, 743 (1984)). The court concluded that because "cell site information is clearly a business record" and does not reveal the contents of communications, and because a person voluntarily uses a cellular telephone, which necessarily sends a signal to a nearby cell tower, a person has no reasonable expectation of privacy in cell site information. *Id.* at 611–15; *accord United States v. Skinner,* 690 F.3d 772, 777–81 (6th Cir.2012) (no reasonable expectation of privacy in cell site data). The Third Circuit has also decided that § 2703(d) "does not require the traditional probable cause determination," but is instead "governed by the text of § 2703(d)." *In re Order Directing Provider,* 620 F.3d at 313. Examining the legislative history, that court concluded that the "specific and articulable facts" language "creates a higher standard than that required by the pen register and trap and trace statutes," but "less stringent than probable cause." *Id.* at 315. FN10

FN9. *Accord United States v. Cerna,* No. CR 08–0730 WHA, 2010 WL 3749449, at *18 (N.D.Cal. Sept. 22, 2010) (holding that § 2703(d) requires "a lesser showing than that required by the Fourth Amendment").

FN10. A panel of the Eleventh Circuit reached a contrary conclusion in *United States v. Davis,* 754 F.3d 1205, *vacated,* 573 F. App'x 925 (11th Cir.2014). The court rejected the argument that historical cell site data is voluntarily conveyed to the service provider, reasoning that users are unlikely to know that their providers collect and store that information. *Davis,* 754 F.3d at 1216–17. The court concluded that historical "cell site location information is within the subscriber's reasonable expectation of privacy," and the "obtaining of that data without a warrant is a Fourth Amendment violation." *Id.* at 1217. However, the *Davis* decision has since been vacated pending rehearing en banc. 573 F. App'x 925 (11th Cir.2014).

District courts within this circuit have universally decided that historical cell site information may be obtained pursuant to a § 2703(d) order without a showing of probable cause. For example, in *United States v. Martinez,* No. 13CR3560–WQH, 2014 WL 5480686 (S.D.Cal. Oct. 28, 2014), the court found no "reasonable expectation of privacy in the third party business records created and maintained by a cellular phone provider derived from information voluntarily conveyed to the cellular telephone provider." *Id.* at *5 (citing *Smith v. Maryland,* 442 U.S. 735, 742 (1979)). That court denied a motion to suppress cell site data and rejected an argument-similar to the one Bailey makes in his reply brief, Dkt. No. 72 at 6–8–that the Supreme Court's recent decisions in *United States v. Jones,* 132 S.Ct. 945 (2012), and *Riley v. California,* 134 S.Ct. 2473 (2014), compelled a different conclusion. The court reasoned that obtaining historical cell site location information under § 2703(d) does not involve (1) physical intrusion on a defendant's property, (2) real-time tracking, or (3) the search or seizure of a cell phone, communication contents, or other information subject to a reasonable expectation of privacy, so as to implicate *Riley* or *Jones.* *Id.* at *4. Rather, the court found that by using her

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

cell phone, the defendant "voluntarily conveyed numerical information to the telephone company and exposed that information to the cell phone towers in the ordinary course of business." *Id.* at *5.[FN11]

FN11. *See also United States v. Moreno–Navarez,* No. 13–CR–0841–BEN, 2013 WL 5631017, at *1–2 (S.D.Cal. Oct. 2, 2013) (upholding § 2703(d) and noting that "even if the statute were to be held unconstitutional, the good faith exception to the warrant requirement would apply"); United *States v. Salas,* No. CR F 11–0354 LJO, 2013 WL 4459858, at *3 (E.D.Cal. Aug. 16, 2013) ("With regard to the argument applying the ... Fourth Amendment to cell site location information, there is no reasonable expectation of privacy since such records are in the hands of third parties."); *United States v. Rigmalden,* No. CR 08–814–PHX–DGC, 2013 WL 1932800, at *10 (D.Ariz. May 8, 2013) ("Courts have rejected ... arguments that historical cell-site records cannot be obtained under the SCA."); *United States v. Ruby,* No. 12CR1073 WQH, 2013 WL 544888, at *3–7 (S.D.Cal. Feb. 12, 2013) (similar); *United States v. Davis,* Crim No. 10–339–HA, 2011 WL 2036463, at *3 (D.Or. May 24, 2011) ("It is well established that a reasonable expectation of privacy extends only to the content of telephone conversations, not to records that indicate that the conversations occurred. Basic subscriber data which identifies a call's origination, destination, duration, and time of call enjoy no privacy protection because the data is incidental to the use of the telephone, and contains no content information." (citations omitted)).

***8** Jurisprudence involving cellular telephones and related technology is evolving. *See United States v. Guerrero,* 768 F.3d 351, 358 (5th Cir.2014) ("It may be that the 'technology is different' rationale that led the *Riley* Court to treat an arrestee's cell phone differently from his wallet will one day lead the Court to treat historical cell site data in the possession of a cellphone provider differently from a pen register in the possession of a pay phone operator."). But absent contrary direction from a higher court, this Court concludes that the government may constitutionally acquire subscriber information and historical cell site data pursuant to a § 2703(d) order by showing "specific and articulable facts showing that there are reasonable grounds to believe that ... the records sought, are relevant and material to an ongoing criminal investigation."[FN12]

FN12. Bailey that the Court should apply a probable cause standard because the application included a "Statement of Probable Cause" and the order stated that it was "based upon probable cause." Bailey argues that "[t]his was consistent with the statutory language in 18 U.S.C. § 2703(c)(1)(A) which permits a governmental entity to obtain the phone records based on a 'warrant' " using state warrant procedures rather than the process contained in § 2703(d). Dkt. No. 72 at 3–4. But the order expressly states that it was issued "pursuant to 18 U.S.C. 2703(c)(1)(B) and 2703(d)." Dkt. No. 43 Ex. A at 2. Given this clear expression of the statutory authority on which the order was based, the Court is not persuaded to construe the order as arising under a different provision merely because the Superior Court found the application supported by a greater showing of suspicion than was actually required.

Even if this Court—along with every other district court within this circuit to have addressed the issue and two Courts of Appeal—is wrong about the inapplicability of the Fourth Amendment, the evidence at issue would likely be admissible under the good faith exception first articulated in *United*

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

States v. Leon, 468 U.S. 897 (1984), which also applies to "an officer acting in objectively reasonable reliance on a statute" authorizing a warrantless search or seizure of evidence, *Illinois v. Krull*, 480 U.S. 340, 350–56 (1987). Because the vast majority of courts has upheld the constitutionality of § 2703(d), and because the orders were supported by affidavits containing some grounds for suspicion, the officers involved in executing the orders at issue could, at the very least, have reasonably relied on the Superior Court's issuance of the orders. *See Moreno–Navarez*, 2013 WL 5631017, at *2 (law enforcement officers relying on § 2703(d) order issued by neutral magistrate would qualify for good faith exception); *United States v. Graham*, 846 F.Supp.2d 384, 405–06 (D.Md.2012) ("Even if the government's acquisition of historical cell site location records in this case had been in violation of the Defendants' Fourth Amendment rights, it obtained those records in good faith reliance on a constitutional statute and valid Orders issued by [neutral judicial officers]."); *United States v. Jones*, 908 F.Supp.2d 203, 214–16 (D.D.C.2012) (similar). Indeed, even the Eleventh Circuit's since-vacated opinion in *Davis*, which decided contrary to the majority of cases cited herein that the Fourth Amendment does protect historical cell site data, applied the good faith exception and declined to suppress the evidence at issue. 754 F.3d at 1218.[FN13] Accordingly, while the Court joins its sister district courts in concluding that the Fourth Amendment does not apply to historical cell site data, a contrary conclusion would still not lead to the suppression of the evidence at issue.

FN13. Contrary to Bailey's assertions at oral argument, the Court's conclusion that the good faith exception would apply is not based on a finding that the search application was supported by probable cause. Rather, like numerous other courts, this Court finds that, in light of considerable case law holding that probable cause need not be established to obtain historical cell site data under § 2703(d), it would be reasonable for a law enforcement officer to rely on an order supported by an affidavit containing some grounds for suspicion, though not a showing of probable cause.

2. The Orders at Issue Met the § 2703(d) Standard.

The Court finds that the orders at issue were supported by "specific and articulable facts" constituting "reasonable grounds" to believe that the records sought were "relevant and material" to the relevant investigation. As regards the 503 number, the November 6, 2013 order was supported by an experienced detective's sworn statement that the 503 number was linked to Bailey, who had a criminal history including bank robberies, and had been recently observed with Dorsey, who had in turn been linked to the owner of a car used in the series of robberies.[FN14] The affidavit also indicated that Bailey and Dorsey matched the rough physical descriptions of the two suspects that had committed the series of robberies. Moreover, because the records sought covered a time period in which the robberies being investigated were committed, they were reasonably likely to help determine the suspects' whereabouts during those robberies, which would have been material to the investigation. Therefore, whether or not the same facts would have supported a finding of probable cause for a search warrant, the November 6, 2013 order was supported by "specific and articulable facts" that met the lesser standard of § 2703(d).[FN15]

FN14. Because the application contained other facts linking the two defendants, the Court does not rely for purposes of this motion on evidence pertaining to the July 7, 2011 traffic stop, which Bailey has challenged through a separate motion.

FN15. Defendants argue that the orders are also invalid because the affidavits omitted other, inconsistent physical descriptions of the robbery suspects. This argument is unpersuasive and, in any event, could not overcome the unavailability of a suppression remedy under the SCA.

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

***9** As regards the 947 number, the November 14, 2013 application was supported by the same facts, as well as by surveillance that further linked Dorsey to the car used in the robberies, and to a person matching the description of the second robbery suspect. Moreover, the affidavit supporting that order indicated "numerous phone calls" between the 503 and 947 telephone numbers. This order, too, was supported by specific facts giving the issuing judge reasonable grounds to believe that the records sought were material to the ongoing investigation.

3. No Suppression Remedy Is Available for Violations of the SCA.

Even if the orders did not meet the § 2703(d) standard, the "Stored Communications Act does *not* provide an exclusion remedy. It allows for civil damages, and criminal punishment, but nothing more." *United States v. Smith,* 155 F.3d 1051, 1056 (9th Cir.1998) (emphasis in original) (citations omitted). Indeed, the SCA "expressly rules out exclusion as a remedy" by making its remedial provisions exclusive. *Id.* (citing 18 U.S.C. § 2708); *see also United States v. Corbitt,* 588 F. App'x 594 (9th Cir.2014) ("Suppression of the evidence seized is not available as a remedy for a statutory violation of the [Stored Communications] Act."); *United States v. Guerrero,* 768 F.3d 351, 358 (5th Cir.2014) ("[S]uppression is not a remedy for a violation of the Stored Communications Act."); *United States v. Rigmalden,* No. CR 08–814–PHX–DGC, 2013 WL 1932800, at *10 (D.Ariz. May 8, 2013) ("[E]ven if the SCA had been violated in some respect, Defendant's motion to suppress would be denied. Suppression is not an available remedy for violations of the SCA."). Defendants' suppression motions fail for this additional and independent reason.

4. To the Extent the Order Authorized the Real-time Collection of Cell Site Information, That Authorization Was Improper; However, Suppression of the Historical Cell Site Information Is Not Warranted on That Basis.

In contrast to the less stringent standard for obtaining historical cell site data pursuant to § 2703(d), described above, a majority of courts have taken the position that the government must make a showing of probable cause to acquire "real-time" or "prospective" cell site location data. *See United States v. Espudo,* 954 F.3d 1029, 1035 (S.D.Cal.2013) (collecting cases). The orders here authorized law enforcement to obtain real-time cell site data for the thirty days subsequent to the issuance of the orders. The government concedes that such prospective data collection runs contrary to the majority of recent decisions, and represents that it "will not seek to introduce such evidence obtained through these orders," but rather "only seek to use the data ... collected during the periods of September 1, 2013 through the date each order was signed." Dkt. No. 59 at 7 n. 4. At oral argument, the government reiterated that it will not seek to introduce any real-time data obtained pursuant to the state court orders.

***10** Because the government clearly sought and obtained § 2703(d) orders for historical cell site data, the Court rejects Bailey's suggestion in his reply brief-unaccompanied by legal authority-that because that order also authorized the collection of prospective data, the application to obtain historical data must also have been supported by probable cause, and should be suppressed. Even assuming *arguendo* that some portions of the order were invalid, suppression of evidence validly obtained through other portions of the order would not follow. *See United States v. Sears,* 411 F.3d 1124, 1129 (9th Cir.2005) (" '[O]nly those items seized pursuant to invalid portions of a warrant must be suppressed.' " (citing *United States v. Gomez–Soto,* 723 F.2d 649, 654 (9th Cir.1984)). This rule of severance is especially appropriate where the government disclaims the intention to use the arguably unlawful evidence.[FN16] Nevertheless, at the February 23, 2015 hearing, the Court instructed government counsel to assist defense counsel in separating historical from real-time cell site data.

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

FN16. Because the government represents that it will not seek to introduce real-time cell site data obtained pursuant to the order, the Court need not resolve the question of whether such evidence would be admissible under the good faith exception. *Compare Espudo*, 954 F.3d at 1044 ("[E]ven though the Government did not obtain a warrant based on probable cause prior to seeking real-time cell site location data, which this Court finds is required, this evidence is nonetheless admissible under the good faith exception.").

C. Conclusion

For the foregoing reasons, the Court **DENIES** defendants' motion to suppress subscriber information and historical cell site data obtained pursuant to the November 6 and November 14, 2013 state court orders.

IV. BAILEY'S MOTION TO SUPPRESS CELL SITE INFORMATION OBTAINED PURSUANT TO FEDERAL SEARCH WARRANT

On December 24, 2014, Bailey filed a motion to suppress cell site information and records obtained pursuant to a federal search application and order issued on or about December 12, 2013, by United States Magistrate Judge Frederick F. Mumm. Dkt. No. 44. The government filed a consolidated opposition to the instant motion, as well as Dorsey's related motion discussed below, on January 26, 2015. Dkt. No. 58. Bailey filed a reply on February 9, 2015. Dkt. No. 68. For the reasons that follow, the motion is **DENIED.**

A. Background

On or about December 12, 2013, the government applied for an order that the relevant cellular telephone service provider must furnish the FBI and LASD with information relating to a cellular telephone believed to be used by Bailey, linked to the number (213) 503–3495 (the "Subject Telephone"). *See* Dkt. No. 44 Ex. A. Specifically, the government sought "information reflecting the location of cellular towers ... related to the use of the Subject Telephone" for a prospective period of sixty days. *Id.* at 2. The government did not seek to intercept the contents of any communications, but instead sought to ascertain the locations at which calls were sent and received, as well as the telephone numbers involved and the duration of the communications. *See id.* at 2–4.

The application attached a declaration sworn by Sean Sterle ("Sterle"), who at that time had been employed as an FBI special agent for fifteen years. Dkt. No. 44 Ex. A (Sterle Decl.) ¶ 1. Sterle represented that through his experience, which included investigating robberies of banks and other commercial institutions, he had become "familiar with the methods employed by robbers to take money from banks and commercial institutions." *Id.* ¶¶ 2–3. After explaining his qualifications and the purpose of the declaration, Sterle set forth the following information in support of probable cause.

***11** Sterle explained that Bailey and Dorsey were suspected to be the "Cowboy Gun Bandits" thought to have committed a series of thirty-one armed robberies or attempted armed robberies of banks and commercial institutions in the Los Angeles area. *Id.* ¶ 5. Sterle declared that the modus operandi in each of the robberies was similar. Specifically, "[i]n most cases," both suspects entered the target location "wearing the same dark clothing (black hoodie sweatshirt, black or dark blue jeans)," with masks or bandanas covering their faces. One or both of the suspects was typically "armed with a large chrome/blue steel revolver and/or a blue steel semiautomatic handgun." The suspects would "point the firearm at the cashier, demand he or she open the cash register, and take the money." *Id.* ¶ 6.

Sterle declared that in six of the robberies, "witness statements or security video revealed that Bailey and Dorsey fled the robbery in a dark colored vehicle." In a September 30, 2013 robber of a Papa John's, a witness observed the suspects enter a compact vehicle, and the witness gave authorities the partial license plate number "6TNB." In an Oc-

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

tober 6, 2013 ARCO gas station robbery, a witness observed a dark Nissan Altima parked behind the gas station, and reported the last three digits of the license plate as "435." On October 10, 2013, Dorsey was involved in a minor traffic collision while driving a black Nissan Altima with the license plate "6TBN435." The registered owner of that vehicle was Dorsey's wife. Sterle explained that this license plate "matches the previously reported combined license plates-with the 'B' and 'N' in switched positions." *Id.* ¶ 7.

The declaration states that surveillance video of an October 25, 2013 robbery of another ARCO gas station shows Dorsey exiting a black Nissan Altima, entering the ARCO to pay for gas, and looking into the cash register when it is opened by the cashier. According to Sterle, Dorsey "appears to be wearing the same jeans and dark tennis shoes with white trim which were worn by him in the majority of the above robberies." Sterle stated that approximately five minutes later, the video shows a suspect Sterle believed to be Bailey entering the ARCO and pointing the chrome revolver at the clerk and another person. Sterle declared that when the suspect "attempted to take the money with his left hand [he] appeared to have trouble grasping it." Further, the "ring finger on Bailey's left glove appears to be empty in the security video." The video then shows the robber "set[ting] the gun down on the counter and [taking] the money with his right hand" before fleeing "in the direction the black Nissan Altima was last seen." Sterle noted that a "query of Bailey's Criminal History Record revealed that he is missing a finger on his left hand." Sterle related that in two of the other robberies (of a Shell gas station on September 24, 2013 and a Valero gas station on October 28, 2013), "a finger on Bailey's glove appears to be empty in the security videos." *Id.* ¶ 8.

***12** Sterle asserted that Bailey and Dorsey were also suspected of robbing a Citibank branch in Glendale, California on November 5, 2013. *Id.* ¶ 9. In that robbery, two men entered the bank and a suspect Sterle believed to be Dorsey "pointed a semi-automatic handgun at the employees and climbed over one of the teller's windows." A second man, believed to be Bailey, then "ordered several of the customers and employees to the ground while Dorsey removed the cash from each teller's cash drawer." The two men fled, and a witness "observed the suspects leave the area in a gold/champagne colored Nissan Versa." *Id.* In a security video of the robbery, the suspect believed to be Dorsey "can be seen wearing the same black with white trim tennis shoes and jeans that are seen in the security videos of the previous robberies and the instance in which he purchased gas before the [October 25, 2013] ARCO Gas robbery." *Id.* ¶ 10. Additionally, "[s]everal frames of the security video show a finger of" the man believed to be Bailey's "left glove bent in odd directions, which is consistent with Bailey's lack of a ring finger on his left hand." *Id.*

Sterle next set forth information linking Bailey and Dorsey. On August 6, 2013, Dorsey was cited while driving a vehicle rented by Bailey. Additionally, security video indicates that on November 2, 2013, Bailey and Dorsey drove to an impound lot, Hollywood Tow, to retrieve something from Dorsey's Jaguar automobile, which had been towed to that lot. The video shows Bailey and Dorsey "wearing similar pants and shoes [as those] seen in many of the robbery security videos," and "clearly" shows Bailey's missing left ring finger. *Id.* ¶ 12.

The declaration then describes information linking Bailey to the Subject Telephone. On January 2, 2010, Bailey was involved in a traffic collision and, in a related police report, listed the Subject Telephone's number as his own. Sterle declared that "[r]eview of publicly available databases also indicate[s] that Bailey is the user of the Subject Telephone Number." The declaration also asserts that Bailey had "provided this number to rental car companies. Finally, Sterle declared that the number "was also in contact with a number used by Dorsey during the period of the robberies." [FN17] *Id.* ¶ 13.

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

FN17. The declaration asserts that LASD previously obtained call detail records for the Subject Telephone through a state court order that expired on December 6, 2013. Sterle Decl. ¶ 14. Information obtained pursuant to that order "indicate[d] that Bailey and Dorsey communicated during the time of the robberies, including within several hours of many of the robberies." *Id.* Bailey unsuccessfully seeks to suppress evidence from this order in a separate motion discussed in this order; even if that evidence were suppressed, the Court's conclusion on the instant motion would not change.

Sterle declared that there had not been a suspected robbery by the pair since the November 2013 Citibank robbery, but that law enforcement anticipated that the two could "restart their robbery spree" once the $55,000 stolen from Citibank ran out. The declaration asserts that "[i]n order to track Bailey to see if he is planning or committing additional robberies, it is important for law enforcement to be able to monitor his movements." Sterle stated that cell site data "would assist law enforcement by providing a rough location for Bailey which would then allow for physical surveillance or the installation ... of tracking devices on his vehicle." The declaration also claims that the location information "may become relevant if and when [Bailey] is charged ... and his arrest is sought," and would reduce the risk that the ongoing investigation would be compromised. *Id.* ¶ 15.

***13** United States Magistrate Judge Frederick R. Mumm issued the requested order on December 12, 2013, finding "probable cause to believe that cell-site information, likely to be received concerning the approximate location of the Subject Telephone ... will constitute or yield evidence of" bank robbery and Hobbs Act violations committed by Bailey and Dorsey. Dkt. No. 44 Ex. A. Judge Mumm ordered the relevant service carrier to

disclose, at such intervals and times as directed by the Investigating Agency, information concerning the location (physical address) of the cell-site at call origination (for outbound calling), call termination (for incoming calls), and, if reasonably available, during the progress of a call, for the Subject

Telephone, as well as other information, apart from the content of any communication, that is reasonably available to the Carrier and that is requested by the Investigating Agency or any law enforcement agency working with the Investigating Agency, concerning the cell sites/sectors receiving and transmitting signals to and from the Subject Telephone while a call is in progress.

Id. The order was to be effective for a period of sixty days, and apply to any changed telephone number assigned to the same telephone account. *Id.*

B. Analysis

1. Legal Standards

"A search warrant is supported by probable cause if the issuing judge finds that, '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.' " *United States v. Underwood,* 725 F.3d 1076, 1081 (9th Cir.2013) (quoting *Illinois v. Gates,* 462 U.S. 213, 238 (1983)). "Whether there is a fair probability depends upon the totality of the circumstances, including reasonable inferences, and is a 'commonsense, practical question.' " *United States v. Kelley,* 482 F.3d 1047, 1050 (9th Cir.2007) (quoting *United States v. Gourde,* 440 F.3d 1065, 1069 (9th Cir.2006) (en banc)). "Neither certainty nor a preponderance of the evidence is required." *Id.*

"A magistrate judge's finding of probable cause is entitled to great deference." *United States v. Clark,* 31 F.3d 831, 834 (9th Cir.1994); *see also Gourde,* 440 F.3d at 1069 ("We are not in a position to flyspeck the affidavit through de novo review.... This deferential approach is the antithesis

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

of a 'grudging or negative attitude' toward search warrants and a 'hypertechnical rather than a commonsense' analysis." (citations omitted)); *United States v. Wong*, 334 F.3d 831, 835–836 (9th Cir.2003) ("We review a magistrate judge's finding of probable cause to issue a search warrant for clear error."). Still, "[a] reviewing court should find that probable cause is not met when the issuing judge lacked a 'substantial basis for ... conclud[ing] that probable cause existed.' " *Underwood*, 725 F.3d at 1081 (brackets in original; internal quotation marks omitted) (quoting *Gates*, 462 U.S. at 238–39). "Conclusions of the affiant unsupported by underlying facts cannot be used to establish probable cause." *Id.* The supporting affidavit or declaration "must recite underlying facts so that the issuing judge can draw his or her own reasonable inferences and conclusions; it is these facts that form the central basis of the probable cause determination." *Id.* "Under the totality of the circumstances test," however, "otherwise innocent behavior may be indicative of criminality when viewed in context." *United States v. Chavez–Miranda*, 306 F.3d 973, 978 (9th Cir.2002). "Additionally, issuing judges may rely on the training and experience of affiant police officers." *Id.*

2. Whether The Order Was Supported by Probable Cause to Suspect that Bailey Was One of the Robbers

***14** Bailey argues that "the warrant declaration made an insufficient showing ... that Mr. Bailey was one of the robbers," and consists largely of unsupported conclusions. Dkt. No. 44 at 9. He contends that the declaration is even weaker once references to evidence he seeks to suppress through other motions is excised.[FN18] Bailey also argues that, even if not excised, evidence that Bailey and Dorsey were together in a vehicle years prior to the commission of the first robbery, or that there were calls "between phones connected to Bailey and Dorsey during the period of the robberies," does not without more show any connection to the robberies. *Id.* at 10–11. Further, Bailey discounts the observations of Bailey and Dorsey together at the Hollywood Tow in clothing matching that worn during the robberies, arguing that the clothing at issue is too commonplace to support a finding of probable cause. *Id.* at 12. Finally, although he admits that evidence that both Bailey and one of the suspects were missing fingers on their left hands has "some probative value," Bailey stresses that the affiant used words of "qualification" in describing the security videos (for example, that the ring finger of a glove "appears to be empty" or that a finger of a glove was bent in odd directions, "consistent with" Bailey's missing finger). *Id.* at 12–13.

FN18. *See United States v. Nora*, 765 F.3d 1049, 1058 (9th Cir.2014) (explaining that where evidence cited in a search warrant affidavit is inadmissible, the warrant "remains valid if, after excising the tainted affidavit, the affidavit's remaining untainted evidence would provide a neutral magistrate with probable cause"; that determination is made "without the usual deference owed to the magistrate's initial finding of probable cause" (internal quotation marks and citations omitted)).

Under the applicable "practical, commonsense" approach, the Court finds that the factual allegations summarized in the background section above are sufficient to show probable cause.[FN19] Even excising evidence Bailey seeks to suppress through other motions, there was ample evidence that Bailey and Dorsey were associates; therefore, the magistrate judge was not required to disregard entirely with regard to Bailey the significant evidence linking Dorsey to the robberies. More importantly, a highly distinctive physical feature—a missing finger on the left hand—directly linked Bailey to the target robberies. Bailey's suggestion that four separate videos suggesting that one of the robbers was missing a finger on the same hand should be discounted, because the affiant did not express absolute certainty, is an unpersuasive attempt to impose "a hypertechnical, rather than a commonsense" approach to interpreting a search warrant af-

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

fidavit. *See Gates*, 462 U.S. at 236. In sum, the magistrate judge had a substantial basis for concluding that there was a reasonable probability that Bailey was one of the robbers.

> FN19. In its application, the government sought the requested information pursuant to a "hybrid theory" based on 18 U.S.C. §§ 3122(a)(1) and 3123(a)(1), which govern orders authorizing the installation and use of pen registers or trap and trace devices, and 18 U.S.C. § 2703(d), discussed above in section III.B. In that application and the opposition to the instant motion, the government has maintained that, as a matter of law, it need not show probable cause to obtain an order of this type-pbut that because the application *does* show probable cause, the Court need not consider that position. Accordingly, the Court applies traditional probable cause standards and does not address the government's "hybrid theory."

2. Whether the Order Was Supported by Probable Cause to Suspect that Evidence of the Target Crimes Would Be Found

Bailey argues that even if there was probable cause to suspect that he was one of the robbers, the warrant declaration "made an insufficient showing ... that a search conducted well over one month from commission of the last robbery would reveal criminality." Dkt. No. 44 at 9. Even if the cell site information obtained pursuant to a state court order and linking Dorsey to Bailey is ignored (and it need not be in light of the Court's ruling in Section III), the magistrate judge would still have had grounds to conclude that Bailey was linked to the Subject Telephone because (1) Bailey provided that number to law enforcement, (2) public databases list Bailey as the number's user, and (3) Bailey provided the number to car rental companies. Thus, the issue is whether the physical location information sought by the government was reasonably likely to reveal evidence of the target crimes.

***15** Bailey contends that the declaration supports only tracking him to see if he was "planning or committing additional robberies" or in the event that he was charged and his arrest sought. Accordingly, Bailey denies that the declaration includes any allegation that his cell site information would lead to evidence of his commission of the target offenses. Dkt. No. 44 at 13. The government responds that Sterle amply explained that "based on the large number of robberies in a short period of time, it was likely that Dorsey and Bailey would commit another robbery," and that being able to track Bailey's phone was important for locating him. Dkt. No. 58 at 10. Once law enforcement located Bailey, the government argues, agents could conduct surveillance of him to determine whether he was committing additional robberies. Moreover, the prosecution contends, because "Bailey used specific firearms during the robberies and had a distinctive physical characteristic, locating Bailey would likely involve finding the firearm and would certainly provide for closer examination of his missing finger, which would be a key piece of evidence" in prosecuting the previous robberies. The government also cites authority to the effect that warrants may be "issued for surveillance or tracking devices on probable cause that the 'search' (the surveillance or tracking) will uncover evidence of a crime, even though the crime may not yet have been committed." *United States v. Rojas*, 671 F.2d 159, 166 n. 8 (5th Cir.1982).

The government has the better of the argument. The magistrate judge had a substantial basis for concluding that there was a fair probability that evidence of Bailey's whereabouts would reveal evidence of the dozens of robberies thought to have been committed by the two robbers, including cash from the robberies, the distinctive handgun used in the robberies, or confirmation of Bailey's missing finger, which is a highly probative identifying detail tying him to the robberies. *See United States v. Steeves*, 525 F.2d 33, 38 (8th Cir.1975) (explaining that people who own handguns often keep them on their persons). The magistrate judge could also have reasonably concluded that, because Bailey

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

was suspected of committing approximately thirty robberies in a then-recent two-month period, Bailey's physical location might be reveal the planning or commission of additional robberies that the two suspects might conduct after their prior robbery proceeds ran out. Given the ample evidence linking Bailey to the robberies, the conclusion that evidence of Bailey's physical location could lead to additional evidence of those robberies was not clearly erroneous.

3. The Good Faith Exception

Evidence obtained pursuant to a facially valid search warrant, later found to be invalid, is admissible if the executing officers acted in good faith and in objectively reasonable reliance on the warrant. *United States v. Leon,* 468 U.S. 897, 922 (1984). The "good faith test is an objective one," through which a court "ask[s] not what the executing officer believed, or could have believed, but 'whether a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization.' " *United States v. Luong,* 470 F.3d 898, 902 (9th Cir.2006) (quoting *Leon,* 468 U.S. at 922). This inquiry is limited to the four corners of the affidavit given in support of the warrant. *Id.* at 904. That affidavit "must establish at least a colorable argument for probable cause." *Id.* at 903; *see Leon,* 468 U.S. at 926 (framing the inquiry as whether the affidavit is "sufficient to create disagreement among thoughtful and competent judges as to the existence of probable cause").

***16** " '[S]earches pursuant to a warrant will rarely require any deep inquiry into reasonableness,' for 'a warrant issued by a magistrate [judge] normally suffices to establish' that a law enforcement officer has 'acted in good faith in conducting the search.' " *Leon,* 468 U.S. at 922. But "the Supreme Court has identified at least four situations in which reliance on a warrant cannot be considered objectively reasonable, and therefore the good faith exception cannot apply:

> (1) when the affiant knowingly or recklessly misleads the judge with false information; (2) when the judge wholly abandons his or her neutral role; (3) when the affidavit is so lacking in indicia of probable cause that official belief in its existence is objectively unreasonable; and (4) when the warrant is so facially deficient that executing officers cannot reasonably presume it to be valid (i.e., it fails to specify the place to be searched or the things to be seized).

Luong, 470 F.3d at 902 (citing *Leon,* 468 U.S. at 914, 923). "The government, not the defendant, bears the burden of proving that its agents' reliance upon the warrant was objectively reasonable." *United States v. Michaelian,* 803 F.2d 1042, 1048 (9th Cir.1986). Bailey argues that "after excising the tainted allegations and affording no weight to the conclusory allegations, the remaining facts would not be sufficient to lead a reasonable judge to find probable cause," or to lead a reasonable law enforcement officer to rely upon the order. Dkt. No. 44 at 14–15. The Court disagrees.

As discussed above, the order in question was supported by probable cause. But even if it were not, the affidavit certainly contains facts establishing a "colorable argument" for probable cause. Additionally, other factors support the applicability of the good faith exception here. First, the order was sought on a "hybrid" Pen Register Statute and Stored Communications Act theory, under which the government need not show probable cause to obtain real-time cell site data. Although rejected by a majority of recent decisions, this theory has been accepted by some district courts, and has not been rejected by the Ninth Circuit. Thus, law enforcement officials could arguably have reasonably relied on the order even if it was supported by a showing less than probable cause. *See United States v. Espudo,* 954 F.Supp.2d 1029, 1037–44 (S.D.Cal.2013) (explaining that this " 'hybrid theory' ... has been commonly put forth by the government when seeking real time cell site location data and rejecting that theory, but nonetheless applying the good faith exception because of conflicting district court decisions on the issue). Second the ap-

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

plication was signed by an Assistant United States Attorney, Dkt. No. 44 Ex. A at 6, which can support the reasonableness of a law enforcement agent's reliance. *See United States v. Freitas,* 856 F.2d 1425, 1431–32 (9th Cir.1988) (noting agents' reliance on legal opinion of Assistant United States Attorney, in addition to magistrate judge, in determining that district court had erred in refusing to apply good faith exception); *Michaelian,* 803 F.2d at 1047 ("The warrants and affidavit came under scrutiny at four levels of attorney review, further adding to the reasonableness of the agents' reliance thereon .").

***17** For the reasons stated, the Court concludes that (1) the order was supported by probable cause and (2) even if it were not, the evidence would be admissible under the *Leon* good faith exception. Therefore, the Court **DENIES** Bailey's motion to suppress real-time cell site information obtained pursuant to the federal order dated December 12, 2013.

V. DORSEY'S MOTION FOR AN EVIDENTIARY HEARING REGARDING USE OF A TELEPHONE NUMBER

On January 13, 2015, Dorsey filed a motion joining in Bailey's motion to suppress cell site information obtained through the federal order discussed above. Dkt. No. 54. In that motion, Dorsey requested a hearing to determine whether there was evidence to link Dorsey to a telephone number which was the basis for a separate warrant. In an opposition filed on January 26, 2015, the government attached the warrant in question, as well as the declaration filed in support of that warrant and a series of documents referenced in that declaration. Dkt. No. 58. On February 10, 2015, Dorsey filed a response stating that "the government has provided counsel with additional documentation, which provides the link" between Dorsey and the telephone number in question. Dkt. No. 75. For that reason, Dorsey withdrew his request for an evidentiary hearing. *Id.* Accordingly, this motion is **DENIED** as moot.

VI. BAILEY'S MOTION TO SUPPRESS BANK ACCOUNT INFORMATION

On December 24, 2014, Bailey filed a motion to suppress evidence seized or derived from his Wells Fargo bank account pursuant to a state search warrant issued on or about November 15, 2013. Dkt. No. 45. The government filed an opposition on January 26, 2015, and Bailey replied on February 9, 2015. Dkt. Nos. 60, 71. For the reasons that follow, the motion is **DENIED.**

A. Background

On November 15, 2013, the California Superior Court issued a warrant to search and seize account information pertaining to a Wells Fargo bank account in Bailey's name. Dkt. No. 45 Ex. A at 1. The warrant covered account statements, deposit slips, and a host of other records pertaining to deposits and withdrawals, checks, credit agreements, wire transfers, credit card applications, safety deposit boxes, communications with the financial institution, and other transactions. *Id.* at 2. The warrant was supported by a Glendale police officer's affidavit stating that he met with LAPD Detective Chris Marsden ("Marsden"), the lead investigator on a series of approximately thirty-one robberies, the last of which occurred at a Citibank branch in Glendale. According to the affidavit, Marsden believed that the same two suspects had committed each robbery based on the modus operandi of each crime, the use of handguns, the clothing and physical size of the suspects, statements made by each suspect during the robberies, and the fact that the suspects concealed their faces with a bandana or similar item in each robbery. Marsden described the suspects as black males, one between 6' and 6'3", and the other around 5'7" with a "thin build." *Id.* at 5–6.

***18** The affidavit states that Marsden had reviewed surveillance videos of the robberies, "spoken to investigators from other law enforcement agencies and reviewed details of each and every robbery that has similar facts and circumstances" to the Citibank robbery. He had identified

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

a possibly involved vehicle, which belonged to Jacqueline Martin. Marsden then searched records and discovered that Martin had a child with Dorsey, who was in turn "associated with" Bailey. Marsden represented that searches of public databases indicate that Bailey and Dorsey two resided at a particular address in Hollywood at the same time. The affidavit then details the two mens' criminal records. Bailey's record includes four robberies conducted between 1968 and 1980, including one bank robbery. *Id.* at 6–7.

The affidavit states that Marsden reviewed surveillance video of a robber at an ARCO station at 18076 Ventura Boulevard, Los Angeles, and that approximately five minutes before the robbery, Dorsey entered the station store and made a purchase. Finally, the affidavit states that a detective had discovered that Bailey used a Wells Fargo credit or debit card to rent a vehicle in August 2013, and that Bailey had rented twenty-one vehicles from a certain car rental business since 2010. *Id.* at 7–8.

B. Analysis

Bailey argues that the search warrant was not supported by probable cause, and that the evidence derived therefrom should be suppressed under the exclusionary rule of the Fourth Amendment. The government contends that Bailey has no Fourth Amendment rights in the information sought, and that under the statute that does apply, suppression is not an available remedy. The government is correct.

In *United States v. Miller,* 425 U.S. 435 (1976), the Supreme Court considered a defendant's motion to suppress documents obtained from two banks pursuant to allegedly defective grand jury subpoenas. The Supreme Court affirmed the district court's denial of that motion on the ground that the defendant had no protected privacy interest in the evidence at issue. *Id.* at 440. The Court reasoned that the documents sought were not the defendant's "private papers," but rather "business records of the banks." *Id.* The Court "perceive[d] no legitimate 'expectation of privacy' " in the documents, which "contain[ed] only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business." *Id.* at 442. The bank records therefore fell under the rule 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. Accordingly, the district court "correctly denied respondent's motion to suppress, since he possessed no Fourth Amendment interest that could be vindicated." *Id.* at 445; *see also United States v. Standefer,* No. 06–CR–2674–H, 2007 WL 2301760, at *3 (S.D.Cal. Aug. 8, 2007) ("There is no reasonable expectation of privacy in financial records such as checks, deposit slips, and financial statements maintained by third party institutions such as banks.' " (quoting *In re Grand Jury Proceedings,* 40 F.3d 959, 962 (9th Cir.1994)).

***19** Bailey argues in his reply brief that *Miller* is "outdated" in light of the Supreme Court's subsequent decision in *United States v. Jones,* 132 S.Ct. 945 (2012), which determined that the attachment of a GPS tracking device to a vehicle, and subsequent use of that device to monitor the vehicle's movement, was a search within the meaning of the Fourth Amendment. Although this argument lacks persuasive force for reasons including the obvious differences between a continuously tracked car and bank records held by a third party, this Court is bound to apply *Miller,* and for that reason does not address Bailey's reply in detail. Because Bailey has no Fourth Amendment rights in his bank records, and because "a court may not exclude evidence under the Fourth Amendment unless it finds that an unlawful search or seizure violated the defendant's own constitutional rights," *United States v. Payner,* 447 U.S. 727, 732 (1980), Bailey's Fourth Amendment suppression argument fails.

"Congress, in response to *Miller,* enacted the Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401–22 (1982)." *United States v. Mann,* 829

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

F.2d 849, 851 (9th Cir.1987). The "RFPA" requires law enforcement agencies to follow certain procedure to obtain bank records. It also sets forth civil penalties and injunctive relief for violations of its provisions. 12 U.S.C. §§ 3417, 3418. However, the RFPA provides that "[t]he remedies and sanctions described in this chapter shall be the only authorized judicial remedies and sanctions for violations of this chapter." *Id.* § 3417. The Ninth Circuit has affirmed that the RFPA's stated "remedies are exclusive," and that the statute "excludes a suppression remedy." *United States v. Frazin*, 780 F.2d 1461, 1466 (9th Cir.1986) (affirming district court's denial of motion to suppress bank records); *see also United States v. Kington*, 801 F .2d 733, 737–38 (5th Cir.1986) (affirming that "bank customers have no legitimate Fourth Amendment expectation of privacy in the records of their accounts maintained by banks," and holding that suppression of such records is not appropriate under the RFPA or a court's inherent supervisory powers).

Neither the Fourth Amendment, which is inapplicable to the evidence seized, nor the RFPA which includes no suppression remedy, permits this Court to suppress the evidence at issue. Because the suppression remedy is simply not available, the Court does not address whether the search warrant was supported by probable cause or otherwise lawful, and **DENIES** Bailey's motion.

VII. DEFENDANTS' MOTIONS TO SUPPRESS EVIDENCE SEIZED FROM VEHICLE STOP AND FRUITS THEREOF

On December 24, 2014, Bailey filed a motion to suppress evidence seized from, observations made of, and statements made during, a vehicle stop and search that occurred on or about January 7, 2011; in the alternative, he requested an evidentiary hearing. Dkt. No. 46. Dorsey joined in the motion on January 13, 2015. Dkt. No. 55. The government filed a consolidated opposition on January 26, 2015, and Bailey replied on February 9, 2015. Dkt. Nos. 64, 69. In briefs and declarations, the parties offered different factual accounts of the traffic stop and search; the parties also contested the legal standards applicable to searches conducted pursuant to probation search terms.

***20** On February 19, 2015, the government filed a supplemental opposition representing that the prosecution and defense had conferred and agreed that the Court should postpone ruling on this motion, and consider the other suppression motions discussed herein "with the evidence of the traffic stop and ski mask excised from the statements of probable cause supporting the other search warrant applications." Dkt. No. 78 at 1. While still maintaining its position that the traffic stop and search were valid, the government asserts that it is willing to forgo the presentation of any evidence arising from the traffic stop. "Specifically, the government is willing to forgo presenting to the jury any evidence that defendants were together on January 7, 2011, as well as any evidence related to the black ski mask that was recovered during a probation search of the vehicle, and anything the defendants said during the stop." *Id.* at 2–3. At oral argument, both government and defense counsel asserted that they wished the Court to defer ruling on the instant motion, and the prosecution affirmed that it would not seek to introduce the aforementioned evidence.

At the February 23, 2015 hearing, Bailey's counsel asserted that even though the government has agreed not to introduce evidence directly obtained from the traffic stop, defendants believe that LAPD documents related to that stop may provide an independent basis to suppress other evidence. At defendants' request, the Court will review *in camera* the subpoenaed documents related to the January 2011 traffic stop, and determine if any of that documentation should be produced to the defense. The Court does not rule on the traffic stop motion at this time.

VIII. BAILEY'S MOTION TO SUPPRESS RESIDENCE AND VEHICLE SEARCHES

On December 24, 2014, Bailey filed a motion to suppress all evidence seized and observations resulting from (1) a search of Bailey's residence at

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

3551 South Western Avenue, Apartment # 5, Los Angeles, California (the "residence"), and (2) a search of a 2005 black Kia sedan allegedly associated with Bailey, both executed pursuant to a federal search warrant issued on or about June 11, 2014 (the "Kia sedan"). Dkt. No. 47. The government filed an opposition on January 26, 2015, and Bailey replied on February 9, 2015. Dkt. Nos. 62, 70.

A. Background

On June 11, 2014, United States Magistrate Judge Charles Eick issued a warrant authorizing the search of Bailey's residence and the black Kia sedan identified above, as well as a hotel room, storage unit, and two vehicles not relevant to the instant motion. Dkt. No. 47 Ex. A. The application for this warrant was supported by an affidavit sworn by Gary Bennett ("Bennett"), an FBI agent with thirteen years of experience at the time. *Id.* Ex. A (Bennett Aff.) ¶ 1. The affidavit identifies the residence by address and physical description, and the Kia sedan by license plate number, registrant, year, make, and color. *Id.* ¶ 5.

***21** The affidavit explains that the FBI and two police departments had been investigating a number of robberies "committed by two men who have worn similar clothing during many of the robberies" and conducted pursuant to a consistent pattern, "including the use of a large 'cowboy-style' pistol.' " *Id.* ¶ 6. Bennett averred that in most of these robberies,

> one or both men would enter the victim commercial institution wearing dark clothing (black hoodie sweatshirt, black sweatshirt, blue jeans, for example) and a mask or bandana concealing his face. One or both of the men would typically be armed with a large chrome revolver and/or a blue steel semiautomatic handgun. One of the men would point a firearm at the cashier, demand that he or she open the cash register, and take the money from the register.

Id. ¶ 10. In six of those robberies, the affidavit continues, witness statements or security video revealed that the robbers fled in a dark-colored vehicle. After the September 30, 2013 robbery of a Papa John's pizza restaurant, a witness observed the suspects entering a dark "compact vehicle" with a license plate that read in part "6TNB." *Id.* ¶ 11. Just prior to the October 6, 2013 robbery of an ARCO gas station, another witness observed a dark Nissan Altima parked in an alley behind the station, with a license plate number that included the last three digits "435." Shortly thereafter, Dorsey was involved in a minor traffic collision while driving a black Nissan Altima registered to Dorsey's wife and with the license plate number "6TBN435," which "matches the two previously-reported partial plates—with the 'B' and the 'N' interposed." *Id.* ¶ 12.

The affidavit details security video footage showing that, just before an ARCO gas station was robbed on October 25, 2013, Dorsey—"wearing the same jeans and black and gray tennis shoes with white trim that one of the Cowboy Gun Bandits wore during many of the robberies"-exited a black Nissan Altima, entered the store, paid for gas with cash, and looked into the open cash register. Approximately five minutes later, the video shows "a person who matches the physical description of Bailey—which also matches the physical description of the second Cowboy Gun Bandit—entering the ARCO and pointing a chrome revolver at the clerk and another person." The video shows the suspect "attempting to take the money with his left hand" and "suggests that the second Cowboy Gun Bandit is having trouble grasping the money." The video also "appears to demonstrate that a finger of the second Cowboy Gun Bandit's left glove is empty," and shows the suspect "setting the gun down on the counter and taking the money with his right hand" before "fleeing in the direction of the place where the black Nissan Altima was last seen." Bennett stated that he knew from Bailey's criminal history records that he "is missing a finger on his left hand." *Id.* ¶ 13. Bennet declared that security videos of two other specific robberies also "appear to show that one finger of the second Cowboy Gun

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

Bandit's glove appears to be empty." *Id.* ¶ 14.

***22** The affidavit then discusses security footage from the November 5, 2013 robbery of a Citibank in Glendale. This video shows one suspect "wearing the same black and gray tennis shoes with white trim and jeans that he wore during some of the previous robberies, which are the same shoes and jeans Dorsey wore at the ARCO gas station on October 25, 2013." According to the affiant, "several frames of the security video show that one finger of the second Cowboy Gun Bandit's left glove is bent in odd directions, as though there is no finger supporting the glove." *Id.* ¶ 15. The video then shows the two men fleeing the bank. A witness reported that the two suspects "left the area in a gold/champagne colored Nissan Versa." Bennet declared that Hertz rental car records reflect that from October 31, 2013 to November 8, 2013, Bailey rented a Nissan Versa. *Id.* ¶ 17.

Next, the affidavit sets forth the following evidence linking Dorsey and Bailey: on August 6, 2013, Dorsey was cited while driving a vehicle that Bailey had rented, and on November 5, 2013 (the same day as the Citibank robbery), Bailey and Dorsey were together at the Hollywood Tow, wearing "pants and shoes similar to the pants and shoes they appear to have been wearing during several of the robberies." *Id.* ¶ 18. The affidavit also mentions that on June 3, 2014, a federal grand jury returned a sealed indictment charging Dorsey and Bailey with conspiracy to commit Hobbs Act robberies, five individual Hobbs Act robberies, and five counts of use of a firearm in furtherance of a crime of violence. *Id.* ¶ 20.

The affidavit sets forth the following facts as basis for the belief that Bailey was at the time using the residence. On June 2, 2014, two LAPD detectives knocked on the door using a ruse; a man who Marsden identified as Bailey answered the door and directed the detectives to the manager of the apartment complex. Additionally, Bailey listed the address of the residence on his California driver's license, and public database information indicated that he had been residing there since March 2013. *Id.* ¶ 21. Bennett averred that there was a reasonable basis for concluding that evidence of the robberies would be found at the residence for several reasons. First, Bailey had worn "the same clothes" for many of the robberies he committed, and "people generally maintain clothing at their residences." *Id.* ¶ 28. Second, Bennett declared that he knows from his training and experience that people "often keep firearms because they are valuable and serve as a means of protection," and that robbers (particularly felons who are not legally permitted to carry firearms, a category that includes Bailey) "often hide or conceal firearms at their residences ... where they can keep them safe from law enforcement." *Id.* ¶ 30. In particular, Bennett noted that the "Cowboy Gun" revolver used in many of the robberies "is very distinctive," is an uncommon "Colt 'Flat Top' revolver," and "may have personal significance to Bailey, who brandishes that particular gun in many of the robberies." "Because of its large size and classic appearance," Bennet stated that he did not think the suspects would "get rid of the 'Cowboy Gun' revolver in the same manner in which robbers might discard other guns used in crimes." *Id.* ¶ 31.

***23** The affidavit sets forth the following facts as basis for the belief that Bailey was using the Kia sedan at the time. LASD surveillance units observed Bailey driving the vehicle on or about November 24, 2013. Marsden also observed the vehicle parked across the street from Bailey's residence on June 2 and June 3, 2014. Finally, law enforcement photographed the vehicle on November 19, 2013 and February 7, 2014; in each photograph, the driver appeared to be Bailey. *Id.* ¶ 26. Bennet declared that he believed that the Kia sedan could contain clothing that might identify him as one of the robbers, the distinctive Cowboy Gun revolver, or Bailey's cellular telephone, and that it also could have been purchased with robbery proceeds. *Id.* ¶ 34. Moreover, the affidavit states that "law enforcement has sophisticated means to obtain trace hair, fiber and DNA evidence" from the car and that if

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

agents were to obtain samples belonging to Dorsey in the Kia sedan, "that would further establish the connection between the two men and show that it was more likely that they were both involved in the robberies." *Id.* ¶ 35. Finally, Bennett indicated his belief that it was "likely that Dorsey and/or Bailey have not yet spent all the money they are believed to have stolen from the Citibank" (over $55,000), and stated that the places to be searched could contain large amounts of cash that would constitute further evidence of criminal involvement. *Id.* ¶ 36.

The warrant authorized the seizure of firearms and related evidence; clothing or footwear identified in any description or surveillance footage of the Cowboy Gun Bandits, Dorsey, or Bailey; cellular telephones possessed by the Cowboy Gun Bandits, Dorsey, or Bailey; certain kinds of digital information; bank records; property and vehicle records; keys to any storage units, lockers, safes, or vehicles; photographs; and currency in excess of $500. *Id.* Attach. B.

B. Analysis

The general legal standards applicable to determining whether a search warrant is supported by probable cause are set forth at section IV.B.1, above.

"[I]t cannot follow in all cases, simply from the existence of probable cause to believe a suspect guilty, that there is also probable cause to search his residence." *United States v. Lucarz,* 430 F.2d 1051, 1055 (9th Cir.1970). But "[d]irect evidence linking criminal objects to a particular sites is not required" for a warrant to issue. *United States v. Jackson,* 756 F.2d 703, 705 (9th Cir.1985). "When a magistrate judge issues a search warrant for a residence, he must find a 'reasonable nexus' between the contraband sought and the residence." *United States v.. Chavez–Miranda,* 306 F.3d 973, 978 (9th Cir.2002). "In making this determination, a magistrate judge need only find that it would be reasonable to seek the evidence there." *Id.* This determination is properly informed by such considerations as "the type of crime, the nature of the missing items, the extent of the suspect's opportunity for concealment, and normal inferences as to where a criminal would be likely to hide stolen property." *Lucarz,* 430 F.2d at 1055.

***24** The prosecution summarizes the relevant evidence contained in the affidavit as follows:

> Among the information before Judge Eick that established probable cause that Bailey was the second Cowboy Gun Bandit—including the fact that a grand jury had already returned an indictment against Bailey and Dorsey for the robberies committed by the Cowboy Gun Bandits—were the following facts: (a) Bailey, like one of the Cowboy Gun Bandits, was missing the ring finger on his left hand; (b) Bailey and Dorsey were known associates ...; (c) one of the Cowboy Gun Bandits' getaway cars was registered to Dorsey's wife; (d) their other getaway car matched the specific description of the car that Bailey was renting at the same time that the Cowboy Gun Bandits robbed the Citibank in Glendale; (e) five minutes after Dorsey was caught on Camera casing an ARCO gas station with no mask on, the second Cowboy Gun Bandit, who was missing a finger on his left hand, robbed the ARCO station; (f) surveillance video taken during the other robberies shows that the second Cowboy Gun Bandit was missing a finger; and (g) security video from a tow-yard in Hollywood show[s] that Bailey and Dorsey [were] together a few days before—and on the same day as—the Cowboy Gun Bandits robbed the Citibank in Glendale.

Dkt. No. 62 at 2. The Court agrees that the affidavit contained facts sufficient for the magistrate judge to conclude that there was a "fair probability" that Bailey was one of the Cowboy Gun Bandits.

Bailey's arguments to the contrary are unpersuasive. Essentially, Bailey dissects each bit of evidence and argues that, standing alone, no reasonable inference of criminality can be drawn from it. He contends that evidence of the modus operandi of the series of robberies suggested that they were

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

committed by the same persons, but not necessarily by Bailey; he also argues that the fact that the black Nissan Altima was sometimes used as a getaway vehicle and was linked to Dorsey has no relevance as to Bailey. Dkt. No. 47 at 9–10. Bailey argues that evidence generally linking him to Dorsey is irrelevant because it lacks a sufficient nexus to the target crimes. He also asserts that "the fact that Bailey and Dorsey were seen together in Hollywood shows that they had contact with one another on the day of the Citibank robbery but does not demonstrate that Mr. Bailey was in Glendale that day robbing the bank." *Id.* at 11–12. This approach ignores the "totality of the circumstances" approach that applies to probable cause. The magistrate judge could reasonably have concluded that the ample evidence linking Bailey and Dorsey, while innocent in isolation, increased the probability that Bailey was involved when viewed in conjunction with the other evidence described above, including evidence linking Dorsey to the series of robberies.

Equally unavailing are Bailey's attempts to undercut evidence identifying him as one of the robbers as bare conclusions, unsupported by underlying facts. Although the clothes and shoes Bailey is alleged to have worn during the robberies and in other settings are not unusual, the magistrate judge could have taken the similarities into account as one of many factors supporting probable cause. More important, several videos showed that one of the robbers—like Bailey—was missing a finger on his left hand, a highly probative identifying detail. Bailey's attempts to discount this evidence by seizing on words like "appears" and "suggests" in the affidavit impose a much higher standard of proof than the "practical, commonsense" inquiry that applies to a determination of probable cause. *See United States v. Kelley,* 482 F.3d 1047, 1050 (9th Cir.2007) ("Neither certainty nor a preponderance of the evidence is required."). Finally, the Court finds unpersuasive Bailey's protest that the "affidavit fails to mention ... that from approximately 2010 to 2013 Mr. Bailey had rented approximately 21 vehicles from rental companies as his regular mode of transportation." Dkt. No. 44 at 12–13. This fact does not undercut the significant probative value of the fact that, at the time of the Citibank robbery, Bailey was renting a car of the same make and model as the one used to escape from that robbery. Finally, the magistrate judge could properly have taken into account the fact that a grand jury had already indicted Bailey and Dorsey for the charged crimes when the search warrant was issued. *See United States v. Hernandez–Escarsega,* 886 F.2d 1560, 1566 (9th Cir.1989) ("Although the fact that the grand jury found probable cause to believe that Hernandez was involved in the importation of narcotics is not determinative, it could certainly be considered by the magistrate." (citations omitted)).

***25** Bailey contends that, even if a magistrate judge could reasonably believe that Bailey was one of the robbers, he could not reasonably believe that a search of the residence and Kia sedan would lead to the discovery of any evidence. Bailey submits that the clothes identified with the robberies were commonplace, and that the affidavit lacks factual support for its statement that "people generally maintain clothing at their residences or in their vehicles ." Dkt. No. 47 at 14. Bailey rejects as similarly conclusory Bennett's statement that he knows from his training and experience that persons often keep firearms at their residences or in their vehicles. *Id.* at 15. Finally, he argues that because there is no allegation that "bait money" was stolen from Citibank, a magistrate judge could not reasonably have concluded that any cash found during the search came from Citibank.

These arguments fail as well. "A magistrate [judge] is permitted to draw reasonable inferences about where evidence is likely to be kept based on the nature of the evidence and the type of offense," and " 'may rely on the conclusions of experienced law enforcement officers regarding where evidence of a crime is likely to be found.' " *United States v. Terry,* 911 F.2d 272, 275 (9th Cir.1990) (quoting *United States v. Fannin,* 817 F.2d 1379, 1382 (9th

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

Cir.1987)); *see United States v. Sayakhom,* 186 F.3d 928, 934 (9th Cir.1999) (affirming denial of motion to suppress evidence of mail fraud found in residence and car where affiant "stated his experience and belief that operators of businesses that involve paperwork typically maintain and carry business records into and out of their offices, in their cars and to and from their residences," permitting the "reasonable conclusion that the evidence described in the warrant would be found in [defendant's] vehicle and residence"). The magistrate judge could reasonably have credited, as supported by Bennett's experience and basic common sense, the assertion that Bailey was likely to keep in his residence and car clothes he had repeatedly worn in robberies, as well as a distinctive gun used in many of those robberies and cash obtained therefrom. *See, e.g., Jackson,* 756 F.2d at 705 ("It was a reasonable inference that Jackson might keep stolen currency in his apartment from a bank robbery two months earlier," where not all of the money stolen had been accounted for.); *United States v. Gann,* 732 F.2d 714, 722 (9th Cir.1984) (finding probable cause where affidavit included agent's "perception that bank robbers frequently use firearms and leave such weapons, ammunition and clothing in their cars or residences"); *United States v. Jones,* 994 F.2d 1051, 1056 (3d Cir.1993) ("[C]ash is the type of loot that criminals seek to hide in secure places like their homes .... Similarly, clothing and firearms [ ] are the also the types of evidence likely to be kept in a suspect's residence."). The affiant's contention that any traces of Dorsey in the Kia sedan would have further linked Bailey to Dorsey (and thus to the robberies) could also reasonably have factored in to the magistrate judge's finding of probable cause.

***26** Bailey also argues that the information contained in the affidavit was stale, and could not support a reasonable belief that, more than seven months after the commission of the last robbery, Bailey would keep in his residence or a vehicle that he drove the Cowboy Gun, distinctive clothing, or other evidence. "The age of the information supporting the application for a warrant is a factor that a magistrate [judge] should consider. It is, however, only one factor. If other factors indicate that the information is reliable and that the object of the search will still be on the premises, then the magistrate [judge] should not hesitate to issue a warrant." *United States v. Batchelder,* 824 F.2d 563, 564 (7th Cir.1987) (finding probable cause to search for illegal gun silencers despite nine-month delay, where affiant indicated that individuals who purchased such silencers tend to keep them for extended periods of time). Here, it was reasonable to conclude that clothes that were not on their face incriminating would remain in Bailey's residence or a car he was driving, even several months after the last robbery. *See United States v. Jacobs,* 715 F.2d 1343, 1346 (9th Cir.1983) (per curiam) ("The articles of clothing identified in the affidavit and warrant were not unusual, nor incriminating in themselves. Although three and a half months passed between the earliest prior bank robbery in which the clothing sought had been worn by the robbers and the issuance of the warrant, it was reasonable for the magistrate to conclude that such articles of clothing would remain at the residence."). It was also reasonable to conclude that Bailey may have retained a distinctive and uncommon firearm that had been repeatedly used in a series of multiple robberies over a two-month span, and that the firearm might be found in Bailey's residence or the Kia sedan even several months later. *See United States v. Dozier,* 844 F.2d 701, 707 (9th Cir.1988) (in evaluating a staleness argument, an "important factor is the ongoing nature of a crime which might lead to the maintenance of tools of the trade"). Finally, it was reasonable to conclude, based on an affidavit that included facts going to how much of the allegedly stolen money could be accounted for by previous purchases, that Dorsey and Bailey may not have spent all of the robbery proceeds, and that significant amounts of cash might remain at Dorsey's residence or in the vehicle he had been using.

The Ninth Circuit and other courts have found probable cause for search warrants issued after sim-

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

ilar intervals and for similar evidence. *See, e.g., Dozier,* 844 F.2d at 707 (warrant for documentary records issued almost six months after an investigation, and despite intervening raid and arrest of others involved in marijuana cultivation operation); *United States v. Grandstaff,* 813 F.2d 1353, 1355–57 (9th Cir.1987) (per curiam) (reversing suppression of evidence obtained pursuant to warrant issued five months after robbery); *Jacobs,* 715 F.2d at 1346 (upholding search warrant for clothing worn by robbers issued three-and-a-half months after robbery); *United States v. Pelham,* 749 F.Supp. 304, 308–09 (D.D.C.1990) (finding probable cause despite six-month delay, and collecting cases for the proposition that a long delay is less significant where the "search warrant lists items innocent on their face" such as clothing). Here, the Court concludes that the magistrate judge's finding of probable cause was reasonable despite the seven-month gap between the last robbery and the issuance of the search warrant.

***27** For the foregoing reasons, the Court finds that the search warrant in question was supported by probable cause to believe that Bailey was one of the Cowboy Gun Bandits, and that there was a "fair probability" that evidence of the target crimes could be found in the residence and the Kia Sedan. At the very least, the government has carried its burden of showing that a reasonably well-trained executing officer could reasonably have relied on the validity of the warrant. *See United States v. Leon,* 468 U.S. 897, 922 (1984) (holding that evidence is admissible if the executing officers acted in objectively reasonable reliance on a facially valid warrant later found to be invalid). Therefore, the Court **DENIES** Bailey's motion to suppress evidence obtained from the residence and vehicle searches.

IX. DEFENDANTS' MOTIONS TO SEVER COUNTS AND DEFENDANTS

On December 24, 2014, Bailey filed a motion to sever the robbery counts from each other, and for a separate trial from Dorsey. Dkt. No. 48. On January 13, 2015, Dorsey joined in that motion and added limited briefing of his own. Dkt. No. 50. The government filed a consolidated opposition on January 26, 2015. Dkt. No. 57. For the following reasons, the motions are **DENIED.**

A. Legal Standards

An indictment "may charge a defendant in separate counts with 2 or more offenses if the offenses charged—whether felonies or misdemeanors or both—are of the same or similar character, or are based on the same act or transaction, or are connected with or constitute parts of a common scheme or plan." Fed.R.Crim.P. 8(a). An indictment "may charge 2 or more defendants if they are alleged to have participated in the same act or transaction, or in the same series of acts or transactions, constituting an offense or offenses." Fed. R. Crim P. 8(b). "[W]here both multiple defendants and multiple offenses are involved, the propriety of joinder is governed by Fed.R.Crim.P. 8(b)." *United States v. Guerrero,* 756 F.2d 1342, 1345 (9th Cir.1984) (citing *United States v. Ford,* 632 F.3d 1354, 1371 (9th Cir.1980)).

" '[B]ecause Rule 8 is concerned with the propriety of joining offenses in the indictment, the validity of the joinder is determined solely by the allegations in the indictment.' " *United States v. Jawara,* 474 F.3d 565, 573 (9th Cir.2006) (quoting *United States v. Terry,* 911 F.2d 272, 276 (9th Cir.1990)). "Rule 8 has been 'broadly construed in favor of initial joinder.' " *Id.* at 573 (quoting *United States v. Friedman,* 445 F.2d 1076, 1082 (9th Cir.1971)); *United States v. Armstrong,* 621 F.2d 951, 954 (9th Cir.1980) ("[J]oinder is the rule rather than the exception.").

Even where initial joinder was proper, "[i]f the joinder of offenses or defendants in an indictment ... appears to prejudice a defendant or the government, the court may order separate trials of counts, sever the defendants' trials, or provide any other relief that justice requires." Fed.R.Crim.P. 14(a). The decision whether to sever properly joined defendants under Rule 14 is "committed to the sound dis-

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

cretion of the trial court." *United States v. Adams,* 581 F.2d 193, 197 (9th Cir.1978).

B. Severance of Counts

***28** In this case, the substantive robbery counts were properly joined as the overt acts of a charged conspiracy. "Ordinarily, the mere charging of a conspiracy count linking together substantive counts against various defendants fully satisfies the Rule 8(b) requirement of relatedness and makes joinder proper under the rule." *United States v. Valenzuela,* 596 F.2d 824, 829 (9th Cir.1979); *see also United States v. Guerrero,* 756 F.2d 1342, 1345 (9th Cir.1984) ("As the conspiracy charged encompassed both the robbery and drug offenses, the joinder of these defendants and offenses was proper."); *Fernandez v. United States,* 329 F.2d 899, 905 (9th Cir.1964) ("In view of the conspiracy count wherein all of the defendants were alleged to have participated in the same series of acts or transactions constituting the offenses described in the substantive counts, the initial joinder of offenses and defendants in the two indictments was authorized under Rule 8(b)."); *United States v. Sexton,* 586 F. App'x 304, 305 (9th Cir.2014) (unpublished) ("The indictment alleges that the [three bank robberies] were committed in furtherance of a single, overarching conspiracy. The substantive counts were therefore part of a 'common scheme or plan' for joinder purposes.").

Further, neither defendant has shown grounds for severance under Rule 14. Bailey argues that severance is required or advisable because "distinctly different victims were [ ] robbed, namely a pizza restaurant, gas station stores and a bank." He contends that "it will be difficult for the jury to consider each robbery separately." Dkt. No. 48 at 8.[FN20] The government responds that the counts may properly be tried together because "[t]he charged robberies were all committed with[in] a span of 35 days, all involved the armed robbery of the employees of a business that transacted in cash, and all involved men in black hoodies, wearing masks or bandanas that covered their faces." The government also points out that the charged robberies took place in a relatively concentrated geographical area, and are linked as the overt acts of a charged conspiracy. Dkt. No. 57 at 3 & Ex. A. Finally, the prosecution argues that, even absent the conspiracy charge, evidence from the various counts would be admissible to prove the others because "identity is expected to be the central issue for trial" and significant modus operandi evidence will be introduced. *Id.* at 6.

FN20. Bailey also argues that the "prejudice is heightened" because of the 18 U.S.C. § 924(c) gun counts attached to the robbery charges, which provide for greater sentencing enhancements for a "second or subsequent conviction" than for a first conviction under the subsection. Dkt. No. 48 at 9. But Bailey cites no legal authority for the proposition that the charging of sentencing enhancements linked to the substantive counts militates in favor of severance.

The Court agrees with the prosecution. Bailey's arguments boil down to the generic proposition that a jury cannot compartmentalize evidence of distinct but similar crimes. But prejudice from a refusal "to sever counts can be cured by proper jury instructions, and juries are generally presumed to follow their instructions." *United States v. Hickerson,* 489 F.3d 742, 746 (5th Cir.2007). Bailey has advanced no persuasive reason to sever the properly joined robbery counts, and has not explained why the jury will be unable to separate evidence of the various counts. Moreover, evidence from one count may be admissible with regard to others to prove identity, further reducing the prejudice from joint trial. *See United States v. Johnson,* 820 F.2d 1065, 1070–71 (9th Cir.1987) (affirming denial of severance motion where evidence of one count would have been admissible to prove identity with regard to the other count under Federal Rule of Evidence 404(b)). In short, Bailey has not shown that a failure to sever will result in clear, manifest, or undue prejudice, so as to deny him a fair trial. *United States v. Fe-*

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

lix–Gutierrez, 940 F.2d 1200, 1209 (9th Cir.1991). *See Sexton,* 586 F. App'x at 305 (affirming refusal to sever three separate bank robberies); *United States v. Son Van Nguyen,* No. CR SP99–0433 WBS, 2002 WL 32103063, at *2–3 (E.D.Cal. Nov. 7, 2002) (rejecting an argument that charged robberies of a jewelry store should be severed from charged robberies of a computer store, finding a "logical relationship" and "large area of overlapping proof" between the counts).

***29** Dorsey adds no substantive argument on the propriety of a joint trial of the various counts. Therefore, neither defendant has met his burden of showing that the counts should be severed.

B. Severance of Defendants

1. Bailey Has Not Shown that Joinder Is Improper or Severance Justified.

The indictment properly joins Bailey and Dorsey as coconspirators alleged to have jointly carried out robberies that form the overt acts of the charged conspiracy. As discussed above, the Ninth Circuit has long "held that a conspiracy count will provide the necessary link to satisfy the requirements of Rule 8(b)." *United States v. Adams,* 581 F.2d 193, 197 (9th Cir.1978); *see United States v. Abushi,* 682 F.2d 1289, 1296 (9th Cir.1982) ("We have repeatedly held that a conspiracy count may provide the necessary link to satisfy the requirements of Rule 8(b).").

Nor has Bailey shown that joinder of the codefendants is so prejudicial as to warrant severance under Rule 14. "Generally, defendants who are indicted together in federal court should be jointly tried." *United States v. Tootick,* 952 F.2d 1078, 1080 (9th Cir.1991). "Joinder is favored in federal criminal cases largely for reasons of judicial economy and efficiency, despite some degree of bias inherent in joint trials." *Id.* On a Rule 14 motion, "[t]he burden of demonstrating prejudice rests on the [defendant], and is a heavy one." *Adams,* 581 F.2d at 198. The defendant "must show that 'joinder was so manifestly prejudicial that it outweigh[s] the dominant concern with judicial economy.' " *United States v. Garcia,* 506 F. App'x 593, 595 (9th Cir.2013) (unpublished) (quoting *United States v. Douglass,* 780 F.2d 1472, 1478 (9th Cir.1986)). It is not enough for a defendant to show that he "may have a better chance of acquittal in separate trials," [FN21] that his codefendant is more culpable,[FN22] or that the evidence against his codefendant is stronger.[FN23] This burden is especially heavy when a conspiracy is charged. *See United States v. Cruz,* 127 F.3d 791, 799 (9th Cir.1997), *abrogated on other grounds by United States v. Jiminez Recio,* 537 U.S. 270 (2003) ("A joint trial was particularly appropriate here because the defendants were charged with conspiracy."). This is so because where a conspiracy is charged, much of the evidence admitted against one defendant would be admissible against the other—even in a separate trial—as proof of the conspiracy. *See id.*

FN21. *Zafiro v. United States,* 506 U.S. 534, 540 (1993); *United States v. Tootick,* 952 F.2d 1078, 1080 (9th Cir.1991) ("Merely showing that a comparative advantage would result from separate trials will not satisfy [the defendant's] burden.").

FN22. *United States v. Van Cauwenberghe,* 827 F.2d 424, 432 (9th Cir.1987) ("[T]he mere fact that a criminal defendant is jointly tried with a more culpable codefendant is not alone sufficient to constitute an abuse of the district court's discretion.").

FN23. *United States v. Brady,* 579 F.2d 1121, 1127 (9th Cir.1978) ("[T]he fact that the evidence against one codefendant is more damaging than the evidence against another one is not a ground for severance.").

Bailey argues that he should be tried separately because the prosecution intends to offer evidence that Dorsey "originally made his money working as

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

a ‘pimp,’ but when his source of prostitutes disappeared, he resorted to the robberies to account for the lost income.” Dkt. No. 48 at 4. But the prosecution represents that it “does *not* intend to introduce, in its case-in-chief, the fact that Dorsey is a known ‘pimp’ ... or the fact that Bailey has at least three prior felony convictions for robbery.” Dkt. No. 57 at 2 (emphasis in original). Bailey's argument is therefore unpersuasive at this point and, to the extent that any of the prostitution-related evidence comes in as impeachment evidence, “[j]udicial economy justifies reliance on the jury to follow the instructions of the court that segregate the evidence and limit the applicability of the evidence to each defendant.” *United States v. Vaccaro,* 816 F.2d 443, 448 (9th Cir.), *cert denied,* 484 U.S. 928 (1987).

***30** Bailey also argues that he will be prejudiced by evidence that (1) Dorsey was found to be in possession of ammunition that purportedly matches the “Cowboy Gun” used in the charged robberies; (2) Dorsey was connected with the car belonging to Martin and allegedly used in some of the robberies; and (3) a security video shows Dorsey entering one of the robbed stores five minutes before it was robbed, wearing clothing that appears to match that worn by one of the suspects in previous robberies. The government responds that much of this evidence is also relevant to Bailey, arguing that, among other evidence linking Bailey and Dorsey, the same surveillance video capturing Dorsey's face shows a suspect who the government contends is Bailey committing the robbery a few minutes later. The government also posits that the ammunition “would be admitted against Bailey, as he brandished that firearm in several of the robberies.” Dkt. No. 57 at 10–11.

Without expressing any opinion on the ultimate admissibility of this evidence against Bailey, the Court finds that Bailey has not met his heavy burden of showing the type of prejudice that would justify severing the trials of alleged coconspirators. *See United States v. Matta–Ballesteros,* 71 F.3d 754, 771 (9th Cir.1995) (affirming district court's refusal to sever where codefendants were jointly tried for conspiring to commit and committing various violent acts, even though the joint trial meant the introduction of evidence involving three homicides and a marijuana enterprise with which the appellant was not involved). To the extent that any of the evidence Bailey identifies as prejudicial would not be admissible against him in a separate trial, “[t]he prejudicial effect of evidence relating to the guilt of co-defendants is generally held to be neutralized by careful instruction by the trial judge.” *United States v. Escalante,* 637 F.2d 1197, 1201 (9th Cir.1980); *see United States v. Van Cauwenberghe,* 827 F.2d 424, 432 (9th Cir.1987) (“When, as here, the District Court instructed the jury to consider the guilt or innocence of each co-defendant separately, in light of the evidence against that defendant, the jury is presumed to have obeyed.”); *Guerrero,* 756 F.2d at 1345–46 (“Although some of the evidence adduced at trial related only to the guilt of one or more, but less than all of the defendants, defendants have not satisfactorily demonstrated why the jury could not reasonably have compartmentalized the evidence against each defendant in view of the careful instructions given by the trial judge.”).

2. Dorsey Has Not Shown That Severance Is Justified.

Joining in Bailey's motion, Dorsey adds that Bailey has prepared an affidavit in which he “relates that Mr. Dorsey is not involved in any of the robberies that Mr. Bailey is charged with.” FN24 Dkt. No. 50 at 2. Dorsey argues that severance is mandatory because he has a right to call Bailey to testify on his behalf, and cannot do so if the two defendants are tried together.

FN24. Dorsey also states that “there are factors in the evidence concerning Mr. Bailey that would potentially prejudice the jury's consideration of the evidence against Mr. Dorsey.” Dkt. No. 50 at 2. But Dorsey provides no details that would permit the

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

Court to evaluate this claim.

***31** "Severance is rarely granted on the ground that a codefendant's testimony was excluded, primarily because considerations of judicial economy merit serious attention when defendants move for severance." *United States v. Hernandez,* 952 F.2d 1110, 1115 (9th Cir.1991) (internal quotation marks, citations, and brackets omitted). When a defendant argues for severance because of the need for a codefendant's testimony, he must show " '(1) that he would call the codefendant at a severed trial, (2) that the codefendant would in fact testify, and (3) that the testimony would be favorable to the moving party.' " *Id.* (quoting *United States v. Jenkins,* 785 F.2d 1387, 1393 (9th Cir.1986)). "In considering a defendant's claim that a codefendant will provide exculpatory testimony, a district court must weigh a number of factors, among them, the good faith of the defendant's intent to have a codefendant testify, the possible weight and credibility of the predicted testimony, the probability that such testimony will materialize, and the economy of a joint trial." *United States v. Mariscal,* 939 F .2d 884, 885 (9th Cir.1991) (internal quotation marks and brackets omitted); *see also United States v. Castro,* 887 F.2d 988, 998 (9th Cir.1989) ("The district court must then consider the weight and credibility of the proposed testimony and the economy of severance."). The court "must also consider the exculpatory nature and effect of the desired testimony-in other words, the degree to which the asserted codefendant testimony is exculpatory." *Mariscal,* 939 F.2d at 885. The movant "must show more than that the offered testimony would benefit him; he must show that the codefendant's testimony is 'substantially exculpatory' in order to succeed." *Id.* at 886 (quoting *United States v. Ford,* 870 F.2d 729, 732 (D.C.Cir.1989)).

Dorsey admits that "[i]t is not clear under what circumstances [ ] Mr. Bailey prepared and filed his declaration, or whether he was represented by counsel at the time," and that he is unable to specify what the testimony would be because Dorsey's defense counsel cannot speak with Bailey. *Id.* at 2–4. Dorsey nevertheless submits that Bailey "would be prepared to testify and provide exculpatory evidence" on Dorsey's behalf. *Id.* at 2–3.

At present, Dorsey has not met his burden of showing that Bailey's purportedly exculpatory testimony justifies severance. The Court finds persuasive the D.C. Circuit's analysis of a similarly vague and uncertain proffer of exculpatory codefendant testimony. *See United States v. Ford,* 870 F.2d 729 (D.C.Cir.1989), *cited with approval in Mariscal,* 939 F.2d at 885–86. In that case, counsel for the appellant, Ford, had represented that Ford's codefendant, Green, would provide exculpatory testimony on Ford's behalf if the trials were severed. The court first found that the Ford had not sufficiently shown that Green would be willing to testify, even though counsel for both codefendants had said that he would, because the offer of testimony "was conditioned on Green's case being tried first." *Id.* at 731. The court noted widespread judicial disapproval of this type of conditional offer, and warned that Rule 14 is not "a mechanism for alleged co-conspirators to control the order in which they are tried." *Id* . (citing *United States v. Gay,* 567 F.2d 916, 919–20 (9th Cir.1978)). The court then held that Ford had "failed to meet the burden of establishing with requisite specificity the exculpatory 'nature and effect' of his co-defendant's testimony." *Id.* at 732. The court explained:

> ***32** [T]he nature of Green's expected testimony was addressed by counsel on three separate occasions. First, when appellant's counsel initially moved for severance, he simply stated his belief that Green would provide exculpatory evidence. Later, Green's counsel added his understanding of Green's expected testimony (that appellant "had nothing to do with the transaction"). Finally, at the close of the government's case, appellant's counsel raised the severance issue again, stating that Green "would testify that Mr. Ford never got out of the car and didn't participate in the transaction." None of these statements are of sufficient

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

> specificity to warrant overturning the District Court's determination [not to sever]. In essence, these statements reduce to a reaffirmation of appellant's "not guilty" plea. They represent an assertion of ultimate fact, but do not provide the specific facts necessary for the District Court to determine that the movant "will be unable to obtain a fair trial without severance ."

Id. (paragraph structure altered; citations omitted).

Here, it is even less certain that Bailey would in fact testify on Dorsey's behalf, because the Court does not have Bailey's position on whether he would testify, and Dorsey admits that it is unclear under what circumstances Dorsey prepared the affidavit, or whether he was represented by counsel at the time. As in *Ford*, the fact that Dorsey is attempting to control the order in which the codefendants are tried counsels caution. *See* Dkt. No. 50 at 5 ("[T]he court should grant Mr. Dorsey's request to sever the trials and permit Mr. Dorsey to conduct his trial after that of Mr. Bailey, so that [Dorsey] can call [Bailey] as a witness."). Additionally, Dorsey has not provided specific details of how Bailey's testimony would exculpate him, other than generally denying Dorsey's involvement—that is, Dorsey has "not provide[d] the specific facts necessary for the District Court to determine that the movant will be unable to obtain a fair trial without severance." *Ford*, 870 F.2d at 732 (internal quotation marks omitted). Accordingly, Dorsey has not shown that Bailey would in fact testify on his behalf, and that the testimony would be significantly favorable to Dorsey and non-cumulative. *Hernandez*, 952 F.2d at 1115.[FN25]

> FN25. At oral argument, Dorsey's counsel submitted that he did not have any additional information regarding Bailey's potential testimony, but asked that any denial of his motion to sever defendants be granted without prejudice to Dorsey's making a more detailed showing of Bailey's potential testimony at a future date. This motion is granted without prejudice to Dorsey's making such a showing.

For these reasons, the Court **DENIES** the motions to sever counts and defendants, without prejudice to a showing of new facts in support of severance.

X. BAILEY'S MOTION TO SUPPRESS POST–ARREST, PRE–MIRANDA STATEMENTS

On December 24, 2014, Bailey filed a motion to suppress statements he made after his arrest but before being advised of his rights under *Miranda v. Arizona*, 384 U.S. 436 (1966). Dkt. No. 49. Under that decision, a suspect in custody must be advised, in substance, as follows:

> "He must be warned prior to any questioning that he has the right to remain silent, that anything he says can be used against him in a court of law, that he has the right to the presence of an attorney, and that if he cannot afford an attorney one will be appointed for him prior to any questioning if he so desires."

***33** *Berghuis v. Thompkins*, 560 U.S. 370, 380 (2010) (quoting *Miranda*, 384 U.S. at 479). "Before a defendant's self-incriminating statements may be admitted into evidence, 'a heavy burden rests on the government to demonstrate that the defendant knowingly and intelligently waived his privilege against self-incrimination and his right to retained or appointed counsel.' " *United States v. Rodriguez*, 518 F.3d 1072, 1076 (9th Cir.2008) (quoting *Miranda*, 384 U.S. at 475). "Statements obtained in violation of *Miranda* generally are inadmissible in the government's case-in-chief. But a defendant's voluntary statements—even if obtained in violation of *Miranda* —are admissible as impeachment evidence." *United States v. Gomez*, 725 F.3d 1121, 1125–26 (9th Cir.2013) (citations omitted); *see also Oregon v. Elstad*, 470 U.S. 298, 307 (1985) ("Despite the fact that patently voluntary statements taken in violation of Miranda must be excluded from the prosecution's case, the presumption of co-

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

ercion does not bar their use for impeachment purposes on cross-examination." (emphasis omitted)).

On January 26, 2015, the government filed a response stating that it will not seek to introduce "any statements Bailey made during his post-arrest interview unless the defense, either through cross-examination or in the defense case, opens the door to any of his post-arrest statements." Dkt. No. 65. The prosecution states that if this occurs, it will "seek a ruling regarding the admissibility of his statements before raising them in front of the jury." *Id.* Because it is unopposed, the Court **GRANTS** this motion without prejudice to the government seeking a ruling at trial that Bailey has opened the door to impeachment with otherwise inadmissible pre-*Miranda* warning statements.

XI. DORSEY'S MOTION TO PRECLUDE USE BY THE PROSECUTION OF ALLEGATIONS OF OTHER CRIMES, WRONGS, OR ACTS

On January 13, 2015, Dorsey filed a motion to preclude the prosecution from offering evidence or allegations that Dorsey acted as a "pimp" or was otherwise involved in the business of prostitution. Dkt. No. 53. Dorsey contends that such evidence would be irrelevant and unfairly prejudicial, and should be excluded under Federal Rule of Evidence 404(b). *See* Fed.R.Evid. 404(b)(1) ("Evidence of a crime, wrong, or other act is not admissible to prove a person's character in order to show that on a particular occasion the person acted in accordance with the character.").

On January 26, 2015, the government filed a response stating that it does not intend to introduce evidence of Dorsey's alleged prostitution-related conduct in its case-in-chief. Dkt. No. 61. The government maintains, however, that it may seek to admit such testimony if Dorsey "opens the door" to such evidence at trial.[FN26] *Id.* The government also asserts that evidence in the possession of persons who allegedly worked for Dorsey as prostitutes could "be admitted without discussing Dorsey's relationship to the witness." *Id.* Because it is unopposed, the Court **GRANTS** this motion without prejudice to the government seeking a ruling at trial that Dorsey has opened the door to the type of evidence discussed herein.

FN26. "Federal Rule of Evidence 404 restricts the use of evidence solely for purposes of demonstrating a criminal proclivity. It does not proscribe the use of other act evidence as an impeachment tool during cross-examination." *United States v. Gay*, 967 F.2d 322, 328 (9th Cir.1992). Therefore, "404(b) evidence may be used for impeachment purposes." *Id.*

XII. CONCLUSION

***34** In accordance with the foregoing, the Court **GRANTS:**

• Dkt. No. 49: Motion to suppress post-arrest statements (without prejudice to the government's seeking a ruling on admissibility for impeachment purposes at trial);

• Dkt. No. 53: Motion to preclude other act evidence (without prejudice to the government seeking a ruling at trial that Dorsey has opened the door to such evidence).

The Court **DENIES**:

• Dkt. No. 42: Motions to dismiss indictment on jurisdictional grounds;

• Dkt. No 43: Motion to suppress evidence from state cell site "warrant";

• Dkt. No. 44: Motion to suppress evidence from federal cell site warrant;

• Dkt. No. 45: Motion to suppress bank account information;

• Dkt. No. 47: Motion to suppress residence and vehicle searches;

• Dkt. No. 48: Motion to sever;

• Dkt. No. 50: Motion to sever;

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

- Dkt. No. 51: Motion to dismiss indictment on jurisdictional grounds;

- Dkt. No. 54: Motion for an evidentiary hearing with regard to federal cell site warrant.

As indicated in section VII, the Court defers ruling on the traffic stop suppression motion, and will conduct an *in camera* review of the subpoenaed documents related to that traffic stop to determine if they should be produced to the defense.

IT IS SO ORDERED.

C.D.Cal.,2015.
U.S. v. Dorsey
Not Reported in F.Supp.3d, 2015 WL 847395 (C.D.Cal.)

END OF DOCUMENT

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

2015 WL 881578
Only the Westlaw citation is currently available.
United States District Court,
N.D. California.

United States of America, Plaintiff,
v.
Elijah Cooper, Defendant.

Case No. 13–cr–00693–SI–1 | Signed March 2, 2015

Attorneys and Law Firms

Benjamin Patrick Tolkoff, United States Attorney's Office, San Francisco, CA, for Plaintiff.

ORDER DENYING DEFENDANT'S MOTIONS TO SUPPRESS

Re: Dkt. Nos. 72, 73

SUSAN ILLSTON, United States District Judge

***1** On February 6 and February 27, 2015, the Court heard argument on defendant's motions to suppress. For the reasons set forth below, the Court **DENIES** defendant's motions.

BACKGROUND

On February 5, 2013, a confidential human source ("CHS"), working with the FBI, engaged in a controlled narcotics purchase with suspect Anthony Knight. Declaration of Ethan A. Balogh ("Balogh Decl.") Ex. B. While the CHS was discussing the terms of the buy with Knight, a white Mercedes pulled into the parking lot and Knight went to meet with the driver of the Mercedes. *Id.* The Mercedes then drove away again. *Id.* Knight then got into the CHS's car, gave the CHS an ounce of crack cocaine, and told the CHS that Knight's supplier had to go back and get the remainder of the drugs. *Id.* When the Mercedes returned to the parking lot, Knight went to meet with the Mercedes's driver again, and then gave the CHS the remainder of the drugs the CHS had paid for. *Id.*

The FBI sought to ascertain who had been driving the white Mercedes. A query to the California Department of Motor Vehicles, based upon the car's license plate number, revealed that the car was registered to a Johnny Ray Trammell. *Id.* Ex. H ¶ 64 n.11. The CHS was shown a photo of Trammell, but the CHS said that the driver of the Mercedes was younger looking. with close cropped hair. *Id.* ¶ 71. The CHS was then shown a photo of Tony Befford; the CHS identified Befford as the driver. *Id.*

Agents then tried to verify the CHS's identification of the driver as Befford. *Id.* ¶ 72. The agents conducted further surveillance of the white Mercedes, but concluded that the driver was not Befford. *Id.* The agents then asked the San Francisco Police Department ("SFPD") to conduct a traffic stop to determine who the driver was. *Id.* The SFPD complied, and identified the driver as defendant Elijah Cooper. *Id.* Cooper was wearing a royal blue hooded sweatshirt when the SFPD conducted the traffic stop. *Id.*

On February 6, 2013, federal agents asked the CHS about the misidentification of Cooper as Befford. *Id.* ¶ 73. The CHS was then shown a photo of Cooper; the CHS identified Cooper as the driver of the white Mercedes. *Id.* The CHS stated that, during the controlled buy, Cooper's hair was "a bit longer" than depicted in the photo. *Id.* Ex. D. One agent asked the CHS what the driver had been wearing during the controlled drug buy. *Id.* Ex. H. ¶ 73. The CHS responded that the driver of the white Mercedes had been wearing a "royal blue hoodie." *Id.*

On February 21, 2013, the government sought a wiretap for Knight's telephone, and named several individuals, including Cooper, as target subjects for surveillance. *Id.* Ex. G, at 2. On April 4, 2013, the government sought two more wiretaps, one of which was for Cooper's mobile phone. *Id.* Ex. L.

The FBI agents were aware that Cooper, at that time, was serving a term of supervised release for a prior narcotics trafficking conviction. Declaration of Jacob D. Millspaugh ("Millspaugh Decl.") ¶ 2. The agents decided not to contact Cooper directly because they believed that the contact would be noticed and Cooper would be considered a snitch, and thereby placed in danger. *Id.* Therefore, the agents decided to contact Cooper's probation officer, Octavio Magaña, to see if he could help arrange a meeting. *Id.*

***2** On August 16, 2013, FBI agents, SFPD officers, and an Assistant U.S. Attorney ("AUSA") went to Mr. Magafia's office to meet with Cooper. *Id.* ¶ 3. After Cooper arrived and learned who all the individuals were, Cooper was advised that

they had evidence he was engaged in drug dealing, and that it was in his interest to cooperate with them. *Id.* Cooper was not questioned about the crimes under investigation; rather, he was told about some of the evidence against him. *Id.*

On September 26, 2013, following weeks in which Cooper never responded regarding his willingness to cooperate, agents swore out a criminal complaint against Cooper for distribution of cocaine base and conspiracy to distribute. *Id.* ¶ 5. On October 4, 2013, the FBI agents, SFPD officers, and an AUSA, again went to Mr. Magaña's office to meet with Cooper. *Id.* ¶ 6. The AUSA asked Cooper if he had considered what had been discussed at the August, 2013 meeting. *Id.* Cooper stated that he wanted to see a lawyer. *Id.* He was immediately arrested. *Id.*

Two SFPD officers then transported Cooper to the San Francisco Hall of Justice for post-arrest processing. *Id.* ¶ 7. According to Cooper, he was placed in an interrogation room, shown photos of men from his neighborhood, and asked questions about the activities of those men. Declaration of Elijah Cooper ("Cooper Decl.") ¶ 6. Cooper declined to answer any questions. *Id.* Because Cooper was arrested after the Friday morning magistrate calendar had already concluded, Cooper was lodged at the San Francisco County Jail until he could be arraigned on the following Monday. Millspaugh Decl. ¶ 7.

On October 17, 2013, the grand jury returned a two-count indictment against Cooper, charging him with: (1) distribution of cocaine base, in violation of 21 U.S.C. §§ 841(a)(1), 841 (b)(1)(B)(iii); and (2) conspiracy to distribute cocaine base, in violation of 21 U.S.C. § 846. On July 31, 2014, this Court ruled on eight motions filed by defendant. Docket No. 65. The Court granted defendant's motion to dismiss Count Two of the indictment. *Id.* at 7. On August 28, 2014, the grand jury returned a superseding indictment, charging the same two counts as the original indictment. Docket No. 67.

On November 12, 2014, the Court issued an order dismissing Count Two of the Superseding Indictment, and ordered additional briefing on defendant's motions to suppress, and ordering the government to provide Cooper with certain evidence pertaining to his motions. Docket No. 87. The Court noted in pertinent part:

> The Court finds that it is currently unable to rule on these motions for two reasons. First, there is a significant asymmetry of information between the parties which has heretofore prevented a robust adversarial exchange and meaningful briefing on the defendant's suppression motions. This asymmetry of information stems from the government's refusal to provide Cooper with the applications and orders conferring judicial authorization to obtain pen register, trap and trace, and cell site data. This has led to confusion as to the specific statutory provisions the government relied upon to conduct its various forms of surveillance. Second, the government has simply failed to respond to many of Cooper's substantive arguments.

Id. at 6.

The Court will now proceed to address Cooper's motions to suppress in light of the parties' supplemental briefing.

DISCUSSION

I. Motion to Suppress Evidence Obtained Through Pen Registers and Trap and Trace Devices

***3** Cooper moves to suppress evidence obtained through pen register and trap and trace devices. In an earlier order addressing this issue, the Court noted that the parties presented substantially different accounts premised on highly conflicting information, and that there was some confusion amongst the parties as to what was actually collected through this monitoring process. Docket No. 65 at 25. The Court therefore ordered additional briefing on the issue,[1] specifically requesting that the parties explain (1) what information was collected, (2) how it was collected, and include (3) attached exhibits containing the actual evidence collected. *Id.* In response the government filed a declaration from a Metro PCS employee which describes the information the government collected. The information, which the government terms "pen register data," in the case at bar includes the "incoming call number, outgoing call number, duration of call, call date, time call began, [and] time call ended." Docket No. 66, Thompson Decl. ¶ 3. In addition, the data indicates the geographic coordinates (longitude and latitude) of the cell tower used when the call was initiated, and

the tower used at the conclusion of the call ("cell site data"). *Id.* The government was able to obtain this information over a period of 120 days (the 60 days preceding the issuance of the magistrate's order, and 60 days following the issuance of the order).

Cooper argues that this data should be suppressed because (1) the Pen Statute requires a finding of probable cause to obtain prospective cell site data, and (2) the Fourth Amendment requires a showing of probable cause to obtain historical cell site data. The government disagrees, relying on a "hybrid theory" to argue that a lower showing is required.

A. Statutory Framework

(i). The Pen Statute

The Electronic Communications Privacy Act ("ECPA") regulates the means by which government entities may obtain the information of private citizens through electronic surveillance. Title III of the ECPA (the "Pen Statute") governs the use of pen registers and trap and trace devices, and was enacted "to protect effectively the privacy of wire and oral communications." *Bartnicki v. Vopper*, 532 U.S. 514, 523 (2001). A trap and trace device is "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication." 18 U.S.C.A. § 3127(4). A pen register is "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted." 18 U.S.C.A. § 3127(3). Under the Pen Statute, a court *shall* enter an order authorizing the use of a pen register or trap and trace device "if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation." 18 U.S.C.A. § 3123.

In 1994, Congress passed the Communications Assistance of Law Enforcement Act ("CALEA"), which amended certain provisions of the ECPA. In particular, the CALEA prohibits the government from relying solely upon the Pen Statute to obtain cell site data. 47 U.S.C. § 1002(a)(2)(B) ("with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices [...], such call identifying information shall not include any information that may disclose the physical location of the subscriber."). While the CALEA clearly bars the government from obtaining authorization to obtain cell site data by merely showing that its "use is relevant to an ongoing criminal investigation," it did not explicitly establish a standard for obtaining such data. However, in the absence of congressional intent to the contrary, Federal Rule of Criminal Procedure 41"provid[es] a default mode of analysis that governs any matter in which the government seeks judicial authorization to engage in certain investigative activities." *In re Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device*, 396 F.Supp.2d 294, 322 (E.D.N.Y.2005). Under Rule 41, the government must make a showing of "probable cause."

***4** While the question has not been directly addressed by the Ninth Circuit, a number of courts have found that Rule 41 provides the appropriate standard for obtaining prospective, or "real-time," cell site data.[2] *See e.g.United States v. Espudo*, 954 F.Supp.2d 1029, 1043 (S.D.Cal.2013) ("Upon review of the statutory scheme, the Court finds that an application for real-time cell site location data does not implicate any statute regulating search or seizure or special circumstances. Accordingly, the terms of Rule 41 govern in the present case."); *cf.In re U.S. for an Order Authorizing Monitoring of Geolocation & Cell Site Data for a Sprint Spectrum Cell Phone No.*, No. MISC. 06–0186, 2006 WL 6217584, at *4 (D.D.C. Aug. 25, 2006).

(ii). The SCA

Title II of the ECPA, the Stored Communications Act ("SCA"), governs requests for access to stored records, including historical cell site data. Under the SCA, the government may obtain an order to access such records "only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).[3]

B. Prospective Cell Site Data

As discussed above, under the CALEA, a showing of probable cause is required to obtain prospective, or real-time, cell site data. However, the government contends that it may rely on the SCA's lower showing of "specific and

articulable facts" to obtain real-time cell site data on a prospective basis. The government's position arises from its fundamental disagreement with the binary distinction between prospective versus retrospective cell site data. 12/12/14 Sealed Government Brief at 3 ("whether the records are 'historical' or are captured by the phone company and sent out shortly thereafter or 'prospectively' the showing that the government must make to receive the records is the same—specific and articulable facts.").

The government's position—which has been coined the "hybrid theory" by other courts—is that it may simultaneously rely on provisions of the Pen Statute and the SCA to obtain real time cell site data on the lower showing of "specific and articulable facts." The hybrid theory relies on the wording of the CALEA which prohibits the government from obtaining cell site data "*solely* pursuant to the authority for pen registers and trap and trace devices." 47 U.S.C. § 1002(a)(2)(B) (emphasis added). By combining the SCA with the Pen Statute, the Government claims to have complied with the CALEA because it is not *solely* relying on the Pen Statute. Therefore, under the government's hybrid theory, the SCA governs access not only to data which is electronically stored at the time the government seeks access to it, but also to data that is not in existence but that will be recorded and stored at some point in the future.

***5** However, as its name might suggest, the *Stored* Communications Act's "entire focus ... is to describe the circumstances under which the government can compel disclosure of existing communications and transaction records in the hands of third party providers .... Nothing in the SCA contemplates a new form of ongoing surveillance." *Espudo,* 954 F.Supp.2d at 1036. As the *Espudo* court highlighted, the distinctions between the SCA and other provisions of the ECPA put this fact into relief.

> Wiretap orders authorize a maximum surveillance period of 30 days which begins to run no later than 10 days after the order is entered. 18 U.S.C. § 2518(5). Pen/trap orders authorize the installation and use of a pen register for a period "not to exceed sixty days." 18 U.S.C. § 3123(c)(1). By contrast, Congress imposed no duration period whatsoever for § 2703(d) orders. Likewise, Congress expressly provided that both wiretap orders and pen/trap orders may be extended by the court for limited periods of time. 18 U.S.C. §§ 2518(5), 3123(c)(2). There is no similar provision for extending § 2703(d) orders ... Another notable omission from § 2703(d) is sealing of court records. Wiretap orders and pen/trap orders are automatically sealed, reflecting the need to keep the ongoing surveillance under wraps. 18 U.S.C. §§ 2518(8)(b), 3123(d)(1). The SCA does not mention sealing. Pen/trap orders must also direct that the service providers not disclose the existence of the order to third parties until otherwise ordered by the court. 18 U.S.C. § 3123(d)(2). Section 2705(b) of the SCA authorizes the court to enter a similar non-disclosure order, but only upon a showing of possible adverse consequences, such as "seriously jeopardizing an investigation or unduly delaying a trial." 18 U.S.C. § 2705(b)(1–5).

Id. at 1036–37.

The cumulative weight of these distinctions shows Congress's intent that the SCA was to be used as a means to obtain data which has already been stored at the time the government seeks to obtain it. While the government relies primary on three cases—from the Southern District of New York and Northern District of Georgia—which lend support to its "hybrid theory," the majority of courts have rejected it as an attempt to circumvent the CALEA's mandate that real time cell site data may be obtained only by a showing of probable cause. *In re Application of U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel.,* No. 06 CRIM. MISC. 01, 2006 WL 468300, at *1 (S.D.N.Y. Feb. 28, 2006) ("join[ing] eight decisions by seven other Magistrate Judges" in rejecting the hybrid theory); *In re U.S. For an Order Authorizing the Disclosure of Prospective Cell Site Info.,* 412 F.Supp.2d 947, 956 (E.D.Wis.2006)*aff'd,*No. 06–MISC–004, 2006 WL 2871743 (E.D.Wis. Oct. 6, 2006) (relying in part on congressional testimony of FBI Director to reject hybrid theory); *In re U.S. for Orders Authorizing Installation & Use of Pen Registers & Caller Identification Devices on Tel. Numbers,* 416 F.Supp.2d 390, 396 (D.Md.2006) (the hybrid theory "leaves the court with authority that is at best murky and, at worst, illusory."); *In re U.S. for an Order Authorizing Monitoring of Geolocation & Cell Site Data for a Sprint Spectrum Cell Phone No.,* No. MISC. 06–0186, 2006 WL 6217584, at *2 (D.D.C. Aug. 25, 2006) ("Most of the Magistrate Judges that have considered the hybrid theory have found it to be unavailing."); *In re Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device,* 396 F.Supp.2d 294, 318 (E.D.N.Y.2005) (disapproving of "the fallacy of the [hybrid theory's] overarching endeavor of stitching together disparate laws to achieve a result that none alone permits."). Accordingly, the Court joins the growing number of district courts which have rejected the hybrid theory's contorted statutory interpretation. A contrary decision would

circumvent the very safeguards Congress meant to put in place by enacting the CALEA.

C. Historical Cell Site Data

***6** Cooper also argues that the government must make a showing of probable cause in order to obtain historical cell site data, and that its failure to do so violates his rights under the Fourth Amendment. Conversely, the government argues that it need only comply with the SCA's required showing of "specific and articulable facts." 18 U.S.C. § 2703(d).

The Fourth Amendment protects the right of the people to be secure in their "persons, houses, papers, and effects" against unreasonable searches and seizures. U.S. Const. amend. IV. "A search occurs for Fourth Amendment purposes when the government physically intrudes upon one of these enumerated areas, or invades a protected privacy interest, for the purpose of obtaining information." *Patel v. City of Los Angeles,* 738 F.3d 1058, 1061 (9th Cir.2013). In order to establish a violation, the defendant must show that he "can claim a justifiable, a reasonable, or a legitimate expectation of privacy that has been invaded by government action." *Smith v. Maryland,* 442 U.S. 735, 740 (1979) (internal quotation marks omitted); *see also*Crowley v. Holmes, 107 F.3d 15 (9th Cir.1997) ("To establish a Fourth Amendment violation, a plaintiff must show that he had an objectively reasonable expectation of privacy.") (internal citations omitted).

In *Smith v. Maryland,* 442 U.S. 735(1979), the Supreme Court held that the warrantless use of pen registers did not violate the Fourth Amendment, even when a call was placed from within the caller's home. The Court noted that while individuals have a reasonable expectation of privacy in the *content* of their phone conversations, the Fourth Amendment does not extend to information collected by pen registers. However, the pen registers employed in 1979 bear little resemblance to their modern day counterparts. In the early years, "a law enforcement official could not even determine from the use of a pen register whether a communication existed ... They disclose[d] only the telephone numbers that have been dialed—a means of establishing communication. [They did not capture] any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed [was] disclosed." *Id.* at 741, *citing*United States v. New York Tel. Co., 434 U.S. 159, 167 (1977). Therefore *Smith* does not answer the question of whether persons who place a call have a reasonable expectation of privacy in their location as conveyed by historical cell site data. *Cf.Riley v. California,* 134 S.Ct. 2473, 2488 (2014) (The Supreme Court recently rejected the government's reliance on old cases holding that police could search the physical belongings of an arrestee, in order to justify searching the data on an arrestee's cell phone: "That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together.").

In *United States v. Jones,* 132 S.Ct. 945 (2012), the Supreme Court held that the installation of a GPS device on the defendant's car, tracking his movements for a month, violated his rights under the Fourth Amendment. The majority opinion, authored by Justice Scalia and joined by three other Justices, held that the installation of the GPS device constituted a warrantless physical trespass onto the defendant's property; as such, the majority found it unnecessary to reach the question of whether the defendant had a reasonable expectation of privacy in his physical location over the course of a month. Justice Sotomayor concurred with the majority's reasoning, but wrote separately to discuss the potential applicability of individual privacy rights in the digital collection of information indicating their location. Finally, Justice Alito, joined by three other Justices, authored a concurrence which held that Jones did indeed have a reasonable expectation of privacy in the location data conveyed by the GPS device.

***7** In her concurrence, Justice Sotomayor notes that GPS monitoring "generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations," and that the government's ability to obtain such information without a warrant "may alter the relationship between citizen and government in a way that is inimical to democratic society." *Id.* at 955–56 (Sotomayor, J., concurring) (internal citations omitted). She further questioned the vitality of the idea that individuals have no expectation of privacy in information voluntarily disclosed to third parties, noting that it is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *Id.* at 957. Justice Alito's concurrence went a step further, noting that "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy ... [S]ociety's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period." *Id.* at 964 (Alito, J., concurring).

The Sotomayor and Alito concurrences implicitly adopt the reasoning of the lower court, which held that although Jones' movements were publicly visible, "the whole of one's movements is not exposed *constructively* even though each individual movement is exposed, because that whole reveals more—sometimes a great deal more—than does the sum of its parts." *United States v. Maynard,* 615 F.3d 544, 558 (D.C.Cir.2010) (emphasis in original). Additionally, even though the majority in *Jones* rested its holding solely upon the trespassory nature of the installation of the tracking device, it also recognized that "[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to [the] *Katz* analysis [employed in the concurrences]." *United States v. Jones* 132 S.Ct. at 953 (emphasis in original).

United States v. Davis, 754 F.3d 1205, 1215 (11th Cir.)*vacated pending reh'g en banc,*573 Fed.Appx. 925 (11th Cir.2014) [4] is the only case to have considered a suppression motion raising the precise issue of whether warrantless collection of historical cell site data violates a criminal defendant's Fourth Amendment rights. [5] The Davis court conducted an exhaustive historical survey of Supreme Court Fourth Amendment jurisprudence, including the recent Jones decision. It ultimately held that historical cell site data is within the subscriber's reasonable expectation of privacy. *Id.* at 1218. The court highlighted three primary distinctions between the GPS data (analyzed in *Jones*) and historical cell site data, which militated in favor of finding that a person has a reasonable expectation of privacy in their location as conveyed by historical cell site data. First, it noted that while an automobile is generally confined to traveling on public roadways, a cell phone "can accompany its owner anywhere. Thus, the exposure of the cell site location information can convert what would otherwise be a private event into a public one." *Id.* at 1216. Second, unlike GPS data, cell site data "is private in nature rather than being public data that warrants privacy protection only when its collection creates a sufficient mosaic to expose that which would otherwise be private." *Id.* Third, the fact that GPS data may be more precise has no "constitutional significance." *Id.*

While the Ninth Circuit has yet to address this precise question, the Court finds no case which would foreclose adopting the reasoning espoused in *Davis.* In *United States v. Forrester,* 512 F.3d 500 (9th Cir.2008), the court held that computer users had no reasonable expectation of privacy in the "to/from" addresses of email messages, or the IP addresses of the websites they visited. However, it noted that its "holding extends only to these particular techniques and does not imply that more intrusive techniques or techniques that reveal more content [*sic*] information are also constitutionally identical." *Id.* at 511. Additionally, in *United States v. Reyes,* 435 Fed.Appx. 596 (9th Cir.2011), the court declined to address the defendant's argument that the government's collection of his cell site data violated the Fourth Amendment because he failed to raise the issue before the trial court. Nonetheless, the court noted that "[t]he government's use at trial of Reyes's cell site location information raises important and troublesome privacy questions not yet addressed by this court." *Id.* at 598.

***8** Technological advances, coupled with declining cost, have rendered cell phones ubiquitous, and for many, an indispensible gizmo to navigate the social, economic, cultural and professional realms of modern society. *SeeJones,* 132 S.Ct. at 963 (there are "more than 322 million wireless devices in use in the United States."). This dynamic dictates that many, if not most, will find their cell phone quite literally attached to their hip throughout the day. *SeeRiley v. California,* 134 S.Ct. 2473, 2484, 189 L.Ed.2d 430 (2014) (cell phones are "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."). All the while, these phones connect to cell towers, and thereby transmit enormous amounts of data, detailing the phone-owner's physical location any time he or she places or receives a call or text. [6] Cell phone users may assume that the numbers they dial will be transmitted to the phone company, thus defeating any reasonable expectation of privacy. However, "there is no indication to the user that making that call will also locate the caller; when a cell phone user receives a call, he hasn't voluntarily exposed anything at all." *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, 317–18 (3d Cir.2010). A cell phone user's reasonable expectation of privacy in his or her location is especially acute when the call is made from a constitutionally protected area, such as inside a home, but is also reasonable even when the call is made in public. *See Davis* 754 F.3d at 127; *cf.Katz* 389 U.S. at 352 ("[Defendant] did not shed his right [to privacy] simply because he made his calls from a place where he might be seen."); *Smith* 442 U.S. at 743 (the "site of the call is immaterial for purposes of [Fourth Amendment] analysis.").

Society's expectation of privacy in historical cell site data is also evidenced by many state statutes and cases which suggest that this information exists within the ambit

of an individual's personal and private realm. *SeeTracey v. State,* 152 So.3d 504, 526 (Fla.2014) (reasonable expectation of privacy in real-time cell site data under U.S. Constitution); *Commonwealth v. Augustine,* 467 Mass. 230, 255 (2014) (under state constitution, defendant had reasonable expectation of privacy in cell site data, requiring government to obtain a warrant before seeking it); *State v. Earls,* 214 N.J. 564, 588 (2013) (same); Colo.Rev.Stat. Ann. § 16–3–303.5(2) (requiring warrant to obtain cell site data); 16 Me.Rev.Stat. § 648 (same); Minn.Stat. Ann. §§ 626A.28(3)(d), 626A.42(2) (same); Mont.Code Ann. § 46–5–110(1)(a) (same); Utah Code Ann. § 77–23c–102(1)(a) (same); *cf.People v. McKunes,* 51 Cal.App.3d 487, 492 (Ct.App.1975) (finding a right to privacy in phone records, reasoning that "in this age and place, it is virtually impossible for an individual or a business entity to function in the economic sphere without a telephone and that a record of telephone calls also may provide a virtual current biography.") (internal citations omitted). While state law is, of course, not dispositive on this question, "the recognition of a privacy right by numerous states may provide insight into broad societal expectations of privacy." *United States v. Velasquez,* No. CR 08–0730 WHA, 2010 WL 4286276, at *5 (N.D.Cal. Oct. 22, 2010); *see alsoTrujillo v. City of Ontario,* 428 F.Supp.2d 1094, 1106 (C.D.Cal.2006)*aff'd sub nom.Bernhard v. City of Ontario,* 270 Fed.Appx. 518 (9th Cir.2008) (the "laws that prohibit or regulate conduct in locker rooms ... represent society's understanding that a locker room is a private place requiring special protection."); *Maynard,* 615 F.3d at 564 ("state laws are indicative that prolonged GPS monitoring defeats an expectation of privacy that our society recognizes as reasonable.").

The government has many important and appropriate reasons for tracking the cell site data of suspected criminals. Today, the Court only holds that the Fourth Amendment provides the appropriate mechanism to balance the government's interest in law enforcement and the people's right to privacy in their physical location as conveyed by historical cell site data over a period of 60 days.

To be clear, the SCA makes no mention of cell site data, but rather speaks in general terms of "records concerning electronic communication." As a matter of statutory construction, it is axiomatic that "where an otherwise acceptable construction of a statute would raise serious constitutional problems, the Court will construe the statute to avoid such problems unless such construction is plainly contrary to the intent of Congress." *Edward J. DeBartolo Corp. v. Florida Gulf Coast Bldg. & Const. Trades Council,* 485 U.S. 568, 575 (1988). Accordingly, the Court does not find the SCA to be constitutionally deficient. Rather, the Court assumes, as it must, that Congress could not have intended the SCA to be used to obtain constitutionally protected information absent a showing of probable cause.

D. Good Faith Exception

***9** The government urges that even if the Court finds that probable cause is required to obtain cell site data, the evidence in this case should not be supressed, because of operation of the good faith exception to the exclusionary rule.

In *United States v. Leon,* 468 U.S. 897 (1984), the Supreme Court "held that the exclusionary rule does not apply when the police conduct a search in 'objectively reasonable reliance' on a warrant later held invalid." *Davis v. United States,* 131 S.Ct. 2419, 2428 (2011). "If the purpose of the exclusionary rule is to deter unlawful police conduct, then evidence obtained from a search should be suppressed only if it can be said that the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional under the Fourth Amendment." *Leon,* 468 U.S. at 919 (citing *United States v. Peltier,* 422 U.S. 531, 542 (1975)). "For exclusion to be appropriate, the deterrence benefits of suppression must outweigh the rule's heavy costs." *Davis,* 131 S.Ct. at 2422 (2011). In general, evidence will not be suppressed when the magistrate, not the officer, errs. *United States v. Mendosa,* 989 F.2d 366, 369 (9th Cir.1993). Evidence should be suppressed only if: (1) the magistrate has abandoned his detached and neutral role, (2) the officers were dishonest or reckless in preparing their affidavit, or (3) the officers could not have "harbored an objectively reasonable belief that probable cause existed." *Leon,* 468 U.S. at 926.

When presented with the same issue, the Eleventh Circuit found that

> The only differences between *Leon* and the present case are semantic ones. The officers here acted in good faith reliance on an order rather than a warrant, but, as in *Leon,* there was a 'judicial mandate' to the officers to conduct such search and seizure as was contemplated by the court order. As in *Leon,* the officers 'had a sworn duty to carry out' the provisions of the order. Therefore, even if there was a defect in the issuance of the mandate, there is no foundation for the application of the exclusionary rule.

Davis, 754 F.3d at 1218 (internal citations omitted).

The Court concurs with this reasoning. While the magistrate court's order required resolving an unsettled question of law—namely, whether the SCA allows the government to obtain cell site data absent a showing of probable cause—there is nothing in the record to suggest that it "abandoned its detached and neutral role" in arriving at its ultimate conclusion. Contrary to Cooper's suggestions, 1/16/15 Def. Sealed Brf. at 21–22, the Court can find nothing to show that the government was dishonest or misleading in its applications for cell site data. Nor can the Court conclude, given the lack of binding precedent to the contrary, that "a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization." *United States v. Luong*, 470 F.3d 898, 902 (9th Cir.2006) (citing *Leon*, 468 U.S. at 922); *see also*Leon, 468 U.S. at 898 ("Once the warrant issues, there is literally nothing more the policeman can do in seeking to comply with the law, and penalizing the officer for the magistrate's error, rather than his own, cannot logically contribute to the deterrence of Fourth Amendment violations."). The Court therefore finds that the good faith exception applies, and accordingly, **DENIES** Cooper's motion to suppress pen register and trap and trace data on this basis alone.

II. Motion to Suppress Evidence Obtained Through Wiretap Devices

***10** Cooper argues that the evidence obtained through wiretap devices must be suppressed. First, Cooper points out that government affidavits appear to show that the government commenced electronically surveying him before it obtained the proper judicial authorization. Docket No. 72, Def. Wiretap Mot. at 1–2. Cooper asserts that the information obtained through this unauthorized surveillance contributed to the probable cause showing the government had to make to obtain permission to use wiretaps, and that therefore the wiretap evidence must be suppressed. Second, Cooper highlights that Special Agent May claims in an affidavit that Knight texted Cooper at 2:14pm on February 5, 2013 in order to establish probable cause to obtain a wiretap, yet the records the government has turned over in discovery do not show any text communication between Knight and Cooper during the relevant time period. Finally, Cooper expresses general concerns that the government may be using "Stingray technology and/or the Hemisphere program" in order to conduct unauthorized surveillance. Docket No. 72, Def. Wiretap Mot. at 3; *see also* Docket No. 74, Balogh Decl. In the Court's prior order, it directed the government to produce certain documents, and respond in greater detail to Cooper's allegations. Docket No. 87. In response to the Court's order, government's counsel asserts in a sworn declaration that the government did not employ "stingray," "hemisphere," or any other means of surveillance without court order. Tolkoff Decl ¶ 3. He also explains that that the discrepancy regarding the missing text message was due to Agent May's misclassification of a two-second call as a text message. Tolkoff Decl ¶ 4. In his brief, Cooper attacks the government's explanation as insufficient, primarily because no one with personal knowledge swore to this explanation. 1/16/15 Sealed Def. Brf. at 2. In a reply brief, the government denies surveying Cooper without explicit judicial authorization. 1/30/15 Sealed Gov't Brf. at 3. The government also attached a sworn declaration of Special Agent May, who was the affiant for the wiretap application at issue. Sealed May Decl. ¶ 2. Agent May explains that he erroneously assumed, because of its brevity, that a two second phone contact was a text message, when in fact it was a call, *Id.* at ¶ 4. This would explain the missing text message at 2:14pm on February 5, 2013 of which Mr. Cooper complains. Agent May also declares that neither he, nor anyone else on the investigative team, used unauthorized surveillance techniques. *Id.* at ¶ 6.

The Court is satisfied that the government did not engage in any unauthorized surveillance of Cooper, or thereby rely on tainted evidence in order to establish the probable cause necessary to wiretap Cooper. Accordingly, the Court **DENIES** defendant's motion to suppress evidence obtained through wiretaps.

CONCLUSION

For the foregoing reasons, the Court **DENIES** Cooper's motions to suppress. This order resolves Docket Nos. 72 and 73.

IT IS SO ORDERED.

All Citations

Not Reported in F.Supp.3d, 2015 WL 881578

Footnotes

1 This would be the first of two rounds of additional briefing ordered by the Court. *See* Docket Nos. 65, 87.

2 By providing the location of the nearest cell tower used by the target phone, cell site data is essentially a clumsy version of GPS tracking. This result therefore squares with the statutory framework of the ECPA, which requires a showing of probable cause under Rule 41 for the installation of a tracking device. *See*18 U.S.C.A. §§ 3104, 3117.

3 Under 18 U.S.C. § 2703(c)(A), the government may obtain this information by obtaining a warrant under the "probable cause" standard, although it appears that the government relied only on the lower "reasonable grounds" standard under subsection (d).

4 Oral argument before the Court *en banc* was scheduled to occur on February 24, 2015 in Atlanta, Georgia. http://www.ca11.uscourts.gov/enbanc-cases

5 While the Third and Fifth Circuits have addressed the issue, neither was in the context of a suppression motion in a criminal proceeding, and the Third Circuit's decision issued before the Supreme Court decided *Jones*. The Fifth Circuit held that magistrate judges have no discretion to require a showing of probable cause to obtain historical cell site data, and that the "specific and articulable facts" standard was not *per se* unconstitutional. The Third Circuit held that a magistrate judge did indeed have the discretion to require a showing of probable cause. *See*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); *In re Application of U.S. for Historical Cell Site Data,* 724 F.3d 600 (5th Cir.2013).

6 At oral argument on February 6, 2015, the government stated that cell site data is recorded for both calls and text messages.

End of Document

© 2015 Thomson Reuters. No claim to original U.S. Government Works.

Filed
APR 09 2015
RICHARD W. WIEKING
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE

United States District Court
For the Northern District of California

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

HRL

IN RE: APPLICATION FOR TELEPHONE INFORMATION NEEDED FOR A CRIMINAL INVESTIGATION

No. CR 15 90304 MISC

ORDER

_____/

The government has submitted, under seal, an Application for an order pursuant to 18 U.S.C. §§ 3122 and 3123 (hereafter, the "Pen Statute") authorizing the installation of a pen register and trap and trace device on several cell phone numbers. In broad terms, a pen register records the dialed number of outgoing calls (or texts) along with the date, time, and length of each call. A trap and trace device captures the same information on incoming calls (or texts). The order, if signed by the court, would be served on the service provider(s) for the target cell phone numbers and would be effective for 60 days going forward. The Pen Statute requires the court to issue the order so long as the attorney for the government certifies that the information sought is relevant to an ongoing criminal investigation. The certification was made here.

For a number of years the government has also included in Pen Statute applications directed to cell phone numbers a request for cell site data. The court understands that every cell phone is, in effect, a radio transmitter. In order for the cell phone to place and receive calls, it has to communicate by radio with an antenna (cell site tower) controlled by that phone's service provider. The communication goes to the antenna that is closest to the location of the cell phone. The service provider records the telephone numbers and the date, time, and length of call. In addition, it records

DOCUMENT NO.
DISTRICT COURT
CRIMINAL CASE

the identity of the cell site tower handling the call as well as noting which sector of the tower was involved.[1]

That latter information is commonly called cell site information, and with it someone could get a decent idea where the subject cell phone was at the time of the call (in a particular sector in that tower's coverage area). Out in open country, where towers are few, a single tower may cover a very large area. Not so in a crowded urban locale, where towers are numerous. The application at hand seeks cell site information for 60 days back from the date of the court's order (historical data), as well as for 60 days going forward (prospective, or "real time" data).

In 1994, Congress passed the Communication Assistance of Law Enforcement Act (CALEA), which amended in part the Pen Statute. As with the Pen Statute (part of the Electronic Communication Privacy Act (ECPA)), Congress in CALEA was trying to balance a citizen's privacy interest with the legitimate investigatory pursuits of the government. In 47 U.S.C. § 1002(a)(2)(B), CALEA describes the obligations of telecommunications carriers in responding to the government's requests for information about subscribers, with a significant proviso: ". . . with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices . . . , such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number) . . . ."

Despite the prohibition just quoted from CALEA, the government has routinely been asking for cell site data in Pen Statute applications, and this court, as well as most if not all Magistrate Judges in this District, have been granting those applications. This has occurred because the government has argued that, by *including* in the Pen Statute application a request for cell site information pursuant to the Stored Communications Act (SCA) (Title II of the ECPA, 18 U.S.C. § 2701 *et seq.*), it trumps CALEA's prohibition on NOT getting cell site information solely through a pen register and trap and trace device. That is, it skirts the prohibition against physical location

[1] As the court understands it, the tower receives and sends within range calls anywhere in a 360 degree radius. In addition to capturing tower location, the service provider divides the tower's 360 degree radius into three sectors of 120 degrees each and records the sector from which the call came in or went out.

United States District Court
For the Northern District of California

information "solely" through the Pen Statute by seeking it simultaneously under the SCA. The SCA offers the government an option on how to get stored electronic information: a search warrant issued under the Federal Rules (§ 2703(a)(c)(A)), or a court order obtained on a representation of facts showing there are reasonable grounds to believe the information is relevant and material to an ongoing criminal investigation (§ 2703(a)(C)(b) and (d)). The government chooses the "court order" option.

The government's grafting of the SCA to the Pen Statute has come to be known as the "hybrid theory" for getting prospective cell site information without showing probable cause. While this court and courts elsewhere have been granting applications based on the hybrid theory, many others have rejected it.[2] There is no clear Supreme Court or Ninth Circuit authority.

On March 3, 2015, one of this court's colleagues, Senior District Judge Susan Illston, issued an order on Motions to Suppress in *United States v. Cooper*, 13-cr-00693, Dkt. No. 117. Judge Illston carefully examined the question of whether the hybrid theory supports allowing the government to gather prospective cell site information without a showing of probable cause. She likewise considered if the SCA, without a showing of probable cause, suffices for obtaining historical cell site records (for the 60 days immediately prior to the signing of an order for disclosure). Judge Illston's order triggered a desire by this court to revisit its practice of accepting the hybrid theory. The present Application is a proper vehicle for that reexamination.

With respect to prospective or real time cell site information, there is no question that it cannot be obtained relying only on the Pen Statute. CALEA makes it clear that a customer's physical location data is off-limits. That is, Congress chose to accord that particular information a higher level of protection than any of the other information being gathered by a pen register and trap and trace device (number called or received, date, time, length of call, etc.). Add the SCA to the mix and what happens? Well, the SCA applies to *stored* electronic information. That presents a logical problem because the government is asking for information that does not yet exist. It will be created during the 60 days after the order issues. The government, in effect, urges that, although the

[2] See a listing of cases, pro and con, compiled in *In re Application of United States for an Order*, 733 F. Supp. 2d 939 (N.D. Ill. 2009).

United States District Court
For the Northern District of California

information does not yet exist, it *will* soon exist, and then it will be recorded by the service provider and become part of its records. So, once it is *stored*, it can be disclosed to the government. The court does not know what is the lag time, if any (a minute, a second?), between when the information is recorded and when the service provider discloses it to the government. Section 1002(a) of 42 U.S.C. (CALEA) enjoins the telecommunications carrier to "expeditiously" make call-identifying information available to the government ". . . before, during, or immediately after the transmission . . . ." Basically, the government would be getting the information in near "real time". In summary, the Pen Statute prohibits obtaining location information and the SCA says nothing about obtaining prospective information or information that is not stored at the time the order issues. But, put both statutes together and you get prospective location information (without probable cause)? That argument is quite a stretch.

With respect to historical cell site information, that collected for the 60 days immediately prior to the court granting an application, the government relies on the SCA. As the government sees it, this previously gathered cell site data is just a plain, garden-variety business record of the electronic communication service provider. As noted above, the SCA offers the government two paths to getting information: (1) a search warrant on probable cause, or (2) a court order on a showing that the information is relevant and material to an ongoing investigation. The government takes the position it does not need a search warrant and can get what it wants by simply certifying relevance and materiality. It is not entirely clear why Congress created two different paths. This court suggests that the two paths are a recognition that some information should be accorded a higher level of protection from disclosure than other information. That is, some information, surely if it were constitutionally protected, requires probable cause. And, cell site location information implicates a person's constitutional right to privacy. The 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. Judge Illston discussed the ongoing evolution of the law in this area, as did the government in the brief it submitted to this court in support of its Application. For this court's purposes, it is sufficient that an authorization to install a tracking device requires a probable cause showing as does an application for formal cell phone

United States District Court
For the Northern District of California

tracking. The government argues that historical cell site information is not the same as tracking a person's (or vehicle's) actual location. Maybe, in a given case, the cell site information would only reveal the "general" location of the device (and thus the user), but that distinction seems more a difference in degree than in kind.

This court finds Judge Illston's analysis very persuasive, and concludes, until binding authority says otherwise, 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. As written, the Application is denied.

IT IS SO ORDERED.

Dated: April 9, 2015

HOWARD R. LLOYD
UNITED STATES MAGISTRATE JUDGE

United States District Court
For the Northern District of California

H

United States Court of Appeals,
Eleventh Circuit.
UNITED STATES of America, Plaintiff–Appellee,
v.
Quartavious DAVIS, Defendant–Appellant.

No. 12– 12928.
May 5, 2015.

Background: Defendant was convicted in the United States District Court for the Southern District of Florida of Hobbs Act robbery, conspiracy to violate the Hobbs Act, and knowing possession of a firearm in furtherance of a crime of violence. The Court of Appeals, Sentelle, Circuit Judge, 754 F.3d 1205, affirmed in part and vacated in part. Rehearing en banc was granted.

Holdings: The Court of Appeals, en banc, Hull, Circuit Judge, held that:
(1) government obtaining court order under Stored Communications Act (SCA) for production of cell phone carrier's business records was not a search, and
(2) even if it was a search, obtaining records without a warrant was reasonable.

Affirmed.

William Pryor, Circuit Judge, filed a concurring opinion.

Jordan, Circuit Judge, filed an opinion concurring in part and concurring in the judgment, in which Wilson, Circuit Judge, joined.

Rosenbaum, Circuit Judge, filed a concurring opinion.

Martin, Circuit Judge, filed a dissenting opinion in which Jill Pryor, Circuit Judge, joined.

West Headnotes

[1] Searches and Seizures 349 ⚷13.1

349 Searches and Seizures
349I In General
349k13 What Constitutes Search or Seizure
349k13.1 k. In general. Most Cited Cases

A party may establish a Fourth Amendment search by showing that the government engaged in conduct that would have constituted a search within the original meaning of the Fourth Amendment. U.S.C.A. Const.Amend. 4.

[2] Searches and Seizures 349 ⚷13.1

349 Searches and Seizures
349I In General
349k13 What Constitutes Search or Seizure
349k13.1 k. In general. Most Cited Cases

To determine whether a search occurred under the reasonable-expectation-of-privacy test requires a two-part inquiry: (1) has an individual manifested a subjective expectation of privacy in the object of the challenged search; and (2) is society willing to recognize that expectation as reasonable. U.S.C.A. Const.Amend. 4.

[3] Searches and Seizures 349 ⚷26

349 Searches and Seizures
349I In General
349k25 Persons, Places and Things Protected
349k26 k. Expectation of privacy. Most Cited Cases

A party alleging an unconstitutional search under the Fourth Amendment must establish both a subjective and an objective expectation of privacy to succeed. U.S.C.A. Const.Amend. 4.

[4] Searches and Seizures 349 ⚷21

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

349 Searches and Seizures
349I In General
349k13 What Constitutes Search or Seizure
349k21 k. Use of electronic devices; tracking devices or "beepers.". Most Cited Cases

Government obtaining court order under Stored Communications Act (SCA) for production of cell phone carrier's business records containing historical cell tower location information as to defendant was not a search under the Fourth Amendment; records were created by carrier and stored on its own premises, defendant exercised no control over the records, defendant knew that his cell phone transmitted information to cell towers and registered his phone under fictitious alias, and no law required collection of information in records. U.S.C.A. Const.Amend. 4; 18 U.S.C.A. § 2703(d).

[5] Searches and Seizures 349 ⚷23

349 Searches and Seizures
349I In General
349k23 k. Fourth Amendment and reasonableness in general. Most Cited Cases

The Fourth Amendment prohibits unreasonable searches, not warrantless searches; the ultimate measure of the constitutionality of a governmental search is reasonableness. U.S.C.A. Const.Amend. 4.

[6] Searches and Seizures 349 ⚷24

349 Searches and Seizures
349I In General
349k24 k. Necessity of and preference for warrant, and exceptions in general. Most Cited Cases

Searches and Seizures 349 ⚷40.1

349 Searches and Seizures
349I In General
349k40 Probable Cause
349k40.1 k. In general. Most Cited Cases

A warrant is not required to establish the reasonableness of all government searches, and when a warrant is not required, probable cause is not invariably required either. U.S.C.A. Const.Amend. 4.

[7] Searches and Seizures 349 ⚷23

349 Searches and Seizures
349I In General
349k23 k. Fourth Amendment and reasonableness in general. Most Cited Cases

The reasonableness of a search or seizure is evaluated under traditional standards of reasonableness by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests. U.S.C.A. Const.Amend. 4.

[8] Searches and Seizures 349 ⚷36.1

349 Searches and Seizures
349I In General
349k36 Circumstances Affecting Validity of Warrantless Search, in General
349k36.1 k. In general. Most Cited Cases

There is a strong presumption of constitutionality in a search performed pursuant to an Act of Congress, especially when it turns on what is reasonable within the meaning of the Fourth Amendment. U.S.C.A. Const.Amend. 4.

[9] Telecommunications 372 ⚷1475

372 Telecommunications
372X Interception or Disclosure of Electronic Communications; Electronic Surveillance
372X(B) Authorization by Courts or Public Officers
372k1475 k. Carrier's cooperation; pen registers and tracing. Most Cited Cases

Even if government obtaining court order under Stored Communications Act (SCA) for production of cell phone carrier's business records contain-

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

ing historical cell tower location information as to defendant was a search, obtaining the records without a warrant was reasonable; defendant had no reasonable expectation of privacy in records made, kept, and owned by carrier, records were not recordings of conversations, records were not real-time tracking of precise movements, SCA guarded against improper acquisition or use of personal information theoretically discoverable through such records, including requiring neutral magistrate to find records were relevant and material to an ongoing criminal investigation, records served compelling government interest in assisting investigation of various crimes, and society had compelling interest promptly apprehending criminals and vindicating rights of innocent suspects. U.S.C.A. Const.Amend. 4; 18 U.S.C.A. § 2703(d).

***499** Amit Agarwal, Roy K. Altman, Kevin Quencer, Wifredo A. Ferrer, Amanda Perwin, Kathleen Mary Salyer, Anne Ruth Schultz, U.S. Attorney's Office, Miami, FL, for Plaintiff–Appellee.

Anne Margaret Hayes, Law Office of Anne M. Hayes, Cary, NC, Jacqueline Shapiro, Jacqueline E. Shapiro, Esq., David Oscar Markus, Markus & Markus, ***500** PLLC, Miami, FL, for Defendant–Appellant.

Appeal from the United States District Court for the Southern District of Florida. D.C. Docket No. 1:10–cr–20896–JAL–2.

Before ED CARNES, Chief Judge, TJOFLAT, HULL, MARCUS, WILSON, WILLIAM PRYOR, MARTIN, JORDAN, ROSENBAUM, JULIE CARNES, and JILL PRYOR, Circuit Judges.

HULL, Circuit Judge:

I. BACKGROUND

Appellant Quartavius Davis [FN1] was convicted by a jury on several counts of Hobbs Act robbery, 18 U.S.C. § 1951(b)(1), (3), conspiracy, *id.* § 1951(a), and knowing possession of a firearm in furtherance of a crime of violence, *id.* §§ 924(c)(1)(A)(ii), 2. The district court entered judgment on the verdict, sentencing Davis to consecutive terms of imprisonment totaling 1,941 months. In this appeal, we are called on to decide whether the court order authorized by the Stored Communications Act, *id.* § 2703(d), compelling the production of a third-party telephone company's business records containing historical cell tower location information, violated Davis's Fourth Amendment rights and was thus unconstitutional. We hold it did not and was not.

FN1. The Presentence Investigation Report notes that "Quartavius" is the correct spelling of appellant's first name, despite the spelling in the caption.

Therefore, the district court did not err in denying Davis's motion to suppress and we affirm Davis's convictions. We reinstate the panel opinion, *United States v. Davis,* 754 F.3d 1205 (11th Cir.), *reh'g en banc granted, opinion vacated,* 573 Fed.Appx. 925 (11th Cir.2014), with respect to all issues except those addressed in Parts I and II, 754 F.3d at 1210–18, which are now decided by the en banc court.[FN2]

FN2. Davis's advisory guidelines range was 57 to 71 months' imprisonment for his Hobbs Act robberies. However, each of his seven § 924(c) convictions required consecutive sentences. 18 U.S.C. § 924(c)(1)(D)(ii). The district court sentenced Davis to concurrent terms of 57 months' imprisonment on counts 1, 2, 4, 6, 8, 10, 13, 15, and 16, plus a consecutive term of 84 months on count 3, plus consecutive terms of 300 months' imprisonment on counts 5, 7, 9, 11, 14, and 17.

The panel opinion affirmed Davis's convictions but vacated the application of the guidelines sentencing increase for "brandishing" of a firearm. *Davis,* 754 F.3d at 1220–21, 1223. To be clear, that disposition stands.

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

A. Seven Armed Robberies in a Two–Month Period

Quartavius Davis committed seven separate armed robberies in a two-month period. From the beginning of August 2010 to the beginning of October 2010, Davis and accomplices, bearing an array of firearms, terrorized a wide range of South Florida businesses, including a pizzeria, a gas station, a drugstore, an auto parts store, a beauty salon, a fast food restaurant, and a jewelry store.

On February 18, 2011, a federal grand jury returned a seventeen-count indictment against Davis and five codefendants. Davis was named in sixteen of the seventeen counts. The indictment charged violations of the Anti–Racketeering Act, 18 U.S.C. § 1951 (Hobbs Act), and conspiracy to violate the Hobbs Act. The indictment specifically charged Davis with conspiracy to engage in Hobbs Act robbery, in violation of 18 U.S.C. § 1951(a) (Counts 1, 15); seven Hobbs Act armed robberies, in violation of 18 U.S.C. §§ 1951(a), 2 (Counts 2, 4, 6, 8, 10, 13, 16); and knowingly using, carrying, and possessing a firearm in furtherance***501** of a crime of violence, in violation of 18 U.S.C. §§ 924(c)(1)(A)(ii), 2 (Counts 3, 5, 7, 9, 11, 14, 17).

All of Davis's codefendants pled guilty to various counts. Davis alone went to trial. The jury convicted Davis on all charged counts.

At trial, the prosecution offered evidence of two conspiracies to commit Hobbs Act robbery and evidence that Davis took part in each conspiracy and each robbery. The prosecution further presented evidence that the conspirators committed such robberies. One member of each conspiracy testified for the government. Codefendant Willie Smith ("Smith") testified as to the first conspiracy, encompassing six robberies at commercial establishments, including a Little Caesar's restaurant, an Amerika Gas Station, a Walgreens drug store, an Advance Auto Parts store, a Universal Beauty Salon, and a Wendy's restaurant. Codefendant Michael Martin ("Martin") testified as to the second conspiracy, encompassing the robbery of a Mayors Jewelry store. Smith and Martin testified that Davis was involved in each robbery, where they wore masks, carried guns, and stole items such as cash, cigarettes, and watches.

Separately, an eyewitness, Edwin Negron, testified regarding Davis's conduct at the Universal Beauty Salon and the adjacent martial arts studio. He testified that Davis pointed a gun at his head, pushed both a 77–year–old woman and Negron's wife to the ground, and took several items from Negron and others. Another eyewitness, Antonio Brooks, testified that Brooks confronted Davis and his accomplices outside the Wendy's after that robbery. Brooks testified that Davis fired a gun at Brooks, and that Brooks returned fire towards the getaway car.

Beyond the accomplice and eyewitness testimony, the government produced additional evidence. Surveillance videos showed a man matching Davis's description participating in the robberies at Walgreens, Advance Auto Parts, Wendy's, and Mayors Jewelry. Smith and Martin identified Davis on the videos. DNA shown to be Davis's was recovered from the getaway car used to flee the scene of the Universal Beauty Salon robbery and the Mayors Jewelry store robbery.

In addition, the prosecution introduced telephone records obtained from MetroPCS for the 67–day period from August 1, 2010, through October 6, 2010, the time period spanning the first and last of the seven armed robberies. [FN3] The toll records show the telephone numbers for each of Davis's calls and the number of the cell tower that connected each call. A MetroPCS witness identified his company's cell tower glossary, which lists the physical addresses, including longitude and latitude, of MetroPCS's cell towers. A police witness then located on a map the precise addresses (1) of the robberies and (2) of the cell towers connecting Davis's calls around the time of six of the seven robberies. While there was some distance between them, the cell tower sites were in the general vicinity of the robbery sites.

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

FN3. The first robbery took place on August 7, 2010, and the final robbery took place on October 1, 2010.

The location of the cell user, though, is not precise. The testimony tells us (1) the cell tower used will typically be the cell tower closest to the user, (2) the cell tower has a circular coverage radius of varying sizes, and (3) although the tower sector number indicates a general direction (North, South, etc.) of the user from the tower, the user can be anywhere in that ***502** sector. Despite this lack of precision as to where Davis's cell phone was located, the cell tower evidence did give the government a basis for arguing calls to and from Davis's cell phone were connected through cell tower locations that were near the robbery locations, and thus Davis necessarily was near the robberies too.

This appeal concerns the introduction of MetroPCS's toll records and glossary as evidence against Davis at trial. We thus review in more detail how the government acquired MetroPCS's records, the types of data in the records, and the witnesses' testimony about the records.

B. Court Order Regarding MetroPCS Business Records

After Davis's arrest, the government acquired MetroPCS's business records by court order. In February 2011, the government applied to a federal magistrate judge for a court order directing various phone companies to disclose stored telephone communications records for four subject telephone numbers that included a number ending in 5642 (the "5642 number"). The application requested production of stored "telephone subscriber records" and "phone toll records," including the "corresponding geographic location data (cell site)," for the 5642 number. The government requested only records "for the period from August 1, 2010 through October 6, 2010." The government sought clearly-delineated records that were both historical and tailored to the crimes under investigation.

The government did so following the explicit design of the governing statute, the Stored Communications Act ("SCA"), 18 U.S.C. § 2701 *et seq.* Section 2703 of the SCA provides that a federal or state governmental entity may require a telephone service provider to disclose "a record ... pertaining to a subscriber to or a customer of such service (not including the contents of communications)" if "a court of competent jurisdiction" finds "specific and articulable facts showing that there are reasonable grounds to believe" that the records sought "are relevant and material to an ongoing criminal investigation." *Id.* § 2703(c)(1)(A), (B), (d). The court order under subsection (d) does not require the government to show probable cause.

No one disputes that the government's § 2703 application to the magistrate judge contained "specific and articulable facts" showing "reasonable grounds" to believe MetroPCS's business records—pertaining to Davis's 5642 cell phone number—were "relevant and material" to the government's investigation. The government's § 2703 application provided a detailed summary of the evidence implicating Davis in the seven robberies, including post-*Miranda* statements from two accomplices and the DNA evidence found in two getaway cars. Undisputedly, a sufficient showing was made to satisfy the SCA's statutory requirements.

The magistrate judge's order granted the § 2703 application. The court order required MetroPCS, the third-party cellular telephone service provider, to produce "all telephone toll records and geographic location data (cell site)" for the 5642 number during the period August 1, 2010 through October 6, 2010.

MetroPCS complied. For this two-month time period, MetroPCS produced its stored telephone records for number 5642 showing these five types of data: (1) telephone numbers of calls made by and to Davis's cell phone; (2) whether the call was outgoing or incoming; (3) the date, time, and duration of the call; (4) the number assigned to the cell tower that wirelessly connected the calls from and to Dav-

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

is; and (5) the sector number associated with that tower. For ease of reference, ***503** the fourth and fifth items are collectively called "historical cell tower location information."

Importantly though, MetroPCS's business records did not show (1) the contents of any call; (2) the contents of any cell phone; (3) any data at all for text messages sent or received; or (4) any cell tower location information for when the cell phone was turned on but not being used to make or receive a call. The government did not seek, nor did it obtain, any GPS or real-time (also known as "prospective") location information.

Before trial, Davis moved to suppress MetroPCS's business records for number 5642. Although the government obtained them through a statutorily-prescribed judicial order, Davis argued the evidence should be suppressed because the § 2703(d) production of MetroPCS's records constituted a search under the Fourth Amendment and thus required probable cause and a search warrant. The district court denied the motion.[FN4]

FN4. Davis did not present any evidence in support of his Fourth Amendment claim, either at the suppression hearing or at trial.

C. Evidence at Trial

During the jury trial, the government introduced the MetroPCS records for the 5642 number, which was registered to "Lil Wayne." [FN5] The government also introduced evidence tying Davis to the 5642 phone number. One of Davis's codefendants testified that Davis used the 5642 number from August 2010 to October 2010. And a codefendant's cell phone, which was entered into evidence, listed the 5642 number under Davis's nickname, "Quat," in the phone's contact list.[FN6]

FN5. MetroPCS had not required the subscriber Davis to give his true name. Instead, MetroPCS sells phones with monthly plans—averaging $40 a month—paid up front. When that plan expires, the subscriber pays another monthly payment up front or the plan is cancelled.

FN6. The government also obtained MetroPCS records for three other cell phone numbers used by Davis's co-conspirators, which were registered under the alias names of "Nicole Baker," "Shawn Jay," and "Dope Boi Dime." The issue before us involves only Davis's cell phone number, the 5642 number registered to "Lil Wayne." In this en banc appeal, Davis did not raise arguments about the other cell phone numbers.

Michael Bosillo, a custodian of records from MetroPCS, identified and testified about the business records regarding number 5642. He testified that MetroPCS's toll records, described above, are created and maintained in the regular course of its business.

As to cell tower location, Bosillo explained that, when a cellular phone user makes a call, the user's cell phone sends a signal to a nearby cell tower, which is typically but not always the closest tower to the phone. Two people driving together in the same car might be using different cell towers at the same time. Each cell phone tower has a circular coverage radius, and the "coverage pie" for each tower is further divided into either three or six parts, called sectors.

Bosillo testified that a cell tower would generally have a coverage radius of about one to one-and-a-half miles and that an individual cell phone user could "be anywhere" in the specified sector of a given cell tower's range. Bosillo also testified that the density of cell towers in an urban area like Miami would make the coverage of any given tower smaller, but he never said how much smaller. [FN7]

FN7. Davis and various *amici* argue that some cellular telephone companies have now increased their network coverage by

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

augmenting their cell tower network with low-power small cells, or "femtocells," which can cover areas as small as ten meters. There is no evidence, or even any allegation, that the MetroPCS network reflected in the records in this case included anything other than traditional cell towers and the facts of this case do not require, or warrant, speculation as to the newer technology.

***504** Bosillo also testified that the toll records for Davis's cell number 5642 show only (1) the number of the cell tower used to route Davis's call, and (2) the sector number associated with that tower. Thus, to determine the location of any cell tower used, Bosillo identified and explained the cell tower glossary created and kept by MetroPCS. The MetroPCS glossary listed (1) each of its cell tower numbers, (2) the physical address, including latitude and longitude, of that cell tower, and (3) how many sectors are within each cell tower's range.

This MetroPCS glossary, along with its toll records, allowed the government to determine the precise physical location *of the cell towers* that connected calls made by and to Davis's cell phone around the time of the robberies, but not the precise location of that cell phone or of Davis.

Davis objected to the introduction of the toll records for the account corresponding to the 5642 number, the subscriber records, and MetroPCS's cell-tower glossary. The district court overruled those objections.

The government also introduced into evidence maps that showed the locations of six of the armed robberies in relation to certain cell towers. Detective Mitch Jacobs examined the records, analyzing the records only for the days the armed robberies occurred. Detective Jacobs had, at that time, been employed by the Miami-Dade Police Department for 27 years and for the last ten years had worked with cases involving cell tower location information. He had utilized cell tower location information for his investigations of homicides, parental kidnappings, robberies, fugitives, and various other types of crime.

Detective Jacobs created the maps introduced at trial based on MetroPCS's records. These maps showed that, at or near the time of the armed robberies, cell phones linked to Davis and his codefendants made and received numerous calls routed through cell towers located in the general vicinity of the robbery locations. Detective Jacobs testified, and the maps showed, that this was true for six of the seven armed robberies. On the maps, Jacobs placed: (1) the location of the robberies and (2) the location of the cell towers that routed calls from Davis and his codefendants' phones.[FN8]

FN8. The maps did not show any cell tower's coverage radius or display any cell tower's sectors.

The distance between the robbery and cell tower locations was never quantified. The distance between the cell user and the cell tower was never quantified, but the evidence—records and testimony—as a whole suggests Davis's calls occurred within an area that covers at least several city blocks. The government argued the cell tower evidence showed Davis was near the robberies when they occurred.

D. The Appeal

Following his convictions by the jury, Davis appealed. A panel of this Court affirmed his convictions, but held that the government violated Davis's rights under the Fourth Amendment by obtaining stored telephone communications records from MetroPCS, a third-party telephone service provider, pursuant to the order of the magistrate judge issued under the ***505** SCA, 18 U.S.C. § 2703(c)(1)(B), (d). *United States v. Davis,* 754 F.3d 1205, 1217 (11th Cir.2014). Nevertheless, the panel affirmed Davis's convictions based on the good-faith exception to the exclusionary rule. *Id.* at 1217–18. This Court vacated the panel's decision and granted the government's petition for rehearing en banc. *United*

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

States v. Davis, 573 Fed.Appx. 925 (11th Cir.2014).

II. STANDARD OF REVIEW

This Court reviews *de novo* constitutional challenges to a federal statute. *United States v. Campbell,* 743 F.3d 802, 805 (11th Cir.), *cert. denied,* ——U.S. ——, 135 S.Ct. 704, 190 L.Ed.2d 438 (2014). We review the district court's legal conclusions *de novo* and its findings of fact for clear error. *United States v. Jordan,* 635 F.3d 1181, 1185 (11th Cir.2011). In the context of an appeal from the denial of a suppression motion, all facts are construed in the light most favorable to the party prevailing below—here, the government. *United States v. Gibson,* 708 F.3d 1256, 1274 (11th Cir.2013).

III. DISCUSSION

On appeal, Davis argues the government violated his Fourth Amendment rights by obtaining historical cell tower location information from MetroPCS's business records without a search warrant and a showing of probable cause. Davis contends that the SCA, as applied here, is unconstitutional because the Act allows the government to obtain a court order compelling MetroPCS to disclose its historical cell tower location records without a showing of probable cause. Davis claims the Fourth Amendment precludes the government from obtaining a third-party company's business records showing historical cell tower location information, even for a single day, without a search warrant issued to that third party.

In the controversy before us, there is no GPS device, no physical trespass, and no real-time or prospective cell tower location information. This case narrowly involves only (1) government access to the existing and legitimate business records already created and maintained by a third-party telephone company and (2) historical information about which cell tower locations connected Davis's cell calls during the 67-day time frame spanning the seven armed robberies. We start by reviewing the SCA, which authorized the production of MetroPCS's business records.

A. The Statute

Under the SCA, Congress authorized the U.S. Attorney to obtain court orders requiring "a provider of electronic communication service ... to disclose a record or other information pertaining to a subscriber to ... such service (not including the contents of communications)." 18 U.S.C. § 2703(c). Section 2703 directs that a judge "shall issue" the order if the government "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.* " *Id.* § 2703(d) (emphasis added). While this statutory standard is less than the probable cause standard for a search warrant, the government is still required to obtain a court order and present to a judge specific and articulable facts showing reasonable grounds to believe the records are relevant and material to an ongoing criminal investigation. *See id.*

The SCA does not lower the bar from a warrant to a § 2703(d) order. Rather, requiring a court order under § 2703(d) raises the bar from an ordinary subpoena to one with additional privacy protections ***506** built in. The government routinely issues subpoenas to third parties to produce a wide variety of business records, such as credit card statements, bank statements, hotel bills, purchase orders, and billing invoices.[FN9] In enacting the SCA, Congress has required more before the government can obtain telephone records from a third-party business. The SCA goes above and beyond the constitutional requirements regarding compulsory subpoena process.

FN9. *See, e.g., United States v. Willis,* 759 F.2d 1486, 1498 (11th Cir.1985) (motel registration records); *United States v. Phibbs,* 999 F.2d 1053, 1077 (6th Cir.1993) (credit card statements). Those statements not only show location at the time of purchase, but also reveal intimate details of daily life, such as shopping habits, medical visits, and travel plans.

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

A number of the SCA's privacy-protection provisions warrant mention. First, the SCA affords citizens protection by "interpos[ing] a 'neutral and detached magistrate' between the citizen and the officer engaged in the often competitive enterprise of ferreting out crime." *See United States v. Karo,* 468 U.S. 705, 717, 104 S.Ct. 3296, 3304, 82 L.Ed.2d 530 (1984) (internal quotation marks omitted). Congress made review by a judicial officer a precondition for the issuance of a § 2703(d) order. Moreover, the telephone records are made available *only if* a judicial officer finds (or the government shows) a factual basis for why the records are material to an ongoing criminal investigation.

In addition, the SCA generally prohibits telephone companies from voluntarily disclosing such records to "a governmental entity." *Id.* § 2702(a)(3), (c)(4), (c)(6). As that prohibition underscores, a telephone company (like MetroPCS) would, absent privacy-protecting laws (like the SCA), be free to disclose its historical cell tower location records to governmental and nongovernmental entities alike—without any judicial supervision and without having to satisfy the statutory standard in § 2703(d).

Further, the SCA bars "[i]mproper disclosure" of records obtained under § 2703(d). *See id.* § 2707(g). The SCA also provides remedies and penalties for violations of the Act's privacy-protecting provisions, including money damages and the mandatory commencement of disciplinary proceedings against offending federal officers. *See id.* §§ 2707(a), (c), (d), 2712(a), (c).

Despite the SCA's protections, Davis claims the court's § 2703(d) order compelling the production of MetroPCS records violated his Fourth Amendment rights. To prevail on his Fourth Amendment claim, Davis must show both (1) that the application of the SCA to the facts of his case involved a "search" within the meaning of the Fourth Amendment, and (2) that such search was unreasonable. This Davis cannot do.

B. What Constitutes a "Search"

[1] The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. A party may establish a Fourth Amendment search by showing that the government engaged in conduct that "would have constituted a 'search' within the original meaning of the Fourth Amendment," *United States v. Jones,* 565 U.S. ——, ——, 132 S.Ct. 945, 950 n. 3, 181 L.Ed.2d 911 (2012). "Search" originally was tied to common-law trespass and involved some trespassory intrusion on property. *See, e.g., Kyllo v. United States,* 533 U.S. 27, 31–32, 121 S.Ct. 2038, 2042, 150 L.Ed.2d 94 (2001).

Davis makes no trespass claim, nor could he.

***507** In 1967, the Supreme Court *added* a separate test—the reasonable-expectation-of-privacy test—to analyze whether a search occurred for purposes of the Fourth Amendment. *See Smith v. Maryland,* 442 U.S. 735, 739–40, 99 S.Ct. 2577, 2579–80, 61 L.Ed.2d 220 (1979) (citing *Katz v. United States,* 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967)). The reach of the Fourth Amendment now does not turn on the presence or absence of a physical intrusion. *Katz,* 389 U.S. at 353, 88 S.Ct. at 512.

Thus, to determine whether the government's obtaining access to MetroPCS's records constitutes a search within the meaning of the Fourth Amendment, our lodestar is *Katz's* reasonable-expectation-of-privacy test. *Smith,* 442 U.S. at 739, 99 S.Ct. at 2579–80 (citing *Katz,* 389 U.S. 347, 88 S.Ct. 507).

[2][3] " *Katz* posits a two-part inquiry: first, has the individual manifested a subjective expectation of privacy in the object of the challenged search?" *California v. Ciraolo,* 476 U.S. 207, 211, 106 S.Ct. 1809, 1811, 90 L.Ed.2d 210 (1986). "Second, is society willing to recognize that expectation as reasonable?" *Id.* Thus, "a party alleging an unconstitu-

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

tional search under the Fourth Amendment must establish *both* a subjective *and* an objective expectation of privacy to succeed." *United States v. Robinson,* 62 F.3d 1325, 1328 (11th Cir.1995).

Notably, it was the interception and recording of *conversations* reasonably intended to be private that drove the new test and result in *Katz. See* 389 U.S. at 351–53, 88 S.Ct. at 511–12. The government recorded Katz's conversations by attaching an electronic listening and recording device to the outside of a public phone booth in which Katz made calls. *Id.* at 348, 88 S.Ct. at 509. The government had no warrant or court order of any sort. *See id.* at 354–56, 88 S.Ct. at 512–514. The Supreme Court held that the government's conduct in "electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth," and thus constituted a "search and seizure" under the Fourth Amendment. *Id.* at 353, 88 S.Ct. at 512. The critical fact was that one who enters a telephone booth, "shuts the door behind him, and pays the toll that permits him to place a call" is entitled to assume that *his conversation* is not being intercepted and recorded. *Id.* at 352, 88 S.Ct. at 511–12; *id.* at 361, 88 S.Ct. at 516–17 (Harlan, J., concurring).

C. Third Party's Business Records

In subsequently applying *Katz's* test, the Supreme Court held—in both *United States v. Miller* and *Smith v. Maryland* —that individuals have no reasonable expectation of privacy in certain business records owned and maintained by a third-party business.

In *United States v. Miller,* during an investigation into tax fraud, federal agents presented subpoenas to the presidents of two banks, seeking to obtain from those banks all of Miller's bank account records. 425 U.S. 435, 437–38, 96 S.Ct. 1619, 1621, 48 L.Ed.2d 71 (1976). The issue was whether the defendant Miller had a "legitimate expectation of privacy" in the documents' contents. *See id.* at 440–43, 96 S.Ct. at 1622–24. The Supreme Court held that Miller had no protectable Fourth Amendment interest in the account records because the documents were: (1) business records of transactions to which the banks were parties and (2) Miller voluntarily conveyed the information to the banks. *Id.* Miller had "neither ownership nor possession" over the papers and the records. *Id.* at 437, 440, 96 S.Ct. at 1621, 1623. Rather, the papers were "the business***508** records of the banks." *Id.* at 440–41, 96 S.Ct. at 1623. All of the bank records contained information "voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business." *Id.* at 442, 96 S.Ct. at 1624. The Supreme Court noted "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 and the confidence placed in the third party will not be betrayed." *Id.* at 443, 96 S.Ct. at 1624; *see also In re Grand Jury Proceeding,* 842 F.2d 1229, 1234 (11th Cir.1988) ("[A]n individual has no claim under the fourth amendment to resist the production of business records held by a third party.").

Then, in *Smith v. Maryland,* the Supreme Court held that telephone users have no reasonable expectations of privacy in dialed telephone numbers recorded through pen registers and contained in the third-party telephone company's records. 442 U.S. at 742–46, 99 S.Ct. at 2581–83. The Supreme Court determined that Smith had no subjective or objective expectation of privacy in the numbers he dialed on the telephone and thus the installation of the pen register, by the telephone company at the government's request, did not constitute a search under the Fourth Amendment. *Id.*

As to the subjective expectation of privacy, the Supreme Court in *Smith* doubted that "people in general entertain any actual expectation of privacy in the numbers they dial" because "[a]ll telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

telephone company switching equipment that their calls are completed." *Id.* at 742, 99 S.Ct. at 2581. The Supreme Court stated that "[t]elephone users, in sum, 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, 99 S.Ct. at 2581. "Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret." *Id.* The Supreme Court stressed that "a pen register differs significantly from the listening device employed in *Katz,* for pen registers do not acquire the *contents* of communications." *Id.* at 741, 99 S.Ct. at 2581.

More telling in *Smith* though for this case is the location information revealed through the telephone records. Smith argued that, "whatever the expectations of telephone users in general, he demonstrated an expectation of privacy by his own conduct here, since he us[ed] the telephone *in his house* to the exclusion of all others." *Id.* at 743, 99 S.Ct. at 2582 (internal quotation marks omitted). The Supreme Court expressly rejected Smith's argument that he demonstrated an expectation of privacy in his own conduct here *by using the telephone only in his house.* The Supreme Court found that "[a]lthough [Smith's] conduct may have been calculated to keep the *contents* of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed." *Id.* The Supreme Court reasoned: "[r]egardless of his location, [Smith] had to convey that number to the telephone company in precisely the same way if he wished to complete his call. The fact that he dialed the number on his home phone rather than on some other phone could make no conceivable difference, ***509** nor could any subscriber rationally think that it would." *Id.*

As to the objective expectation of privacy, the Supreme Court determined that, "even if [Smith] 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.* (quoting *Katz,* 389 U.S. at 361, 88 S.Ct. at 516) (internal quotation marks omitted). The Supreme Court "consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Id.* at 743–44, 99 S.Ct. at 2582. The Supreme Court found that, "[w]hen he used his phone, [Smith] voluntarily conveyed numerical information to the telephone company." *Id.* at 744, 99 S.Ct. at 2582. The Supreme Court explained: "[t]he switching equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber." *Id.*

In *Smith,* the Supreme Court decided that "a different constitutional result is [not] required because the telephone company has decided to automate." *Id.* at 744–45, 99 S.Ct. at 2582. "The fortuity of whether or not the phone company in fact elects to make a quasi-permanent record of a particular number dialed does not in our view, make any constitutional difference." *Id.* at 745, 99 S.Ct. at 2583. The Supreme Court concluded: "[Smith] in all probability entertained no actual expectation of privacy in the phone numbers he dialed, and ... even if he did, his expectation was not 'legitimate.' " *Id.*

D. Fifth Circuit Decision

Before turning to Davis's case, we review the Fifth Circuit's recent decision holding that a court order under § 2703(d) compelling production of business records—showing this same cell tower location information—does not violate the Fourth Amendment and no search warrant is required. *In re Application of the United States for Historical Cell Site Data ("In re Application (Fifth Circuit)"),* 724 F.3d 600, 611–15 (5th Cir.2013).[FN10] At the outset, the Fifth Circuit stressed who had collected the cell tower information. *See id.* at 609–10. The telephone company, not the government, collected

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

the cell tower location information in the first instance and for a variety of legitimate business purposes. *Id.* at 611–12. The Fifth Circuit emphasized:

> FN10. The dissent mistakenly argues that we are faced with "persuasive ... authority on both sides of the debate...." Dissenting Op. at 534 n. 2. To purportedly illustrate this, the dissent cites a Third Circuit decision, but that decision did not hold, as the dissent would, that a search warrant is required to obtain historical cell tower location data. *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't* ("In re Application (Third Circuit)"), 620 F.3d 304 (3d Cir.2010). Rather, after the lower courts denied the government's § 2703(d) application for historical cell tower data, the government appealed and the Third Circuit actually vacated that denial. *Id.* at 319. The Third Circuit concluded that the SCA itself gave the magistrate judge the discretionary option to require a warrant showing probable cause and that the discretionary warrant option should "be used sparingly because Congress also included the option of a § 2703(d) order." *Id.*
>
> The dissent also cites a Florida Supreme Court decision, but that case involved real-time data and did not involve a § 2703(d) order. *Tracey v. State,* 152 So.3d 504, 507–08 (Fla.2014).

The Government does not require service providers to record this information or store it. The providers control what they record and how long these records are retained.... In the case of such historical cell site information, the Government merely comes in after the fact ***510** and asks a provider to turn over records the provider has already created.
Id. at 612.

The Fifth Circuit reasoned these are the telephone company's "own records of transactions to which it is a party." *Id.* The telephone company created the record to memorialize its business transactions with the customer. *Id.* at 611–12. The Fifth Circuit was careful to define business records as records of transactions to which the record-keeper business is a party. *See id.* It also pointed out that these business records contained no content of communications, such as the content of phone calls, letters, or emails. *Id.*

After discussing the nature of the business records, the Fifth Circuit, relying on *Smith,* explained why the cell user had no subjective expectation of privacy in such business records showing cell tower locations. The court reasoned: (1) the cell user has knowledge that his cell phone must send a signal to a nearby cell tower in order to wirelessly connect his call; (2) the signal only happens when a user makes or receives a call; (3) the cell user has knowledge that when he places or receives calls, he is transmitting signals through his cell phone to the nearest cell tower and thus to his service provider; (4) the cell user thus is aware that he is conveying cell tower location information to the service provider and voluntarily does so when he uses his cell phone for calls. *Id.* at 613–14.

The Fifth Circuit concluded that "[c]ell phone users, therefore, understand that their service providers record their location information when they use their phones at least to the same extent that the landline users in *Smith* understood that the phone company recorded the numbers they dialed." *Id.* at 613.[FN11] Just as the petitioner in *Smith* knew that when he dialed telephones, he was conveying and exposing those numbers to electronic equipment, cell phone users have knowledge they are conveying signals and exposing their locations to the nearest cell tower. *Id.* at 612–14.

> FN11. In the Fifth Circuit case, the court stated that the "contractual terms of service and providers' privacy policies expressly state[d] that a provider uses a subscriber's

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

> location information to route his cell phone calls" and, moreover, "that the providers not only use the information, but collect it." *In re Application (Fifth Circuit),* 724 F.3d at 613. The government stresses that MetroPCS's privacy policy, accessible from the company website, plainly states that cell tower location data may be recorded, stored, and even shared with law enforcement. Although Davis would have signed a contract when beginning service with MetroPCS, that contract does not appear on this record to have been entered into evidence here. Thus we cannot consider it, or MetroPCS's privacy policy, in this particular case.

The Fifth Circuit agreed "that technological changes can alter societal expectations of privacy," but reasoned, "[a]t the same time, '[l]aw enforcement tactics must be allowed to advance with technological changes, in order to prevent criminals from circumventing the justice system.' " *Id.* at 614 (quoting *United States v. Skinner,* 690 F.3d 772, 778 (6th Cir.2012)). The Fifth Circuit concluded 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." *Id.* (quoting *Jones,* 565 U.S. at ——, 132 S.Ct. at 964 (Alito, J., concurring)). In the end, the Fifth Circuit determined: (1) "Congress has crafted such a legislative solution in the SCA," and (2) the SCA "conforms to existing Supreme Court Fourth Amendment precedent." *Id.* The Fifth Circuit "decline[d] to create a new rule to hold ***511** that Congress's balancing of privacy and safety is unconstitutional." *Id.* at 615.

E. Davis's Case

[4] Based on the SCA and governing Supreme Court precedent, we too conclude the government's obtaining a § 2703(d) court order for the production of MetroPCS's business records did not violate the Fourth Amendment.

For starters, like the bank customer in *Miller* and the phone customer in *Smith,* Davis can assert neither ownership nor possession of the third-party's business records he sought to suppress. Instead, those cell tower records were created by MetroPCS, stored on its own premises, and subject to its control. Cell tower location records do not contain private communications of the subscriber. This type of *non-content evidence,* lawfully created by a third-party telephone company for legitimate business purposes, does not belong to Davis, even if it concerns him. Like the security camera surveillance images introduced into evidence at his trial, MetroPCS's cell tower records were not Davis's to withhold. Those surveillance camera images show Davis's location at the precise location of the robbery, which is far more than MetroPCS's cell tower location records show.

More importantly, like the bank customer in *Miller* and the phone customer in *Smith,* Davis has no subjective or objective reasonable expectation of privacy in MetroPCS's business records showing the cell tower locations that wirelessly connected his calls at or near the time of six of the seven robberies.

As to the subjective expectation of privacy, we agree with the Fifth Circuit that cell users know that they must transmit signals to cell towers within range, that the cell tower functions as the equipment that connects the calls, 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, and that cell phone companies make records of cell-tower usage. *See In re Application (Fifth Circuit),* 724 F.3d at 613–14. Users are aware that cell phones do not work when they are outside the range of the provider company's cell tower network. *Id.* at 613. Indeed, the fact that Davis registered his cell phone under a fictitious alias tends to demonstrate his understanding that such cell tower location information is collected by MetroPCS and may be used to incriminate him.

Even if Davis had a subjective expectation of

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

privacy, his expectation of privacy, viewed objectively, is not justifiable or reasonable under the particular circumstances of this case. The unreasonableness in society's eyes dooms Davis's position under *Katz.* In *Smith,* the Supreme Court presumed that phone users knew of uncontroverted and publicly available facts about technologies and practices that the phone company used to connect calls, document charges, and assist in legitimate law-enforcement investigations. *See* 442 U.S. at 742–43, 99 S.Ct. at 2581. Cell towers and related records are used for all three of those purposes. We find no reason to conclude that cell phone users lack facts about the functions of cell towers or about telephone providers' recording cell tower usage.

Smith's methodology should not be set aside just because cell tower records may also be used to decipher the approximate location of the user at the time of the call. Indeed, the toll records for the stationary telephones at issue in *Smith* included location data far more precise than the historical cell site location records here, because the phone lines at issue in Smith corresponded to stationary landlines at known ***512** physical addresses. At the time of *Smith,* telephone records necessarily showed exactly where the user was—his home—at the time of the call, as the user's telephone number was tied to a precise address. And the number dialed was also tied to a precise address, revealing if the user called a friend, a business, a hotel, a doctor, or a gambling parlor.

In certain respects, Davis has an even less viable claim than the defendant in *Miller.* For example, the Supreme Court in *Miller* held that a customer did not have a reasonable expectation of privacy in records made and kept by his bank even where the bank was *required by law* to maintain those records. *See Miller,* 425 U.S. at 436, 440–41, 96 S.Ct. at 1621, 1623. Here, federal law did not require that MetroPCS either create or retain these business records.

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. *See* 442 U.S. at 744–45, 99 S.Ct. at 2582–83. 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, 99 S.Ct. at 2582. Further, 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.[FN12]

FN12. To avoid the third-party doctrine, the dissent claims that "[t]he extent of voluntariness of disclosure by a user is simply lower for cell site location data." Dissenting Op. at 535. Not so. Cell phone users voluntarily convey cell tower location information to telephone companies in the course of making and receiving calls on their cell phones. Just as in *Smith,* users could not complete their calls without necessarily exposing this information to the equipment of third-party service providers. The government, therefore, did not search Davis when it acquired historical cell tower location information from MetroPCS. In order to reach its result, the dissent effectively would cast aside longstanding and binding Supreme Court precedents in favor of its own view of the Fourth Amendment.

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

The use of cell phones is ubiquitous now and some citizens may want to stop telephone companies from compiling cell tower location data or from producing it to the government. Davis and *amici* advance thoughtful arguments for changing the underlying and prevailing law; but these proposals should be directed to Congress and the state legislatures rather than to the federal courts. As aptly stated by the Fifth Circuit, "the recourse for these desires is in the market or the political process; in demanding that service providers do away with such records (or anonymize them) or in lobbying elected representatives to enact statutory protections." *In re Application (Fifth Circuit),* 724 F.3d at 615; *See also In re Application (Third Circuit),* 620 F.3d at 319 ("The considerations for and against [§ 2703(d) orders not requiring a warrant] would be for Congress to balance. A court is not the appropriate forum for such balancing, and we decline to take a step as to which Congress is silent.").

***513** Following controlling Supreme Court precedent most relevant to this case, we hold that the government's obtaining a § 2703(d) court order for production of MetroPCS's business records at issue did not constitute a search and did not violate the Fourth Amendment rights of Davis.[FN13]

FN13. Rather than legal analysis, the dissent consists mainly of myriad hypothetical fact patterns and a tabloid-type parade of horribles. As the dissenting author well knows, our "decision can hold nothing beyond the facts of [this] case." *Edwards v. Prime, Inc.,* 602 F.3d 1276, 1298 (11th Cir.2010) (citing *Watts v. BellSouth Telecomms., Inc.,* 316 F.3d 1203, 1207 (11th Cir.2003) ("Whatever their opinions say, judicial decisions cannot make law beyond the facts of the cases in which those decisions are announced."); *United States v. Aguillard,* 217 F.3d 1319, 1321 (11th Cir.2000) ("The holdings of a prior decision can reach only as far as the facts and circumstances presented to the Court in the case which produced that decision." (quotation marks omitted))).

F. *United States v. Jones*

Instead of focusing on the SCA and *Smith,* Davis relies on *United States v. Jones,* 565 U.S. ——, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012), where the government surreptitiously attached a GPS device to a private vehicle and used its own device to track the vehicle's movements over a four-week period. *Id.* at ——, 132 S.Ct. at 948. In *Jones,* the Supreme Court held that the government's physical intrusion on the defendant's private property [FN14] was a "search" and violated the Fourth Amendment. *Id.* at ——, 132 S.Ct. at 949. Significantly, the government-initiated physical trespass in *Jones* led to constant and real-time GPS tracking of the precise location of the defendant's vehicle. *Id.* at ——, 132 S.Ct. at 948.[FN15] "The Government physically occupied private property for the purpose of obtaining information." *Id.* at ——, 132 S.Ct. at 949. The Supreme Court had "no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted." *Id.*

FN14. The Fourth Amendment provides in relevant part that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." U.S. Const. amend. IV. "It is beyond dispute that a vehicle is an 'effect' as that term is used in the Amendment." *Jones,* 565 U.S. at ——, 132 S.Ct. at 949.

FN15. The Supreme Court explained: "By means of signals from multiple satellites, the device established the vehicle's location within 50 to 100 feet, and communicated that location by cellular phone to a Government computer. It relayed more than 2,000 pages of data over the 4–week period." *Jones,* 565 U.S. at ——, 132 S.Ct. at 948.

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

The majority opinion in *Jones* acknowledged that "later cases, of course, have deviated from [an] exclusively property-based approach" and have adopted an alternative "reasonable expectation of privacy" standard. *Id.* at ——, 132 S.Ct. at 950 (citing *Katz,* 389 U.S. at 351, 360, 88 S.Ct. at 511, 516 (majority opinion and opinion of Harlan, J., concurring)). But the result in *Jones* required nothing other than the property-based approach. Though the government argued Jones had no "reasonable expectation of privacy," the Supreme Court majority determined it "need not address the Government's contentions, because Jones's Fourth Amendment rights d[id] not rise or fall with the *Katz* formulation." *Id.*

Explaining the distinction, the majority opinion stressed that "the *Katz* reasonable-expectation-of-privacy test has been *added to,* not *substituted for,* the common-law trespassory test." *Id.* at ——, 132 S.Ct. at 952. But the majority holding in *Jones* turned on the physical intrusion of the government placing a GPS device on a ***514** private vehicle. *Id.* at ——, 132 S.Ct. at 949.

That is not this case. The government's obtaining MetroPCS records, showing historical cell tower locations, did not involve a physical intrusion on private property or a search at all. The records belonged to a private company, not Davis. The records were obtained through a court order authorized by a federal statute, not by means of governmental trespass. MetroPCS, not the government, built and controlled the electronic mechanism (the cell towers) and collected its cell tower data for legitimate business purposes. *Jones* is wholly inapplicable to this case.

Davis and the dissent attempt to deploy the concurrences in *Jones* to argue that historical cell tower location data is the equivalent of GPS and constitutes the sort of precise, long-term monitoring requiring the government to show probable cause. This attempt misreads the concurrences. We review the concurrences in detail because they leave the third-party doctrine untouched and do not help Davis's case. If anything, the concurrences underscore why this Court remains bound by *Smith* and *Miller.*

Justice Sotomayor concurred in the majority opinion, but was concerned because the government's GPS monitoring had "generate[d] a precise, comprehensive record of a person's public movements" and gave the government "unrestrained power to assemble data." *Id.* at ——, 132 S.Ct. at 955–56. She found the "[r]esolution of [that] difficult question[ ]" was "unnecessary ... because the Government's *physical intrusion* on Jones' Jeep supplie[d] a narrower basis for decision." *Id.* at ——, 132 S.Ct. at 957 (emphasis added). In joining the majority's opinion, she provided the fifth vote for the physical trespass holding. *Id.*

Justice Sotomayor did state: "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." *Id.* (citing *Smith,* 442 U.S. at 742, 99 S.Ct. at 2581; *Miller,* 425 U.S. at 443, 96 S.Ct. at 1624). But she quickly added and countered her own suggestion, stating: "[p]erhaps, as Justice ALITO notes, some people may find the 'tradeoff' of privacy for convenience 'worthwhile,' or come to accept this 'diminution of privacy' as 'inevitable,' *post,* at 962, and perhaps not." *Id.* Justice Sotomayor, writing alone, raised a question, but did not even purport to answer it.

Justice Alito's concurrence further underscores why this Court is bound by Supreme Court precedent in *Smith* and *Miller.* Justice Alito concurred in the judgment and explained why the government-initiated, and government-controlled, real-time constant GPS monitoring violated the Fourth Amendment. *Id.* at ——, 132 S.Ct. at 957–64. Only the government did the tracking and its tracking was not authorized or regulated by a federal statute. *See id.* at ——, 132 S.Ct. at 956 (Sotomayor, J., concurring); *id.* at ——, 132 S.Ct. at 964 (Alito, J., concurring in the judgment). Justice Alito's focus is on unrestrained government power.

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

The context of his concurrence is critical. Nothing Justice Alito says contravenes the third-party doctrine. His concurring opinion does not question, or even cite, *Smith, Miller*, or the third-party doctrine in any way. The opinion never uses the words "third party" or "third-party doctrine." It would be a profound change in jurisprudence to say Justice Alito was questioning, much less casting aside, the third-party doctrine without even mentioning the doctrine.

Further, Justice Alito's concurrence speaks only at a high level of abstraction ***515** about the government's placement and control of an electronic GPS mechanism on a private vehicle that did the *precise, real-time, and long-term* monitoring. *See id.* at ——, 132 S.Ct. at 962–64. In stark contrast, the mechanism in Davis's case is MetroPCS's own electronic mechanism—the cell tower. MetroPCS created and assembled the electronic data. The government obtained access only through judicial supervision and a court order. Nothing in Justice Alito's concurrence in any way undermines the third-party doctrine. If anything, Justice Alito's concurrence, joined by three others, suggests that a legislative solution is needed. *Id.* at ——, 132 S.Ct. at 964 ("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." (citation omitted)). At present, the SCA is that solution.

Not only are Davis and the dissent ignoring controlling law, but even the internal logic of their arguments fails.[FN16]

FN16. The dissent remarks that we "ignore[ ] the opinion of five Justices of the Supreme Court at [our] own risk." Dissenting Op. at 540, n. 7. Quite the contrary, the majority opinion has faithfully recounted the two concurring opinions in *Jones* in the factual context of the case *actually decided* by the Supreme Court. Furthermore, because *Jones* involved a government trespass and not the third-party doctrine, eight of the nine Justices did not write or join one word about the "third-party doctrine," much less criticize it. It is the dissent that ignores, and fails to follow, binding Supreme Court precedent.

First, historical cell tower location data is materially distinguishable from the precise, real-time GPS tracking in *Jones,* even setting aside the controlling third-party doctrine discussed above. Historical cell tower location data does not identify the cell phone user's location with pinpoint precision—it identifies the cell tower that routed the user's call. 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. 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. This evidence still does not pinpoint the user's location. Historical cell site location data does not paint the "intimate portrait of personal, social, religious, medical, and other activities and interactions" that Davis claims.

Second, reasonable expectations of privacy under the Fourth Amendment do not turn on the quantity of non-content information MetroPCS collected in its historical cell tower location records. The § 2703(d) order covered 67 days of MetroPCS records. In his brief before this en banc Court, Davis argued that the length of the records covered by the order made the production an unconstitutional "search." But at oral argument Davis's counsel firmly contended that even *one day* of historical cell tower location information would require a search warrant supported by probable cause. Counsel's response at oral argument is faithful to Davis's broader claim, but misapprehends the governing law. Because Davis has no reasonable expectation of privacy in the type of non-content data collected in MetroPCS's historical cell tower records, neither one day nor 67 days of such records, produced by

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

court order, violate the Fourth Amendment.[FN17]

FN17. The SCA necessarily limits the time span of telephone records for which the government may secure a court order, as the government must show that such records are "relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

***516** As an extension of the argument above, Davis and various *amici* argue that cell tower data potentially implicating the home is due particular Fourth Amendment protection. In addition to noting the Supreme Court's clear rejection of this argument as it concerned toll records in *Smith,* we find it useful to recount the manner in which the evidence about Davis's home tower arose in this case.

On cross-examination by Davis's trial counsel, Detective Jacobs was asked whether a person's calls made from his or her home may be connected through a single cell tower—the "home tower." Detective Jacobs responded that they may be. Defense counsel followed up, asking whether, "[o]n the other hand ... you might see more than one tower" even though the person remains in his or her house? Again, Detective Jacobs responded yes. At that time, defense counsel was arguing the imprecision of the data collected. Like two riders in the same car, a user's calls from his home may be connected by different towers if more than one tower is located in range of the home. The government only discussed Davis's home tower after it was introduced by the defense, and only did so to illustrate that none of the robberies were committed in the vicinity of the home tower.

MetroPCS produced 67 days of historical cell site location information for Davis's cellular phone. Davis, a prolific cell phone user, made approximately 86 calls a day.[FN18] Without question, the number of calls made by Davis over the course of 67 days could, when closely analyzed, reveal certain patterns with regard to his physical location in the general vicinity of his home, work, and indeed the robbery locations. But no record evidence here indicates that the cell tower data contained within these business records produces precise locations or anything close to the "intimate portrait" of Davis's life that he now argues.[FN19] The judicial system does not engage in monitoring or a search when it compels the production of preexisting documents from a witness.

FN18. This number comes from an analysis of Davis's cell phone usage by the American Civil Liberties Union in its capacity as *amicus curiae* in this case. While all 67 days of toll records were placed in evidence against Davis, the government witnesses analyzed Davis's cell phone usage only for the seven days on which the armed robberies occurred.

FN19. Davis now also argues that the Supreme Court's recent decision in *Riley v. California,* 573 U.S. ——, 134 S.Ct. 2473, 189 L.Ed.2d 430 (2014), where law enforcement officers seized the cell phones of arrestees and then searched the contents of the phones without obtaining warrants, supports his claim of an unconstitutional search. *Riley* held that this warrantless search of the contents of a cell phone obtained incident to an arrest violated the Fourth Amendment. *Id.* at ——, 134 S.Ct. at 2485. But the Supreme Court in *Riley* made a special point of stressing that the facts before it "do not implicate the question whether the collection or inspection of aggregated digital information amounts to a search under other circumstances." *Id.* at ——, 134 S.Ct. at 2489 n. 1. It is not helpful to lump together doctrinally unrelated cases that happen to involve similar modern technology.

G. Reasonableness

[5][6] Even if this Court were to hold that obtaining MetroPCS's historical cell tower locations for a user's calls was a search and the Fourth

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

Amendment applies, that would begin, rather than end, our analysis. *Maryland v. King,* 569 U.S. ——, ——, 133 S.Ct. 1958, 1969, 186 L.Ed.2d 1 (2013). The Fourth Amendment prohibits unreasonable searches, not warrantless searches. As the text of the Fourth Amendment indicates, the ultimate measure of the constitutionality of a governmental ***517** search is "reasonableness." *Fernandez v. California,* 571 U.S. ——, ——, 134 S.Ct. 1126, 1132, 188 L.Ed.2d 25 (2014). "[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, 115 S.Ct. 2386, 2390–91, 132 L.Ed.2d 564 (1995).

[7][8] Simply put, the reasonableness of a search or seizure is evaluated "under traditional standards of reasonableness by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." *Wyoming v. Houghton,* 526 U.S. 295, 300, 119 S.Ct. 1297, 1300, 143 L.Ed.2d 408 (1999). In addition, "there is a strong presumption of constitutionality due to an Act of Congress, especially when it turns on what is 'reasonable' " within the meaning of the Fourth Amendment. *United States v. Watson,* 423 U.S. 411, 416, 96 S.Ct. 820, 824, 46 L.Ed.2d 598 (1976) (internal quotation marks omitted).

[9] This traditional Fourth Amendment analysis supports the reasonableness of the § 2703(d) order in this particular case. As outlined above, Davis had no reasonable expectation of privacy in business records made, kept, and owned by MetroPCS. At most, Davis would be able to assert only a diminished expectation of privacy in MetroPCS's records. *See King,* 569 U.S. at ——, 133 S.Ct. at 1969 (identifying "diminished expectations of privacy" as one of the factors that "may render a warrantless search or seizure reasonable" (quotation marks omitted)).

Further, any intrusion on Davis's alleged privacy expectation, arising out of MetroPCS's production of its own records pursuant to a § 2703(d) order, was minimal for several reasons. First, there was no overhearing or recording of any *conversations.* Second, there is no GPS real-time tracking of precise movements of a person or vehicle. Even in an urban area, MetroPCS's records do not show, and the examiner cannot pinpoint, the location of the cell user. Ironically, Davis was using *old* technology and not the *new* technology of a smartphone equipped with a GPS real-time, precise tracking device itself.

Third, a § 2703(d) court order functions as a judicial subpoena, but one which incorporates additional privacy protections that keep any intrusion minimal. The SCA guards against the improper acquisition or use of any personal information theoretically discoverable from such records. *See King,* 569 U.S. at ——, 133 S.Ct. at 1979–80. Under § 2703(d), investigative authorities may not request such customer-related records merely to satisfy prurient or otherwise insubstantial governmental interests. Instead, a neutral and detached magistrate must find, based on "specific and articulable facts," that there are "reasonable grounds to believe" that the requested records are "relevant and material to an ongoing criminal investigation." Such protections are sufficient to satisfy "the primary purpose of the Fourth Amendment," which is "to prevent arbitrary invasions of privacy." *Brock v. Emerson Elec. Co., Elec. & Space Div.,* 834 F.2d 994, 996 (11th Cir.1987); *see, e.g., Terry v. Ohio,* 392 U.S. 1, 21, 88 S.Ct. 1868, 20 L.Ed.2d 889 n.18, 392 U.S. 1, 88 S.Ct. 1868, 1880 n. 18, 20 L.Ed.2d 889 (1968) (explaining that the "demand for specificity in the information upon which police action is predicated is the central teaching of this Court's Fourth Amendment jurisprudence").

***518** The stored telephone records produced in this case, and in many other criminal cases, serve compelling governmental interests. Historical cell

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

tower location records are routinely used to investigate the full gamut of state and federal crimes, including child abductions, bombings, kidnappings, murders, robberies, sex offenses, and terrorism-related offenses. *See, e.g., United States v. Troya,* 733 F.3d 1125, 1136 (11th Cir.2013) ("quadruple homicide" involving the "gangland-style murder of two children"); *United States v. Mondestin,* 535 Fed.Appx. 819, 821 (11th Cir.2013) (unpublished) (per curiam) (armed robbery); *United States v. Sanders,* 708 F.3d 976, 982–83 (7th Cir.2013) (kidnapping). Such evidence is particularly valuable during the early stages of an investigation, when the police lack probable cause and are confronted with multiple suspects. In such cases, § 2703(d) orders—like other forms of compulsory process not subject to the search warrant procedure—help to build probable cause against the guilty, deflect suspicion from the innocent, aid in the search for truth, and judiciously allocate scarce investigative resources.

The societal interest in promptly apprehending criminals and preventing them from committing future offenses is "compelling." *See United States v. Salerno,* 481 U.S. 739, 750–51, 107 S.Ct. 2095, 2103, 95 L.Ed.2d 697 (1987). But so too is the societal interest in vindicating the rights of innocent suspects. *See King,* 569 U.S. at ——, 133 S.Ct. at 1974. Both interests are heavily implicated when the government seeks to compel the production of evidence "relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). Cell tower location records have the capacity to tell the police investigators that an individual suspect was in the general vicinity of the crime scene or far away in another city or state.

In sum, a traditional balancing of interests amply supports the reasonableness of the § 2703(d) order at issue here. Davis had at most a diminished expectation of privacy in business records made, kept, and owned by MetroPCS; the production of those records did not entail a serious invasion of any such privacy interest, particularly in light of the privacy-protecting provisions of the SCA; the disclosure of such records pursuant to a court order authorized by Congress served substantial governmental interests; and, given the strong presumption of constitutionality applicable here, any residual doubts concerning the reasonableness of any arguable "search" should be resolved in favor of the government. Hence, the § 2703(d) order permitting government access to MetroPCS's records comports with applicable Fourth Amendment principles and is not constitutionally unreasonable.[FN20]

FN20. In the alternative, we hold that the prosecutors and officers here acted in good faith and therefore, under the well-established *Leon* exception, the district court's denial of the motion to suppress did not constitute reversible error. *See United States v. Leon,* 468 U.S. 897, 919–21, 104 S.Ct. 3405, 3418–19, 82 L.Ed.2d 677 (1984).

IV. CONCLUSION

For the reasons set forth above, we affirm the judgment of conviction and vacate only that portion of the sentence attributable to the enhancement for brandishing.[FN21]

FN21. Because there are multiple opinions, it may be helpful to summarize the final count. Nine members of the en banc court agree there was no Fourth Amendment violation in this case. Seven members of the court join the majority opinion. Two members of the court, Judges Wilson and Jordan, join the majority opinion as to its reasonableness holding.

***519** WILLIAM PRYOR, Circuit Judge, concurring:

I join the majority opinion in full, but I write separately to explain that a court order compelling a telephone company to disclose cell tower location information would not violate a cell phone user's rights under the Fourth Amendment even in the absence of the protections afforded by the Stored

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

Communications Act, 18 U.S.C. §§ 2701–2712, and as judges of an inferior court, we must leave to the Supreme Court the task of developing exceptions to the rules it has required us to apply.

It is well-established that "the application of the Fourth Amendment depends on whether the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action." *Smith v. Maryland,* 442 U.S. 735, 740, 99 S.Ct. 2577, 2580, 61 L.Ed.2d 220 (1979) (citations omitted). And the Supreme Court has made clear that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Id.* at 743–44, 99 S.Ct. at 2582. There is no doubt that Davis voluntarily disclosed his location to a third party by using a cell phone to place or receive calls. For that reason, this appeal is easy.

Smith controls this appeal. In Smith, the Supreme Court held that, because telephone users voluntarily convey the phone numbers they dial to their telephone companies, the installation of a pen register at police request to record those numbers did not constitute a "search" under the Fourth Amendment. *Id.* at 742–46, 99 S.Ct. at 2581–83. But just as telephone users voluntarily convey the phone numbers they dial to a telephone company's switching equipment, cell phone users too voluntarily convey their approximate location to a carrier's cell towers.

To the extent that *Smith* is distinguishable from this appeal, *Smith* presents a *closer* question, because in this appeal the government did not request that MetroPCS maintain records of its customers' cell phone calls. MetroPCS decided what business records to maintain, and the government sought the records of Davis's calls after the fact. And those records contained location information that Davis voluntarily conveyed to MetroPCS by placing calls that were routed through nearby cell towers, which are a familiar part of our landscape.

That Davis had no legitimate expectation of privacy in the information he conveyed to MetroPCS follows from a straightforward application of the third-party doctrine, completely aside from the additional protections of the Stored Communications Act. The Act provides that a court order for disclosure "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." 18 U.S.C. § 2703(d). Davis does not dispute that the government complied with the Act. But the greater protections afforded telephone customers under the Act do not disturb the constitutional principle 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, 99 S.Ct. at 2582. So Davis would have no legitimate expectation of privacy in the information he conveyed to MetroPCS even if Congress repealed the Act tomorrow. A court order compelling a carrier to disclose cell tower location information does not violate a cell phone user's rights under the Fourth Amendment any more than a court order compelling a bank to disclose customer account information, *see* ***520** *United States v. Miller,* 425 U.S. 435, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976).

The dissent's argument that *Smith* is distinguishable from this appeal because the disclosure of location information to cell carriers is less "voluntary" and less "knowing," Dissenting Op. at 534–35, than the disclosure of dialed telephone numbers makes no sense. The dissent argues that the disclosure of location information is less "voluntary" than the disclosure of dialed telephone numbers because "cell phone users do not affirmatively enter their location in order to make a call," *Id.* at 534, but in neither case is a phone user coerced to reveal anything. If a telephone caller does not want to reveal dialed numbers to the telephone company, he has another option: don't place a call. If a cell phone user does not want to reveal his location to a cellular carrier, he also has another option: turn off the cell phone. That Davis had to dis-

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

close his location in order to place or receive a call does not distinguish this appeal from *Smith,* because, as the dissent admits, telephone callers "have to" convey dialed numbers to the telephone company in order to place calls, Dissenting Op. at 534. That a caller "affirmatively enter[s]" phone numbers but a cell phone user does not "affirmatively enter" his location when he places or receives a call may implicate the user's *knowledge* that he is conveying information to a third party, but it does not make the latter disclosure less *voluntary* than the former. Davis's disclosure of his location was also no less "knowing" than the disclosure at issue in *Smith.* In *Smith,* the Supreme Court explained that "[a]ll telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed." 442 U.S. at 742, 99 S.Ct. at 2581. Similarly, cell phone users realize that their calls are routed through nearby cell towers. It is no state secret that cell phones work less effectively in remote areas without cell towers nearby. As the Court made clear in *Smith,* that "most people may be oblivious to" the "esoteric functions" of a technology is consistent with most people having "some awareness" of its purpose. *Id.* at 742, 99 S.Ct. at 2581. In the light of common experience, it is "too much to believe," *id.* at 743, 99 S.Ct. at 2581, that cell phone users lack "some awareness," *id.* at 742, 99 S.Ct. at 2581, that they communicate information about their location to cell towers.

If the rapid development of technology has any implications for our interpretation of the Fourth Amendment, it militates in favor of judicial caution, because Congress, not the judiciary, has the institutional competence to evaluate complex and evolving technologies. "Judges cannot readily understand how ... technologies may develop, cannot easily appreciate context, and often cannot even recognize whether the facts of the case before them raise privacy implications that happen to be typical or atypical." Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution,* 102 Mich. L.Rev. 801, 858–59 (2004). Our decisions resolve adversarial proceedings between parties. Legislatures, by contrast, must consider "a wide range" of factors and balance the opinions and demands of competing interest groups. *Id.* at 875. "The task of generating balanced and nuanced rules requires a comprehensive understanding of technological facts. Legislatures are well-equipped to develop such understandings; courts generally are not." *Id.* Simply put, we must apply the law and leave the task of developing new rules for rapidly changing technologies to the branch most capable of weighing the costs and benefits of doing so.

***521** As judges of an inferior court, we have no business in anticipating future decisions of the Supreme Court. If the third-party doctrine results in an unacceptable "slippery slope," Dissenting Op. at 537, the Supreme Court can tell us as much. *See, e.g., Hohn v. United States,* 524 U.S. 236, 252–53, 118 S.Ct. 1969, 1978, 141 L.Ed.2d 242 (1998) ("Our decisions remain binding precedent until we see fit to reconsider them, regardless of whether subsequent cases have raised doubts about their continuing vitality."); *Rodriguez de Quijas v. Shearson/Am. Express, Inc.,* 490 U.S. 477, 484, 109 S.Ct. 1917, 1921–22, 104 L.Ed.2d 526 (1989) ("If a precedent of this Court has direct application in a case, yet appears to rest on reasons rejected in some other line of decisions, the Court of Appeals should follow the case which directly controls, leaving to this Court the prerogative of overruling its own decisions."); *Evans v. Sec'y, Fla. Dep't of Corr.,* 699 F.3d 1249, 1263 (11th Cir.2012) ("We must not, to borrow Judge Hand's felicitous words, 'embrace the exhilarating opportunity of anticipating' the overruling of a Supreme Court decision.") (internal citation omitted). That is, if "the Supreme Court has given reasons to doubt the rule's breadth," Dissenting Op. at 535, it alone must decide the exceptions to its rule.

JORDAN, Circuit Judge, concurring, in which WILSON, Circuit Judge, joins:

This case is certainly about the present, but it is

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

also potentially about the future. Although the Court limits its decision to the world (and technology) as we knew it in 2010, *see* Maj. Op. at 503–04 n. 7 & 513 n. 13, its holding that Mr. Davis lacked an expectation of privacy in service provider records used to establish his cell site location may have implications going forward, particularly given the Court's reliance on the third-party doctrine. *See, e.g., Smith v. Maryland,* 442 U.S. 735, 743–44, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979); *United States v. Miller,* 425 U.S. 435, 442–43, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976). As technology advances, location information from cellphones (and, of course, smartphones) will undoubtedly become more precise and easier to obtain, *see generally Planet of the Phones,* THE ECONOMIST (Feb. 28, 2015), and if there is no expectation of privacy here, I have some concerns about the government being able to conduct 24/7 electronic tracking (live or historical) in the years to come without an appropriate judicial order. And I do not think I am alone in this respect. *See United States v. Jones,* ——U.S. ——, 132 S.Ct. 945, 964, 181 L.Ed.2d 911 (2012) (Alito, J., concurring, joined by Ginsburg, Breyer, and Kagan, JJ.) ("[T]he use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."); *id.* at 955 (Sotomayor, J., concurring) ("I agree with Justice Alito that, at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.' ").[FN1]

FN1. Three decades ago, a defendant in a case before the Supreme Court argued that allowing the police to place a digital beeper in a container filled with chloroform, in order to monitor the container's location, would lead to "twenty-four hour surveillance of any citizen in this country ... without judicial knowledge or supervision." *United States v. Knotts,* 460 U.S. 276, 283–84, 103 S.Ct. 1081, 75 L.Ed.2d 55 (1983). The Supreme Court's response to that assertion was that "if such dragnet type law enforcement practices as [the defendant] envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable." *Id.*

As a result, I would decide the Fourth Amendment question on reasonableness grounds and leave the broader expectation of privacy issues for another day, much like the Supreme Court did in *City of* ****522*** *Ontario v. Quon,* 560 U.S. 746, 759–60, 130 S.Ct. 2619, 177 L.Ed.2d 216 (2010) (assuming that police officer had an expectation of privacy in text messages he sent from his city-provided pager, even though those messages were routed through and kept by a third-party service provider, and resolving the case on reasonableness grounds). I would assume that Mr. Davis had a reasonable expectation of privacy—albeit a diminished one—and hold that the government satisfied the Fourth Amendment's reasonableness requirement by using the procedures set forth in 18 U.S.C. § 2703(d) to obtain a court order for Mr. Davis' cell site records.

I

The Fourth Amendment's "basic purpose ... is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." *Camara v. Mun. Court of City & Cnty. of S.F.,* 387 U.S. 523, 528, 87 S.Ct. 1727, 18 L.Ed.2d 930 (1967). "As the text of the Fourth Amendment indicates, the ultimate measure of the constitutionality of a governmental search is 'reasonableness.' " *Maryland v. King,* —— U.S. ——, 133 S.Ct. 1958, 1969, 186 L.Ed.2d 1 (2013) (citation and internal punctuation omitted).

"The reasonableness of a search," the Supreme Court recently explained, "depends on the totality of the circumstances, including the nature and purpose of the search and the extent to which the search intrudes upon reasonable privacy expectations." *Grady v. North Carolina,* —— U.S. ——, 135 S.Ct. 1368, 1371, —— L.Ed.2d —— (2015). These circumstances include, among others, "the means adopted" by the government to effectuate the search. *See Carroll v. United States,* 267 U.S. 132,

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

168, 45 S.Ct. 280, 69 L.Ed. 543 (1925).

II

At times, circumstances may render a warrantless search or seizure reasonable. One such scenario is when there are "diminished expectations of privacy." *King,* 133 S.Ct. at 1969 (citation and internal punctuation omitted). Although I am prepared to assume that Mr. Davis enjoyed some expectation of privacy, *cf.* STEPHEN J. SCHULHOFER, MORE ESSENTIAL THAN EVER: THE FOURTH AMENDMENT IN THE TWENTY–FIRST CENTURY 8 (2012) (defining privacy, in today's digital world, in terms of control rather than secrecy, because practical necessities now require individuals to share information about themselves "with trusted individuals and institutions for limited purposes"), I think it is fair to say that such an expectation was somewhat diminished, and not full-throated, due to the third-party doctrine. After all, *Smith* indicates that a person gives up control of certain information when he makes and receives calls from a phone. Although *Smith* does not fit this case like a glove—cellphones and smartphones (and the vast amounts of information they contain and can generate) are qualitatively different from land-line phones—it is nevertheless relevant that the cell site information the government obtained existed due to calls Mr. Davis made and received on his cellphone.[FN2]

FN2. I recognize that some of the cell site information resulted from calls Mr. Davis received but never answered. For obvious reasons, however, Mr. Davis did not make (and has not made) a nuanced Fourth Amendment argument differentiating between data generated from calls he made and answered and data generated from calls he merely received without answering. Such an argument would not have been of much help to Mr. Davis, who sought to suppress all of the cell site data the government obtained.

On the other side of the ledger, Mr. Davis' cell site information was not obtained***523** or seized "outside the judicial process, without prior approval by a judge or magistrate." *Coolidge v. New Hampshire,* 403 U.S. 443, 454–55, 91 S.Ct. 2022, 29 L.Ed.2d 564 (1971). *Cf. Johnson v. United States,* 333 U.S. 10, 13–14, 68 S.Ct. 367, 92 L.Ed. 436 (1948) (noting that the Fourth Amendment's "protection consists in requiring that ... inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime"). The government secured the cell site records under a provision of the Stored Communications Act. And that provision requires a magistrate judge—a neutral judicial officer—to review an application and determine whether the government has offered "specific and articulable facts showing that there are reasonable grounds to believe that the [cell cite location information] sought [is] relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). Significantly, "there is a strong presumption of constitutionality due to an Act of Congress, especially when it turns on what is 'reasonable [,]' " *United States v. Watson,* 423 U.S. 411, 416, 96 S.Ct. 820, 46 L.Ed.2d 598 (1976) (citation and some internal punctuation omitted), and this strong presumption attaches to § 2703(d).

As explained briefly below, the government articulated the necessary "specific and articulable facts." I therefore agree with the Court that the magistrate judge's order, which authorized the government to obtain the cell site information, satisfied the reasonableness requirement of the Fourth Amendment. *See Camara,* 387 U.S. at 528, 87 S.Ct. 1727.[FN3]

FN3. For whatever it is worth, the Supreme Court has on occasion held that the phrase "reasonable grounds," as used in certain federal narcotics laws, is essentially the same as "probable cause" for purposes of the Fourth Amendment. *See Draper v. United States,* 358 U.S. 307, 310 n. 3, 79 S.Ct. 329, 3 L.Ed.2d 327 (1959); *Wong*

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

Sun v. United States, 371 U.S. 471, 478 n. 6, 83 S.Ct. 407, 9 L.Ed.2d 441 (1963). And it has said that "[t]he substance of all the definitions of probable cause is a reasonable ground for belief of guilt." *Maryland v. Pringle,* 540 U.S. 366, 371, 124 S.Ct. 795, 157 L.Ed.2d 769 (2003) (citation and internal punctuation omitted). So maybe the evidentiary showing required by § 2703(d) is not too far removed from the probable cause normally demanded for warrants under the Fourth Amendment. *But cf. Griffin v. Wisconsin,* 483 U.S. 868, 872–77, 107 S.Ct. 3164, 97 L.Ed.2d 709 (1987) (differentiating between "reasonable grounds" standard and "probable cause" standard).

The government's application for Mr. Davis' cell site information stated the following: Willie Smith confessed that he and Mr. Davis were involved in the robberies of a Little Caesar's restaurant, the Universal Beauty Salon, and a Wendy's restaurant in Miami, Florida; Jamarquis Terrell Reid admitted that he had participated with Mr. Davis in the robberies of an Amerika gas station, a Walgreens store, and an Advance Auto Parts store in Miami, Florida; Michael Martin told the authorities that he and Mr. Davis had robbed a Mayor's jewelry store in Weston, Florida; Mr. Davis' DNA was recovered from a stolen BMW that was used as the getaway car in the Mayor's jewelry store robbery; the robberies in question took place between August 7, 2010, and October 1, 2010; and Mr. Smith and Mr. Reid each said that, at the time of certain of the robberies (those of the Little Caesar's restaurant, the Amerika gas station, the Advance Auto Parts store, and the Universal Beauty Salon), Mr. Davis' cellphone number was the 5642 number. Not surprisingly, Mr. Davis conceded at oral argument that the government could have secured a warrant (had it elected to do so) for the cell site information because it had the necessary probable cause.

***524** The temporal scope of the request, moreover, was reasonable. The government sought cell site information spanning from August 1, 2010, to October 6, 2010—a 67–day period which began six days before the first known robbery and ended six days after the last known robbery. The government explained in its application that those records would "assist law enforcement in determining the locations of [Mr. Davis] on days when robberies in which [he was] suspected to have participated occurred," and "whether [he] communicated with [the] other [individuals] on the days of the robberies and, if so, how many times."

Finally, it is important to reiterate that the cell site information was generated from calls Mr. Davis made and received on his cellphone, and was not the result of his merely having his cellphone turned on. There was, in other words, no passive tracking based on Mr. Davis' mere possession of a cellphone, and I do not read the Court's opinion as addressing such a situation. *See* Maj. Op. at 502, 512.

III

For me, this is one of those cases where it makes sense to say less and decide less. *See* CASS R. SUNSTEIN, ONE CASE AT A TIME 4–10 (1999); ALEXANDER M. BICKEL, THE LEAST DANGEROUS BRANCH 111–13 (1st ed.1962). "Prudence counsels caution before the facts in the instant case are used to establish ... premises that define the existence, and extent, of privacy expectations." *Quon,* 560 U.S. at 759, 130 S.Ct. 2619.

With these thoughts, I join Parts I, II, III.G, and IV of the Court's opinion and concur in the judgment.

ROSENBAUM, Circuit Judge, concurring.

I concur in the Majority's opinion. I write separately, though, because, like the Dissent, I think that the third-party doctrine,[FN1] as it relates to modern technology, warrants additional consideration and discussion. I view the third-party doctrine as applying in this case because *Smith v. Maryland,* 442 U.S. 735, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979), implicitly found no historical expectation of privacy implicated by the information that we give

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

to a service provider for the purpose of making a telephone call other than the expectation of privacy that we generally do not have in information that we voluntarily convey to a third party. Since, like *Smith,* this case involves information that we knowingly expose to a service provider for the purpose of making a telephone call and no more specific historically recognized privacy interest is implicated by cell-site location information, this case is necessarily controlled by *Smith.*

FN1. The third-party doctrine applies when a person voluntarily entrusts information to a third party, and it generally renders the Fourth Amendment's warrant requirement inapplicable as it pertains to the procurement of the exposed information from the third party. *See United States v. Miller,* 425 U.S. 435, 442–43, 96 S.Ct. 1619, 1624, 48 L.Ed.2d 71 (1976).

But when, historically, we have a more specific expectation of privacy in a particular type of information, the more specific privacy interest must govern the Fourth Amendment analysis, even though we have exposed the information at issue to a third party by using technology to give, receive, obtain, or otherwise use the protected information. In other words, our historical expectations of privacy do not change or somehow weaken simply because we now happen to use modern technology to engage***525** in activities in which we have historically maintained protected privacy interests. Neither can the protections of the Fourth Amendment. *See Kyllo v. United States,* 533 U.S. 27, 34, 121 S.Ct. 2038, 2043, 150 L.Ed.2d 94 (2001) ("To withdraw protection of this minimum expectation [of privacy] would be to permit ... technology to erode the privacy guaranteed by the Fourth Amendment."). So reliance on the third-party doctrine must be limited to those cases involving alleged privacy interests that do not implicate a more specific historically recognized reasonable privacy interest.

I.

Before exploring why this is so, I pause to express my view that the Dissent is right to raise its concerns. In our time, unless a person is willing to live "off the grid," it is nearly impossible to avoid disclosing the most personal of information to third-party service providers on a constant basis, just to navigate daily life. And the thought that the government should be able to access such information without the basic protection that a warrant offers is nothing less than chilling. Today's world, with its total integration of third-party-provided technological services into everyday life, presents a steroidal version of the problems that Justices Marshall and Brennan envisioned when they dissented in *United States v. Miller,* 425 U.S. 435, 447, 454, 96 S.Ct. 1619, 1626, 1629, 48 L.Ed.2d 71 (1976) (Brennan, J., and Marshall, J., dissenting, respectively), and its progeny, including *Smith v. Maryland,* 442 U.S. 735, 748, 99 S.Ct. 2577, 2584, 61 L.Ed.2d 220 (1979) (Marshall, J., dissenting). As Justice Marshall aptly explained the problem, under the third-party doctrine, "unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance." *Smith,* 442 U.S. at 750, 99 S.Ct. 2577, 2585, 61 L.Ed.2d 220 (Marshall, J., dissenting). Perhaps it was this type of realization that caused Justice Sotomayor to write, "[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." *United States v. Jones,* —— U.S. ——, 132 S.Ct. 945, 957, 181 L.Ed.2d 911 (Sotomayor, J., concurring). Since we are not the Supreme Court and the third-party doctrine continues to exist and to be good law at this time, though, we must apply the third-party doctrine where appropriate.

But, as the Dissent points out, the mere fact that the third-party doctrine could have been applied to an alleged privacy interest does not mean that it always has been. To ensure that this is a case where the third-party doctrine should be applied, I think it important to consider what sets apart those cases where the Supreme Court has chosen not to

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

apply the third-party doctrine, despite the fact that a party has exposed its effects or information to a third party.

II.

The Supreme Court has explained that, in analyzing a Fourth Amendment claim, we begin by determining "whether the action was regarded as an unlawful search or seizure under the common law when the Amendment was framed." *Wyoming v. Houghton,* 526 U.S. 295, 299, 119 S.Ct. 1297, 1300, 143 L.Ed.2d 408 (1999). We do this because, "[a]t bottom, we must 'assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.' " FN2 ***527** *United States v. Jones,* —— U.S. ——, 132 S.Ct. 945, 950, 181 L.Ed.2d 911 (2012) (citation omitted). So it seems to me that existing Supreme Court precedent may fairly be construed to suggest that where society has historically recognized a legitimate expectation of privacy, we must continue to do so for purposes of Fourth Amendment analysis, even if, in our modern world, we must now expose to a third party information that we would have previously kept private, in order to continue to participate fully in society. If we do not, we will face the Hobson's choice of leaving our historically recognized Fourth Amendment rights at the door of the modern world or finding ourselves locked out from it. That the Constitution will not abide.

FN2. Some might suggest that we must first determine whether a search within the meaning of the Fourth Amendment has occurred, and only if one has should we then assess whether that search has violated a constitutionally protected expectation of privacy, in the context of engaging in a reasonableness analysis. But generally, when the alleged search is of information and it is not accompanied by a concurrent physical trespass, we must evaluate whether a reasonable expectation of privacy existed in the information in the first place in order to determine whether a "search" has occurred. *See Katz v. United States,* 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967); *Smith,* 442 U.S. 735, 99 S.Ct. 2577. That inquiry requires us to resolve the conflict between the historical expectation of privacy allegedly violated by the search and the third-party doctrine's rule that no expectation of privacy exists when a person voluntarily exposes information to a third party. And under the reasonableness analysis, we balance the degree to which a search or seizure "intrudes upon an individual's privacy" against "the degree to which it is needed for the promotion of legitimate governmental interests." *Wyoming v. Houghton,* 526 U.S. 295, 300, 119 S.Ct. 1297, 1300, 143 L.Ed.2d 408 (1999). So we would again need to figure out the relationship between the competing historical expectation of privacy and the third-party doctrine to determine the ultimate expectation of privacy to weigh against the government's interest. As a result, this two-step analysis becomes redundant in the context of an alleged search of information without a concurrent physical trespass.

Moreover, if, in conducting the reasonableness analysis, we ignore the historical privacy interest and always defer to the third-party doctrine, that does not account for the way in which the Supreme Court has resolved the conflict between the historical privacy interest and the third-party doctrine in cases like *Katz,* 389 U.S. 347, 88 S.Ct. 507, because ignoring the historical privacy interest in favor of the third-party doctrine would always result in a determination that no warrant is required under a reasonableness evaluation. This is necessarily so because when the third-party doctrine applies, by definition, there is no reasonable privacy interest to weigh on the in-

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

dividual's side of the scale against the government's interest in crime fighting. But "the normal need for law enforcement" generally cannot exempt a search from the warrant requirement where the searched party enjoys a reasonable expectation of privacy, *Vernonia Sch. Dist. 47J v. Acton,* 515 U.S. 646, 653, 115 S.Ct. 2386, 2391, 132 L.Ed.2d 564 (1995), such as when the privacy interest atstakehashistoricallybeenrecognized-unless, of course, it is impracticable to obtain a warrant under the circumstances. *See, e.g., Terry v. Ohio,* 392 U.S. 1, 88 S.Ct. 1868, 20 L.Ed.2d 889 (1967). And if we resolved the conflict between the historically existing privacy interest and the third-party doctrine by assuming a diminished expectation of privacy in the historical interest being weighed against the government's general interest in crime fighting, that still would not seem to account for cases like *Katz,* 389 U.S. 347, 88 S.Ct. 507, even if the Court found that satisfying a lesser requirement than probable cause, such as that set forth by § 2703(d), was necessary to obtain the information. Indeed, I am aware of no case where the Court has expressly found an expectation of privacy diminished because of the third-party doctrine and yet has concluded that a warrant was required. *But cf. Riley v. California,* —— U.S. ——, 134 S.Ct. 2473, 2488, 189 L.Ed.2d 430 (2014) (holding that a warrant is generally required to search an arrestee's cell phone, even though arrestees have a diminished expectation of privacy because of their status as arrestees). Whether we ignored the more specific historical privacy interest in favor of the third-party doctrine or found that the historical privacy interest was diminished, though, privacy interests long recognized as reasonable by society, which therefore historically necessitated a showing of probable cause and a warrant under the Fourth Amendment in order to breach, would be violated without a warrant and on a showing of less than probable cause, simply because we happen to use technology to do more efficiently what we used to do without technology. I do not believe that Supreme Court precedent supports the conclusion that the long-established privacy interests protected by the Fourth Amendment should be subject to the whims of technology. *See Kyllo,* 533 U.S. at 34, 121 S.Ct. at 2043 (2001) ("To withdraw protection of this minimum expectation [of privacy] would be to permit ... technology to erode the privacy guaranteed by the Fourth Amendment."). And even if the Court were prepared to conclude that a privacy interest diminished by the third-party doctrine nonetheless required a warrant to breach, it would still need to articulate why one particular expectation of privacy diminished by the third-party doctrine was sufficient to outweigh the government's general interest in crime fighting, while a different expectation of privacy diminished by the third-party doctrine was not, unless the more specific historical expectation of privacy negates the effects of the third-party doctrine in evaluating the privacy interest for purposes of conducting the reasonableness analysis.

A.

As the Dissent points out, the Supreme Court has held that "[a] hotel room can clearly be the object of Fourth Amendment protection as much as a home or an office." *Hoffa v. United States,* 385 U.S. 293, 301, 87 S.Ct. 408, 413, 17 L.Ed.2d 374 (1966); *see also Minnesota v. Carter,* 525 U.S. 83, 95–96, 119 S.Ct. 469, 476, 142 L.Ed.2d 373 (1998) (Scalia, J., concurring) (citing *Oystead v. Shed,* 13

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

Mass. 520 (1816), for the proposition that a trespass occurs when the sheriff breaks into a dwelling to capture a boarder living there); *Minnesota v. Olson,* 495 U.S. 91, 96–97, 110 S.Ct. 1684, 1688, 109 L.Ed.2d 85 (1990) (holding that overnight guests in the homes of a third person can have a reasonable expectation of privacy in those premises). This is so, even though housekeepers and maintenance people commonly have access to hotel rooms during a guest's stay and can view and even move around a guest's belongings in order to conduct their duties. But the fact that a hotel guest has exposed his or her belongings to hotel workers does not, in and of itself, entitle the government to enter a rented hotel room and conduct a warrantless search.

Similarly, historically, human operators were known to eavesdrop on the contents of telephone calls in the early days of telephone usage. *See* Jeff Nilsson, *What the Operators Overheard in* 1907, The Saturday Evening Post, June 30, 2012, http:// www. saturday eveningpost. com/ 2012/ 06/ 30/ history/ post- perspective/ operators– heard– 1907. html (last visited Apr. 16, 2015). And, as Justice Stewart observed, even after human operators were taken out of the equation, telephone conversations may have been "recorded or overheard by the use of other [telephone] company equipment." *Smith v. Maryland,* 442 U.S. 735, 746, 99 S.Ct. 2577, 2583, 61 L.Ed.2d 220 (1979) (Stewart, J., dissenting). But the fact that, historically, we exposed our private conversations to third parties did not stop the Supreme Court from holding in *Katz v. United States,* 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967), that we have a reasonable expectation of privacy in telephone communications and that the government generally must obtain a warrant before intercepting them.

Why should that be so when the third-party doctrine also speaks to what a reasonable expectation of privacy is (none where it applies), and the doctrine seemingly applies to these situations? I believe that Supreme Court precedent fairly may be read to suggest that the third-party doctrine must be subordinate to expectations of privacy that society has historically recognized as reasonable. Indeed, our ***528** privacy expectations in modern-day hotels and the content of our telephone conversations hearken back to historically recognized reasonable expectations of privacy.

As Justice Scalia has explained, "The people's protection against unreasonable search and seizure in their 'houses' was drawn from the English common-law maxim, 'A man's home is his castle.' " *Carter,* 525 U.S. at 95, 119 S.Ct. at 475 (Scalia, J., concurring) (emphasis omitted). And a person enjoys a recognized expectation of privacy in that home, provided he or she actually is living there. *Id.* at 95–96, 119 S.Ct. at 476. So, when a person rents and dwells in a hotel room,[FN3] that hotel room becomes that person's "home" and "castle," for purposes of the Fourth Amendment, regardless of who else may enter the premises.

FN3. I recognize that inns existed in the Framers' day.

As for the telephone, it, of course, was not invented until the late 1800's and was not widely used until well after the Framers' time.[FN4] Until then, people who were not closely located to each other typically communicated by letter. *See, e.g.,* https:// jefferson papers. princeton. edu/ (last visited Apr. 16, 2015) (noting that Thomas Jefferson wrote and received letters). As the Supreme Court has noted, "Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy...." *United States v. Jacobsen,* 466 U.S. 109, 114, 104 S.Ct. 1652, 1657–58, 80 L.Ed.2d 85 (1984); *see also Ex parte Jackson,* 96 U.S. 727, 733, 6 Otto 727, 24 L.Ed. 877 (1877).

FN4. Alexander Graham Bell obtained a patent for the telephone on March 7, 1876. *See* http:// www. pbs. org/ transistor/ album 1/ addlbios/ bellag. html (last visited Apr. 16, 2015). He successfully transmit-

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

ted speech over the line five days later. *Id.* But the United States House of Representatives has since recognized Antonio Meucci as the inventor of the telephone. H.R. Res. 269, 107th Cong. (June 11, 2002). Meucci reportedly developed the first version of a working telephone in 1860. *See id.*

While the Supreme Court did not mention society's reasonable expectation of privacy in the content of communications sent by letter through third parties when it found a reasonable expectation of privacy in the content of communications transmitted by telephone through third parties in *Katz,* it is clear that the historical expectation of privacy in communications by letter is the same expectation of privacy that we continue to have in communications that we conduct by telephone. And the fact that we have always had to rely on third parties to engage in telephone calls—even when the third parties were known to eavesdrop from time to time—does not somehow change our reasonable expectation of privacy in personal telephone calls. Put simply, the fact that we have changed the way that we conduct personal communications does not mean that we have altered our expectation of privacy in our personal communications.

B.

To help explain how the conflict between historically recognized privacy interests and the third-party doctrine plays out in light of modern technology—and why the cell-site location information at issue in this case is subject to the third-party doctrine—consider a few examples of historical privacy interests implicated by modern technology.

If our expectation of privacy in our personal communications has not changed from what it was when we only wrote letters to what it is now that we use telephones to conduct our personal interactions,***529** it has not changed just because we now happen to use email to personally communicate. [FN5] *See United States v. Warshak,* 631 F.3d 266, 288 (6th Cir.2010). Just as the need to entrust third parties with our personal conversations when we communicate by written letter or by telephone does not affect the analysis, the need to rely on third parties to provide Internet service when we communicate by email cannot do so, either.

FN5. The Supreme Court has held that addressing and other routing information on paper letters, like pen-register and trap-and-trace information (including the date and time of listed calls) regarding telephone calls, is accessible to the government without a warrant. *See Ex parte Jackson,* 96 U.S. 727, 736, 24 L.Ed. 877; *Smith,* 442 U.S. 735, 99 S.Ct. 2577. Email routing information, such as the sender, the receiver, the date, the time, and other routing information (such as Internet Protocol addresses) implicates the same expectations of privacy as older versions of routing information found on paper letters and in pen-register and trap-and-trace information. *See United States v. Forrester,* 512 F.3d 500, 511 (9th Cir.2007). The lack of a reasonable expectation of privacy in routing information as it pertains to paper letters and telephone conversations does not change just because the medium for engaging in personal conversations does. Subject lines in emails, however, are not in any way related to the routing or transaction information of an email; no one writes the subject matter of the letters they send on the outside of the envelope, and people do not give the telephone service provider a general overview of the telephone conversations they are about to have. So subject-matter lines on emails cannot be governed by the lack of an expectation of privacy attending paper-letter or telephone-call routing information. Instead, subject-matter lines usually disclose a summary or general statement about the content of the email communication itself, and the privacy interest implicated by subject-matter

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

> lines is therefore the same as the privacy interest in personal communications conducted by paper letters and telephone calls. As a result, as with the content of paper letters and telephone conversations, a reasonable expectation of privacy exists in the subject-matter lines of emails.

The same is true for our other historically recognized reasonable expectations of privacy. So, for instance, while the Internet and its search engines obviously did not exist in the 18th century, libraries did. *See, e.g.,* http:// franklinma. virtual townhall. net/ Pages/ Franklin MA_ Library/ libraryhistory (last visited Apr. 13, 2015) (discussing the establishment of the Franklin Public Library in 1790). And, though libraries no doubt have always kept track of the books checked out, they have not monitored what a person reviews within the borrowed books, and library users have traditionally been free to anonymously peruse materials at the library without checking them out and creating a record. This anonymity is critical to First Amendment rights. *See, e.g., United States v. Rumely,* 345 U.S. 41, 57–58, 73 S.Ct. 543, 551–52, 97 L.Ed. 770 (1953) (Douglas, J., concurring) ("When the light of publicity may reach any student, any teacher, inquiry will be discouraged.... If [a reader] can be required to disclose what she read yesterday and what she will read tomorrow, fear will take the place of freedom in the libraries ... of the land").

This privacy interest is no less important simply because many of us now use the Internet to do what we used to do at the library. We do not have lower expectations of privacy in what we research—particularly with respect to our expectations that the government will not be looking over our shoulders to review our work—merely because we research and read it online at home or in a coffee shop instead of in hard copies of books and periodicals in the stacks of the library, even though the only way that we can conduct online research is through a third-party service provider. In short, the expectation of privacy in reading and researching what we want, free from government***530** surveillance without a warrant, has not changed just because the mechanism we use for engaging in this conduct has evolved.

As for documents that we store in the Cloud, our privacy interest there is the same as that recognized in documents and other items maintained in a rented office or residence, or a hotel room during a paid visit. As discussed previously, the Supreme Court has plainly recognized as reasonable under the Fourth Amendment the privacy interest in effects held in such places, even though a straightforward application of the third-party doctrine would suggest the opposite conclusion, particularly in the case of a hotel room, where housekeeping and maintenance workers can be expected to enter the premises. The privacy expectation has not abraded simply because the effect to be searched is virtual and the "place" of storage is now the intangible Cloud. *Cf. Riley v. California,* —— U.S. ——, 134 S.Ct. 2473, 2494–95, 189 L.Ed.2d 430 (2014) (recognizing that searches of cell phones implicate the same type of privacy interest invaded by the "reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity," and holding that a warrant is generally required to search a cell phone in an arrestee's possession at the time of arrest, despite the historical rule allowing for a search of effects on an arrestee at the time of arrest). "For the Fourth Amendment protects people, not places." *Katz,* 389 U.S. at 351, 88 S.Ct. at 511.

C.

And Justice Alito's concurrence in *Jones,* 132 S.Ct. at 964 (Alito, J., concurring in the judgment), suggests a viable and apt historical privacy interest that pertains to global-positioning system information: the expectation of privacy as it regards incessant surveillance. Justice Alito has described this expectation of privacy as follows:

> [R]elatively short-term monitoring of a person's movements on public streets accords with expect-

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

> ations of privacy that our society has recognized as reasonable.... But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period.
>
> *Id.*

Three other Justices joined in Justice Alito's *Jones* concurrence, and another, Justice Sotomayor, expressed her agreement with the idea that, "at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.' " *Id.* at 955 (Sotomayor, J., concurring) (quoting *id.* at 964 (Alito, J., concurring)). While this view may not constitute binding Supreme Court precedent, it certainly suggests that society has long viewed as reasonable the expectation of privacy in not being subjected to constant, longer-term surveillance. And if that's the case, the only question that remains about whether the government must obtain a warrant to engage in longer-term GPS monitoring is where we draw the line establishing what constitutes "longer-term" GPS monitoring. But that is not a question that we must answer today.

Nevertheless, in my opinion, the longer-term GPS issue necessarily means that the Dissent is correct in its concerns that the expectation of privacy that is infringed by longer-term GPS monitoring may, at some ***531** point, become the same expectation of privacy implicated by more and more precise cell-site location technology. When that happens, the historical reasonable expectation of privacy in not being subjected to longer-term surveillance may well supersede the third-party doctrine's applicability to information entrusted to third parties as it pertains to cell-site location information.[FN6] But that is not this case.

> FN6. One other perhaps significant difference between GPS technology and precise cell-site location information also exists: GPS monitoring is constant, whereas cell-site location information is produced only when a cell-phone user makes or receives a call. If a person is usually on the cell phone, that may be a distinction without a difference. But if a person is not, that may be a meaningful dissimilarity. We conduct Fourth Amendment jurisprudence "with an eye to the generality of cases." *See Houghton,* 526 U.S. at 304, 119 S.Ct. at 1303 (balancing interests under the Fourth Amendment's reasonableness approach). So that factual issue may require resolution at a future time.

According to the MetroPCS records custodian who testified in this case, the radii of the cell towers at issue were approximately a mile to a mile and a half. Since a sector is generally a one-third to a one-sixth pie slice of the roughly circular tower range, that means that, at best, the government was able to determine where Davis was within approximately 14,589,696 square feet. [FN7] In an urban environment, this is not precise enough to rival the invasion of privacy that pinpoint-longer-term surveillance represents.

> FN7. A one-mile radius (5,280 feet), squared (27,878,400), times II, equals 87,538,176 square feet, divided by six (one sector), equals 14,589,696 square feet.

Since no specific historical privacy interest is implicated by cell-site location information, and further, because the privacy interest in the cell-site location information at issue here is materially indistinguishable from the privacy interest in the pen-register information at stake in *Smith,* [FN8] we must apply the third-party doctrine, as the Supreme Court did in *Smith.* I read *Smith,* in turn, as implicitly finding no historical privacy interest implicated by information provided to the telephone company to allow a call to be made, other than the general third-party doctrine.[FN9] Because no specific

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

historical privacy interest is implicated by pen-register-type information,***532** the more general historical privacy expectation associated with the third-party doctrine governed in *Smith.* The same is true with respect to the cell-site location information at issue in this case.

FN8. I respect the Dissent's thought process in attempting to distinguish the concept of whether cell-phone users know that they are disclosing to their service providers the fact that they are usually located in the range of the nearest cell towers that their cell phones are using when they make and receive calls, from the Supreme Court's conclusion in *Smith* that standard telephone users know that they are disclosing the telephone numbers that they are calling when they dial. But it seems to me that the average cell-phone user knows that cell phones work only when they are within service range of a cell tower. Advertising campaigns are built on this concept. *See, e.g.,* https:// www. youtube. com/ watch? v= OPw Po– IAQ– E (last visited Apr. 13, 2015) ("Can you hear me now?"); https:// www. youtube. com/ watch? v= VZPj JI 0 K 7 Bk (last visited Apr. 13, 2015) ("There's a map for that"). In *Smith,* similar to the Dissent here, Justice Marshall argued that the third-party doctrine did not apply, in part, because people do not " 'typically know' that a phone company monitors call [ ] [information] for internal reasons." 442 U.S. at 748–49, 99 S.Ct. at 2584–85. Right or wrong, he lost that battle. And, while cell-site location information is certainly not pen-register information and I can understand where the Dissent is coming from, I do not feel comfortable taking the position that the average cell-phone user does not know that he or she is disclosing location information to the cell-service provider.

FN9. This makes sense, as the privacy interest in discreet routing information is the same as the privacy interest in address information on letters, which, in turn, has always been subject to the third-party doctrine. *See supra* at n. 5.

III.

Nevertheless, where, as here, no historical privacy interest exists in the information sought, Congress always has the option of legislating higher standards for the government to obtain information. Justice Alito has opined, "In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative." *Jones,* 132 S.Ct. at 964 (Alito, J., concurring in the judgment). This is certainly one potential limitation on the third-party doctrine. And we have seen Congress enact legislation in response to the application of the third-party doctrine to our modern world. *See, e.g.,* the Right to Financial Privacy Act, 12 U.S.C. § 2701, *et seq.*[FN10] Indeed, the Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510, *et seq.,* of which the Stored Communications Act, 18 U.S.C. §§ 2701–2712, is a part—the statute under which the government obtained the order authorizing it to receive Davis's historical cell-site location information in this case—was enacted (and later amended), in part, to protect what Congress recognized as "privacy interests in personal and proprietary information" that travels and is maintained in electronic form by third-party service providers. *See* H.R.Rep. No. 99–541 at § I (1986).

FN10. *See* H.R.Rep. No. 95–1383 at 9306 (1978), 1978 U.S.C.C.A.N. 9273, 9306 ("The Title is a congressional response to the Supreme Court decision in the *United States v. Miller....* The Court did not acknowledge the sensitive nature of [financial records], and instead decided that since the records are the 'property' of the financial institution, the customer has no constitutionally recognizable privacy interest in them.").

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

But legislation should fill only the gaps that occur when no historically recognized privacy interest is implicated by the technology under review. The legislature, after all, does not have the power to entirely redefine the protections of the Fourth Amendment each time that it enacts a new law. While providing more protection than the Fourth Amendment requires represents a choice that Congress may, within its power, make, providing less is not a constitutional option. If it were, the Fourth Amendment would be meaningless because it would simply be whatever Congress said it was at any given time.

That cannot be right under our Constitution. So Congress's ability to legislate reasonable expectations of privacy (other than when Congress elects to increase expectations above the Fourth Amendment baseline) must be limited to, at most, only those circumstances where no historical privacy interest implicated by the technology under review exists.

IV.

For all of these reasons, I believe that *Smith* (and therefore, the third-party doctrine) inescapably governs the outcome of this case. But when we must necessarily expose information to third-party technological service providers in order to make use of everyday technology, and the technological service merely allows us to engage in an activity that historically enjoyed a constitutionally protected privacy interest, Supreme Court precedent can be viewed as supporting the notion that the historically protected privacy interest must trump the third-party doctrine for purposes of Fourth Amendment analysis. If the historically protected privacy interest does not, then with every new technology, we surrender more and more of our historically***533** protected Fourth Amendment interests to unreasonable searches and seizures.

MARTIN, Circuit Judge, dissenting,[FN1] in which JILL PRYOR, Circuit Judge, joins:

FN1. The *en banc* court voted to vacate the panel opinion which held that the warrantless search of Mr. Davis's cell site location data was unconstitutional, but upheld Mr. Davis's conviction based on the good-faith exception. The good-faith exception says that where officers' conduct is based on their good-faith understanding of an existing statute, the exclusionary rule will not apply. *See, e.g., United States v. Williams,* 622 F.2d 830, 843 (5th Cir.1980); *see also Bonner v. City of Prichard,* 661 F.2d 1206, 1209 (11th Cir.1981) (en banc) (adopting as binding precedent all decisions of the former Fifth Circuit handed down before October 1, 1981). The majority here refers to the good-faith exception as an alternative basis for affirming Mr. Davis's conviction. Maj. Op. 518 n. 20. I agree with them about that. My disagreement is with the majority's Fourth Amendment analysis, which permits government access to Mr. Davis's cell site location data without a warrant. I understand the Fourth Amendment to require the government to get a warrant for that information, while the majority does not. I refer to this opinion as a dissent, not a concurrence in the judgment, for that reason.

In this case, the government got 67 days of cell site location data disclosing Quartavious Davis's location every time he made or received a call on his cell phone. It got all this without obtaining a warrant. During that time, Mr. Davis made or received 5,803 phone calls, so the prosecution had 11,606 data points about Mr. Davis's location. We are asked to decide whether the government's actions violated Mr. Davis's Fourth Amendment rights. The majority says our analysis is dictated by the third-party doctrine, a rule the Supreme Court developed almost forty years ago in the context of bank records and telephone numbers. But such an expansive application of the third-party doctrine would allow the government warrantless access not only to where we are at any given time, but also to whom we send e-mails, our search-engine histories,

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

our online dating and shopping records, and by logical extension, our entire online personas.

Decades ago, the Supreme Court observed that "[i]f times have changed, reducing everyman's scope to do as he pleases in an urban and industrial world, ... the values served by the Fourth Amendment [are] more, not less, important." *Coolidge v. New Hampshire,* 403 U.S. 443, 455, 91 S.Ct. 2022, 2032, 29 L.Ed.2d 564 (1971). This is even truer today. The judiciary must not allow the ubiquity of technology—which threatens to cause greater and greater intrusions into our private lives—to erode our constitutional protections. With that in mind, and given the striking scope of the search in this case, I would hold that the Fourth Amendment requires the government to get a warrant before accessing 67 days of the near-constant cell site location data transmitted from Mr. Davis's phone. I respectfully dissent.

I.

I turn first to the third-party doctrine, which the majority believes decides this case for us. They say: "Davis can assert neither ownership nor possession of the third-party's business records he sought to suppress." Maj. Op. 511; *see also* William Pryor Concurrence 45 (" *Smith* controls this appeal."). My reading of Supreme Court precedent suggests that things are not so simple.

The Supreme Court announced the third-party doctrine nearly forty years ago in *United States v. Miller,* 425 U.S. 435, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976). The Court said that "the Fourth Amendment does not prohibit the obtaining of information***534** 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 and the confidence placed in the third party will not be betrayed." *Id.* at 443, 96 S.Ct. at 1624. Three years later, in *Smith v. Maryland,* 442 U.S. 735, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979), the Court applied that doctrine to hold that a defendant did not have a reasonable expectation of privacy in the numbers he dialed on his home telephone, recorded by means of a pen register at a telephone company's central office. *Id.* at 742, 99 S.Ct. at 2581. The Court reasoned that "[w]hen he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business." *Id.* at 744, 99 S.Ct. at 2582. The Court reminisced that "[t]he switching equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber." *Id.* The government believes that *Smith* controls the outcome of this case, and the majority apparently agrees. I do not.

First, the phone numbers a person dials are readily distinguishable from cell site location data. *Smith* involved "voluntarily conveyed numerical information"—voluntary because phone dialers have to affirmatively enter the telephone number they are dialing in order to place a call. By contrast, cell phone users do not affirmatively enter their location in order to make a call. Beyond that, the ACLU informs us that "[p]hones communicate with the wireless network when a subscriber makes *or receives* calls." ACLU Amicus Br. 5 (emphasis added). As our sister Circuit observed, "when a cell phone user *receives* a call, he hasn't voluntarily exposed anything at all." *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't,* 620 F.3d 304, 317–18 (3d Cir.2010) (*Third Circuit Case*) (emphasis added) (quotation marks omitted).[FN2]

FN2. The majority extensively recounts the Fifth Circuit's decision in *In re Application of the U.S. for Historical Cell Site Data,* 724 F.3d 600 (5th Cir.2013), which said that a "cell user ha[s] no subjective expectation of privacy in such business records showing cell tower locations." Maj. Op. 510. That Fifth Circuit case, of course, does not bind us. And in any event, other courts have held that people *do* have a reasonable expectation of privacy in cell

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

site location data, whether historical or real-time in nature. The *Third Circuit Case* , for example, rejected the government's argument that "no [cell site location data] can implicate constitutional protections because the subscriber has shared its information with a third party...." 620 F.3d at 317. Similarly, the Florida Supreme Court has held that cell phone users have a reasonable expectation of privacy in real-time cell site location data. *Tracey v. State,* 152 So.3d 504, 526 (Fla.2014). And a recent decision from the Northern District of California addressed the very same question we address here and held that a person has a reasonable expectation of privacy in 60 days of historical cell site location data. *United States v. Cooper,* No. 13–cr–00693–SI–1, 2015 WL 881578, at *6–8 (N.D.Cal. Mar. 2, 2015). In short, we are faced with persuasive, albeit not binding, authority on both sides of the debate, but none controls the outcome of this case.

The *Smith* Court also emphasized that the numbers a person dials appear on the person's telephone bill and referenced the pre-automation process that required the caller to recite phone numbers out loud to a phone operator in order to make a call. Thus, the Court concluded that "[t]elephone users ... typically *know* that they must convey numerical information to the phone company." *Smith,* 442 U.S. at 743, 99 S.Ct. at 2581 (emphasis added). There is not the same sort of "knowing" disclosure of cell site location data to phone companies because there is no history of ***535** cell phone users having to affirmatively disclose their location to an operator in order to make a call. The extent of voluntariness of disclosure by a user is simply lower for cell site location data than for the telephone numbers a person dials. For that reason, I don't think *Smith* controls this case.

Second, although the *Miller/Smith* rule appears on its own to allow government access to *all* information that *any* third-party obtains, in rulings both before and since those cases, the Supreme Court has given reasons to doubt the rule's breadth. For instance, in *Ferguson v. City of Charleston,* 532 U.S. 67, 121 S.Ct. 1281, 149 L.Ed.2d 205 (2001), the Court stated that "[t]he reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent." *Id.* at 78, 121 S.Ct. at 1288. Though the majority did not mention the third-party doctrine, Justice Scalia noted the incongruity between that doctrine and the *Ferguson* holding in his dissent. As he stated:

> Until today, we have *never* held—or even suggested—that material which a person voluntarily entrusts to someone else cannot be given by that person to the police, and used for whatever evidence it may contain. Without so much as discussing the point, the Court today opens a hole in our Fourth Amendment jurisprudence, the size and shape of which is entirely indeterminate.

Id. at 95–96, 121 S.Ct. at 1297–98 (Scalia, J., dissenting). Further, and again without mentioning the third-party doctrine, the Court has routinely recognized that people retain a reasonable expectation of privacy in things that they have arguably exposed to third parties. *See, e.g., United States v. Jacobsen,* 466 U.S. 109, 114, 104 S.Ct. 1652, 1657, 80 L.Ed.2d 85 (1984) (holding that "[l]etters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy" even though they touch the hands of third-party mail carriers); *Stoner v. California,* 376 U.S. 483, 487–88, 490, 84 S.Ct. 889, 892, 893, 11 L.Ed.2d 856 (1964) (finding unpersuasive the argument that "the search of [a] hotel room, although conducted without the petitioner's consent, was lawful because it was conducted with the consent of the hotel clerk," because a hotel guest's constitutional protections should not be "left to depend on the unfettered discretion of an employee of the hotel"); *see also Smith,* 442 U.S. at

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

746–47, 99 S.Ct. at 2583 (Stewart, J., dissenting) (noting that in *Katz v. United States,* 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967), the Court held that a person has a reasonable expectation of privacy in the contents of phone conversations made in telephone booths even though calls "may be recorded or overheard by the use of other company equipment"). I am well aware that each of these cases can be distinguished from Mr. Davis's case. I mean only to say that a comprehensive review of Supreme Court precedent reveals that the third-party doctrine may not be as all-encompassing as the majority seems to believe.

Third and most importantly, the majority's blunt application of the third-party doctrine threatens to allow the government access to a staggering amount of information that surely must be protected under the Fourth Amendment. Consider the information that Google gets from users of its e-mail and online search functions.[FN3] ***536** According to its website, Google collects information about you (name, e-mail address, telephone number, and credit card data); the things you do online (what videos you watch, what websites you access, and how you view and interact with advertisements); the devices you use (which particular phone or computer you are searching on); and your actual location. *See* Privacy Policy, http:// www. google. com/ intl/ en/ policies/ privacy/ (last accessed March 30, 2015). Beyond that, in its "Terms of Service," Google specifies that "[w]hen you upload, submit, store, send or receive content to or through our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works, ... communicate, publish, publicly perform, publicly display and distribute such content." *See* Google Terms of Service, http:// www. google. com/ intl/ en/ policies/ terms/ (last accessed March 30, 2015). Like in *Miller* and *Smith,* Google even offers a legitimate business purpose for such data storage and mining: "Our automated systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection." *Id.* Under a plain reading of the majority's rule, by allowing a third-party company access to our e-mail accounts, the websites we visit, and our search-engine history—all for legitimate business purposes—we give up any privacy interest in that information.

FN3. I refer to Google only as an example. The same analysis applies to most other online search engine or e-mail service providers.

And why stop there? Nearly every website collects information about what we do when we visit. So now, under the majority's rule, the Fourth Amendment allows the government to know from YouTube.com what we watch, or Facebook.com what we post or whom we "friend," or Amazon.com what we buy, or Wikipedia.com what we research, or Match.com whom we date—all without a warrant. In fact, the government could ask "cloud"-based file-sharing services like Dropbox or Apple's iCloud for all the files we relinquish to their servers. I am convinced that most internet users would be shocked by this. But as far as I can tell, every argument the government makes in its brief regarding cell site location data applies equally well to e-mail accounts, search-engine histories, shopping-site purchases, cloud-storage files, and the like. *See, e.g.,* Appellee's Br. 21–22 ("Davis can assert neither ownership nor possession of the third-party records he sought to suppress."); *id.* at 22 ("Evidence lawfully in the possession of a third party is not *his,* even if it has to do with *him.*"); *id.* at 23 ("Davis is not in a good position to complain that the government improperly obtained 'his location data,' since he himself exposed and revealed to MetroPCS the very information he now seeks to keep private."); *id.* at 24 ("It is not persuasive to argue that phone users do not knowingly or intentionally disclose any location-related information to their service providers."); *id.* at 25 ("For purposes of the Fourth Amendment, it makes no difference whether Davis knew that MetroPCS was collecting

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

location-related information."); *id.* at 27–28 ("[S]ervice contracts and privacy policies typically warn cell-phone customers that phone companies collect location-related information and may disclose such data to law-enforcement authorities.").

The enormous impact of this outcome is probably why at least one Circuit has held that a person's Fourth Amendment rights are violated when the government compels an internet service provider to turn over the contents of e-mails without a warrant. *See United States v. Warshak* 631 F.3d 266, 286–88 (6th Cir.2010). Surely the majority would agree and would also shield e-***537** mails from government snooping absent a warrant. But if e-mails are protected despite the fact that we have surrendered control of them to a third party, then the rule from *Smith* and *Miller* has its limits.

The majority suggests that e-mails can be distinguished because cell site location data is "non-content evidence." Maj. Op. 511 (emphasis omitted). The majority offers no coherent definition of the terms "content" and "non-content," and I am hard-pressed to come up with one. For instance, would a person's Google search history be content or non-content information? Though a person's search terms may seem like "content," a search term exists in the web address generated by a search engine.[FN4] And web addresses, like phone numbers, seem like quintessentially non-content information that merely direct a communication. But regardless, although this content-non-content distinction could—maybe—shield the body of e-mail messages, the government may presumably still access the time and date that we send e-mails, the names of the people who receive them, and the names of the people who email us, without a warrant. Likewise, although our actual activities on a dating or shopping website might be protected, the fact that we visited those websites or any other would still be freely discoverable. The government agreed at oral argument that under its theory, it could at the very least obtain records like the sender and receiver of e-mails, the time of day e-mails are sent, the number of e-mails a person sends, the websites that a person visits, and maybe even the connections a person communicates with on a dating website and whom she meets in person—all without a warrant.

FN4. For example, a search of "Eleventh Circuit" on google.com produces the web address: " https:// www. google. com/? gws_ rd= ssl # q= eleventh+ circuit."

This slippery slope that would result from a wooden application of the third-party doctrine is a perfect example of why the Supreme Court has insisted that technological change sometimes requires us to consider the scope of decades-old Fourth Amendment rules. *See Kyllo v. United States,* 533 U.S. 27, 35, 121 S.Ct. 2038, 2044, 150 L.Ed.2d 94 (2001) (rejecting a "mechanical interpretation of the Fourth Amendment" in the face of "advancing technology"); *cf. Katz,* 389 U.S. at 353, 88 S.Ct. at 512 ("To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication."). For instance, in *Riley v. California,* 573 U.S. ——, 134 S.Ct. 2473, 189 L.Ed.2d 430 (2014), the Court was asked to decide whether the decades-old search-incident-to-arrest exception to the warrant requirement applied to cell phones on an arrestee's person. *Id.* at 2480. California argued that the Court's 41–year–old decision in *United States v. Robinson,* 414 U.S. 218, 94 S.Ct. 467, 38 L.Ed.2d 427 (1973), controlled the outcome in *Riley* because the Court held that a search of objects on an arrestee's person was categorically reasonable. *See Riley,* 134 S.Ct. at 2491. The *Riley* Court agreed that "a mechanical application of *Robinson* might well support the warrantless searches at issue." *Id.* at 2484. But it nonetheless unanimously rejected that argument, saying that cell "phones are based on technology nearly inconceivable just a few decades ago, when ... *Robinson* w[as] decided." *Id.* Thus, to say that a search of cell phone data is "materially indistinguishable" from a search of physical items

is like saying a ride on horseback is materially in-

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

distinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together. Modern***538** cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse.

Id. at 2488–89.

Likewise here, the extent of information that we expose to third parties has increased by orders of magnitude since the Supreme Court decided *Miller* and *Smith.* Those forty years have seen not just the proliferation of cell phones that can be tracked, but also the advent of the internet. Given these extraordinary technological advances, I believe the Supreme Court requires us to critically evaluate how far to extend the third-party doctrine. As Justice Sotomayor observed:

[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.... I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.

United States v. Jones, 565 U.S. ——, ——, 132 S.Ct. 945, 957, 181 L.Ed.2d 911 (2012) (Sotomayor, J., concurring) (citations omitted). Neither would I assume as much. Though the doctrine may allow the government access to some information that we disclose to third parties, I would draw the line short of the search at issue here. Sixty-seven days of near-constant location tracking of a cell phone—a technological feat impossible to imagine when *Miller* and *Smith* were decided—is an application of the doctrine that goes too far.

II.

Because I believe that the third-party doctrine does not dictate the outcome of this case, I turn to fundamental Fourth Amendment principles. The Fourth Amendment says:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV. "As the text makes clear, the ultimate touchstone of the Fourth Amendment is reasonableness." *Riley,* 134 S.Ct. at 2482 (quotation marks omitted). Our analysis is two-fold: "First, we ask whether the individual, by his conduct, has exhibited an actual expectation of privacy; that is, whether he has shown that he sought to preserve something as private." *Bond v. United States,* 529 U.S. 334, 338, 120 S.Ct. 1462, 1465, 146 L.Ed.2d 365 (2000) (quotation omitted) (alteration adopted). "Second, we inquire whether the individual's expectation of privacy is one that society is prepared to recognize as reasonable." *Id.* (quotation omitted). If we conclude that a particular search violates a defendant's reasonable expectation of privacy, the government must get a search warrant.

For me, the answer to the subjective inquiry is easy. It seems obvious that Mr. Davis never intended to disclose his location to the government every time he made or received calls. Recent polling data tells us that 82% of adults "feel as though the details of their physical location gathered over a period of time" is "very sensitive" or "somewhat sensitive." Mary Madden, Public Perceptions of Privacy and Security in the Post–Snowden Era 34, Pew ***539** Research Center (Nov. 12, 2014), http:// www. pewinternet. org/ files/ 2014/ 11/ PI_ Public Percept ionsof Privacy_ 1112 14.pdf. This supports the common-sense notion that people do not expect the government to track them simply as a consequence of owning and using what amounts to a basic necessity of twenty-first century life—the cell phone.[FN5] Beyond that, the prosecutor in this case

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

specifically admitted at closing argument that "what this defendant *could not have known* was that ... his cell phone was tracking his every moment." Trial Tr. 4–5, Feb. 8, 2012, ECF No. 287 (emphasis added); *see also id.* at 14 (arguing that Mr. Davis and his co-conspirators "had no idea that by bringing their cell phones with them to these robberies they were allowing MetroPCS and now [the jury] to follow their movements"). In short, I believe that Mr. Davis—like any other person interacting in today's digital world—quite reasonably had a subjective expectation that his movements about town would be kept private.[FN6]

FN5. The government argues that regardless of what people think, "MetroPCS's current privacy policy ... advises its wireless customers that the company 'may disclose, without your consent, the approximate location of a wireless device to a governmental entity or law enforcement authority when we are served with lawful process.' " Appellee Br. 28 (citation omitted). But as another court recently noted, "[t]he fiction that the vast majority of the American population consents to warrantless government access to the records of a significant share of their movements by 'choosing' to carry a cell phone must be rejected." *In re Application of the U.S. for an Order Authorizing the Release of Historical Cell–Site Info.,* 809 F.Supp.2d 113, 127 (E.D.N.Y.2011). Regardless, and as the majority acknowledges, the "contract does not appear on this record to have been entered into evidence here," so "we cannot consider it." Maj. Op. 510 n. 11.

FN6. The majority does not explain why it believes that "the fact that Davis registered his cell phone under a fictitious alias tends to demonstrate his understanding that such cell tower location information is collected by MetroPCS and may be used to incriminate him." Maj. Op. 511. Mr. Davis's use of an alias more naturally evidences his desire not to tie his identity to his phone's account with MetroPCS. For me, Mr. Davis's use of an alias says nothing about his subjective expectation of privacy in his location.

The more important and more difficult question we must consider is whether Mr. Davis's expectation of privacy is one society is objectively prepared to recognize as reasonable. I believe the answer is yes. The Supreme Court recently reminded us that "there is an element of pervasiveness that characterizes cell phones." *Riley,* 134 S.Ct. at 2490. Today, "it is the person who is not carrying a cell phone ... who is the exception." *Id.* The Court noted that "nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower." *Id.* (quoting Harris Interactive, 2013 Mobile Consumer Habits Study (June 2013)). In other words, "modern cell phones ... are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Id.* at 2484; *see also City of Ontario, Cal. v. Quon,* 560 U.S. 746, 760, 130 S.Ct. 2619, 2630, 177 L.Ed.2d 216 (2010) ("Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification.").

Since we constantly carry our cell phones, and since they can be used to track our movements, the recent opinions of five Justices in *United States v. Jones* that long-term location-monitoring generally violates expectations of privacy are instructive. In *Jones,* the Supreme Court ***540** considered whether warrantless monitoring of the location of a person's car for twenty-eight days by means of a GPS tracker violated the defendant's rights under the Fourth Amendment. 132 S.Ct. at 948–49. All nine Justices said yes. Five Justices held that such tracking violated the Fourth Amendment under a trespass theory

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

that considered the government's physical intrusion of the car. *Id.* at 949. Important for Mr. Davis's case, however, a different set of five Justices were in agreement that "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." *Id.* at 955 (Sotomayor, J., concurring) (quoting *id.* at 964 (Alito, J., joined by Ginsburg, Breyer, and Kagan, JJ., concurring in the judgment)). Said one Justice, "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *Id.* at 955 (Sotomayor, J., concurring). Said four other Justices, "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period." *Id.* at 964 (Alito, J., concurring in the judgment).[FN7]

FN7. The majority chides Mr. Davis for "deploy[ing] the concurrences in *Jones,* " Maj. Op. 514, but a lower federal court ignores the opinion of five Justices of the Supreme Court at its own risk.

The search at issue here similarly impinged on expectations of privacy. The location data the government collected, though not quite as precise as the GPS data in *Jones,* still revealed Mr. Davis's comings and goings around Miami with an unnerving level of specificity. Each time he made or received a call, MetroPCS catalogued the cell tower to which his cell phone connected, typically the "[n]earest and strongest" tower. Trial Tr. 221, Feb. 6, 2012, ECF No. 283. In a "cosmopolitan area [like] Miami," there are "many, many towers" whose coverage radii are "much smaller" than a "mile-and-a-half." *Id.* at 222–23. Each coverage circle is further subdivided into "three or six portions." *Id.* at 222. The data the government obtained in this case specified the sector within a tower's coverage radius in which Mr. Davis made or received a call.

The amount of data the government got is also alarming. The government demanded from MetroPCS sixty-seven days of cell site location data—more than double the time at issue in *Jones.* In total, this data included 5,803 separate call records. Since MetroPCS cataloged the cell tower sector where each phone call started *and* ended, the government had 11,606 cell site location data points. This averages around one location data point every *five and one half minutes* for those sixty-seven days, assuming Mr. Davis slept eight hours a night.

The amount and type of data at issue revealed so much information about Mr. Davis's day-to-day life that most of us would consider quintessentially private. For instance, on August 13, 2010, Mr. Davis made or received 108 calls in 22 unique cell site sectors, showing his movements throughout Miami during that day. And the record reflects that many phone calls began within one cell site sector and ended in another, exposing his movements even during the course of a single phone call.

Also, by focusing on the first and last calls in a day, law enforcement could determine from the location data where Mr. Davis lived, where he slept, and whether those two locations were the same. As a ***541** government witness testified at trial, "if you look at the majority of ... calls over a period of time when somebody wakes up and when somebody goes to sleep, normally it is fairly simple to decipher where their home tower would be." Trial Tr. 42, Feb. 7, 2012, ECF No. 285. For example, from August 2, 2010, to August 31, 2010, Mr. Davis's first and last call of the day were either or both placed from a single sector—purportedly his home sector. But on the night of September 2, 2010, Mr. Davis made calls at 11:41pm, 6:52am, and 10:56am—all from a location that was not his home sector. Just as Justice Sotomayor warned, Mr. Davis's "movements [were] recorded and aggregated in a manner that enable[d] the Government to ascertain, more or less at will, ... [his] sexual habits, and so on." *Jones,* 132 S.Ct. at 956 (Sotomayor, J., con-

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

curring); *see also United States v. Maynard,* 615 F.3d 544, 562 (D.C.Cir.2010) ("A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts.").

Importantly, the specificity of the information that the government obtained was highlighted by the way the government used it at trial. The government relied upon the information it got from MetroPCS to specifically pin Mr. Davis's location at a particular site in Miami. *See, e.g.,* Trial Tr. 58, Feb. 7, 2012, ECF No. 285 (noting that "Mr. Davis's phone [was] literally right up against the America Gas Station immediately preceding and after [the] robbery occurred"); *id.* at 61 (noting "the presence of his cell phone literally ... right next door to the Walgreen's just before and just after that store was robbed"). On this record, Mr. Davis had a reasonable expectation of privacy in the cell site location data the government obtained, and his expectation was one that society should consider reasonable. I would therefore hold that absent a warrant, a Fourth Amendment violation occurred.

III.

The majority, of course, believes that Mr. Davis had no reasonable expectation of privacy in the cell site location data obtained in his case. It emphasizes the large size of the sectors that each location data point revealed as evidence that the privacy intrusion was not so great. *See* Maj. Op. 501–02, 503–04. It also says we need not consider more invasive technologies that have developed since the search that took place here. *Id.* at 504 n. 7 ("There is no evidence, or even any allegation, that the MetroPCS network reflected in the records included anything other than traditional cell towers and the facts of this case do not require, or warrant, speculation as to the newer technology."). Yet the Supreme Court has cautioned us that "[w]hile the technology used in the present case [may be] relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development." *Kyllo,* 533 U.S. at 36, 121 S.Ct. at 2044. Just as the majority appropriates decades-old precedent from *Miller* and *Smith* and applies it to new technologies, the rule we make today necessarily will apply to everyone else's case going forward.

That future impact is troubling. As technology advances, the specificity of cell site location information has increased. Cell phone companies are constantly upgrading their networks with more and more towers. As the ACLU explains:

> ***542** Cell site density is increasing rapidly, largely as a result of the growth of internet usage by smartphones.... As new cell sites are erected, the coverage areas around existing nearby cell sites will be reduced, so that the signals sent by those sites do not interfere with each other. In addition to erecting new conventional cell sites, providers are also increasing their network coverage using low-power small cells, called "microcells," "picocells," and "femtocells" (collectively, "femtocells"), which provide service to areas as small as ten meters.... Because the coverage area of femtocells is so small, callers connecting to a carrier's network via femtocells can be located to a high degree of precision, sometimes effectively identifying individual floors and rooms within buildings.

ACLU Amicus Br. 7–8 (quotations, citations omitted); *see also id.* at 7 (noting that "the number of cell sites in the United States has approximately doubled in the last decade"); *id.* at 8 (noting that "[f]emtocells with ranges extending outside of the building in which they are located can also provide cell connections to passersby, providing highly precise information about location and movement on public streets and sidewalks"). The location features on smartphones are even more precise. *See Riley,* 134 S.Ct. at 2490 ("Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

down to the minute, not only around town but also within a particular building.").

Beyond that, today, the vast majority of communications from cell phones are in the form of text messages and data transfers, not phone calls. The frequency of text messaging is much greater than the frequency of phone calling—particularly among young cell phone users. *See* Amanda Lenhart, Teens, Smartphones & Texting (available at http://www.pew internet.org/2012/03/19/teens-smartphones-texting/) (finding that the median number of texts sent per day by teens ages 12 to 17 rose from 50 in 2009 to 60 in 2011). Also, "smartphones, which are now used by more than six in ten Americans, communicate even more frequently with the carrier's network, because they typically check for new email messages or other data every few minutes." ACLU Amicus Br. 5 (citations omitted). Each of these new types of communications can generate cell site location data. *See, e.g., United States v. Cooper,* No. 13–cr–00693–SI–1, 2015 WL 881578, at *8 n. 6 (N.D.Cal. Mar. 2, 2015) (noting the government's admission that "cell site data is recorded for both calls and text messages").

Finally, not only are cell sites fast growing in number, but the typical user has no idea how precise cell site location data is at any given location. As a person walks around town, particularly a dense, urban environment, her cell phone continuously and without notice to her connects with towers, antennas, microcells, and femtocells that reveal her location information with differing levels of precision—to the nearest mile, or the nearest block, or the nearest foot. And since a text or phone call could come in at any second—without any affirmative act by a cell phone user—a user has no control over the extent of location information she reveals.

The government tells us these technological advances do not change our analysis. At oral argument, it admitted that its theory requires us to hold that it could obtain location data without a warrant even when technology someday allows it to know a person's location to within six inches, and when tracking is continuous and does not require making or receiving a phone call. I reject a theory that allows the government such expansive access to ***543** information about where we are located, no matter how detailed a picture of our movements the government may receive.

But we need not fear the threat of increasing precision of location information, says the majority. At the same time it suggests that today's ruling might not apply to future technology, however, the majority's opinion offers absolutely no guidance to the judges who authorize searches of cell site location data and the officers who conduct them. As the ACLU pointed out, "[a]gents will not have prior knowledge of whether the surveillance target was in a rural area with sparse cell sites, an urban area with dense cell sites or six-sector antennas, or a home, doctor's office, or church with femtocells." ACLU Amicus Br. 9. Thus, a judge will authorize a search of a person's cell site location data for a certain period of time without knowing how precise the location information will be. While I admire the majority's attempt to cabin its holding to the technology of five years ago, its assurances in this regard seem naïve in practice. As a result of today's decision, I have little doubt that all government requests for cell site location data will be approved, no matter how specific or invasive the technology.

IV.

The majority offers dire warnings of the consequences of restricting the government's access to cell site location data, suggesting that without it, all manner of horrific crimes—from child abductions to terrorism—would go uninvestigated. *See* Maj. Op. 517. But if my view of the Fourth Amendment were to prevail, all the officers in this case had to do was get a warrant for this search. That is no great burden. "Under the Fourth Amendment, an officer may not properly issue a warrant ... unless he can find probable cause therefor from facts or circumstances presented to him under oath or af-

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

firmation." *Nathanson v. United States,* 290 U.S. 41, 47, 54 S.Ct. 11, 13, 78 L.Ed. 159 (1933). The probable-cause standard is not onerous. *See Illinois v. Gates,* 462 U.S. 213, 291, 103 S.Ct. 2317, 2360, 76 L.Ed.2d 527 (1983) (Brennan, J., dissenting) (criticizing a probable-cause standard that "imposes no structure on magistrates' probable cause inquiries ... and invites the possibility that intrusions may be justified on less than reliable information from an honest or credible person"); Ricardo J. Bascuas, *Property and Probable Cause: The Fourth Amendment's Principled Protection of Privacy,* 60 Rutgers L.Rev. 575, 592–93 (2008) ("The Supreme Court has set the standard for the quality of information that can support a warrant so low that judges can hardly be expected to uncover a baseless request."); *cf. Riley,* 134 S.Ct. at 2493 (noting that "[r]ecent technological advances ... have ... made the process of obtaining a warrant itself more efficient"). Nor is cell site data the type of information which would spoil or perish during the short time it takes to get a warrant. Finally, requiring a warrant would not do away with the other well-established exceptions to the warrant requirement, like exigent circumstances. *Cf. Riley,* 134 S.Ct. at 2494 (noting that "the availability of the exigent circumstances exception ... address[es] some of the more extreme hypotheticals that have been suggested"). Imposing the requirement for a warrant under these circumstances would hardly shackle law enforcement from conducting effective investigations.

But regardless of how easy it might be to get warrants, the Supreme Court has reminded us time and again of how important they are.

> The warrant requirement has been a valued part of our constitutional law for decades, and it has determined the result***544** in scores and scores of cases in courts all over this country. It is not an inconvenience to be somehow 'weighed' against the claims of police efficiency. It is, or should be, an important working part of our machinery of government, operating as a matter of course to check the 'well-intentioned but mistakenly overzealous, executive officers' who are a part of any system of law enforcement.

Coolidge, 403 U.S. at 481, 91 S.Ct. at 2046 (citation omitted). The majority emphasizes that the Stored Communications Act (SCA) requires the government to "offer[ ] specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). But it does not contest—nor could it—that this standard falls below the probable-cause standard that courts usually demand. *See* Maj. Op. 505.[FN8]

> FN8. Certainly the Stored Communications Act is better than nothing. *See* Maj. Op. 505 (noting that the SCA "raises the bar from an ordinary subpoena to one with additional privacy protections built in"). But the mere fact that the Act provides some judicial oversight before the government can get cell site location data does not answer the question whether the government is constitutionally required to have a warrant.

Once again, the Supreme Court's analysis in *Riley* is instructive. [FN9] There, the Court recognized:

> FN9. "[T]here is dicta and then there is dicta, and then there is Supreme Court dicta." *Schwab v. Crosby,* 451 F.3d 1308, 1325 (11th Cir.2006).

> We cannot deny that our decision today will have an impact on the ability of law enforcement to combat crime. Cell phones have become important tools in facilitating coordination and communication among members of criminal enterprises, and can provide valuable incriminating information about dangerous criminals. Privacy comes at a cost.

Riley, 134 S.Ct. at 2493. But still, the Court insisted that law enforcement officers get a warrant

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

before searching a cell phone incident to arrest. So too here. I would simply require the government do what it has done for decades when it seeks to intrude upon a reasonable expectation of privacy. That is, "get a warrant." *Id.* at 2495.

V.

The majority proclaims that its holding today is "narrow[ ]," Maj. Op. 505, limited only to cell site location data, and only to the kind of data the government could obtain in 2010. But "[s]teps innocently taken may one by one lead to the irretrievable impairment of substantial liberties." *Glasser v. United States,* 315 U.S. 60, 86, 62 S.Ct. 457, 472, 86 L.Ed. 680 (1942). Under the reasoning employed by the majority, the third-party doctrine may well permit the government access to our precise location at any moment, and in the end, our entire digital lives. And although Mr. Davis—as the majority reminds us in great detail, *see* Maj. Op. 500–01—has been convicted of very serious crimes and is not therefore the most sympathetic bearer of this message, [FN10] "the rule[s] we fashion [are] for the innocent and guilty alike." *Draper v. United States,* 358 U.S. 307, 314, 79 S.Ct. 329, 333, 3 L.Ed.2d 327 (1959) (Douglas, J., dissenting). I would not subject the citizenry to constant location tracking of their cell phones without requiring the government to get a warrant.***545** The Fourth Amendment compels this result. I respectfully dissent.

FN10. Though regardless of the outcome of this *en banc* appeal, Mr. Davis's convictions will stand and he will remain incarcerated due to the good-faith exception. *See supra* note 1.

C.A.11 (Fla.),2015.
U.S. v. Davis
785 F.3d 498, 62 Communications Reg. (P&F) 909, 25 Fla. L. Weekly Fed. C 1161

END OF DOCUMENT

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

STEVEN G. KALAR
Federal Public Defender
ELLEN V. LEONIDA
Assistant Federal Public Defender
555 - 12th Street, Suite 650
Oakland, CA 94607-3627
Telephone: (510) 637-3500
Fax: (510) 637-3507
Email: ellen_leonida@fd.org

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

IN RE TELEPHONE INFORMATION NEEDED FOR A CRIMINAL INVESTIGATION	CR 14-XR-90532 NC OPPOSITION TO GOVERNMENT'S APPLICATION, UNDER 18 U.S.C. § 2703(D), FOR CELL SITE LOCATION INFORMATION

TABLE OF CONTENTS

INTRODUCTION.....1

BACKGROUND.....1

DISCUSSION.....1

I. THE FOURTH AMENDMENT PROHIBITS WARRENTLESS SEARCH AND SEIZURE OF CSLI 5

A. CSLI Is Protected by the Fourth Amendment Right to Privacy.....5

B. This Court Should Follow the Eleventh Circuit Holding That Historical Cell Site Location Information Is Protected the Fourth Amendment.....8

C. *Riley v. California* Implicitly Recognizes a Privacy Interest in CSLI.....10

II. CELL PHONE SUBSCRIBERS DO NOT FORFEIT THEIR FOURTH AMENDMENT RIGHTS SIMPLY BECAUSE THEIR CSLI RECORDS ARE MAINTAINED BY THIRD-PARTY CELL PHONE COMPANIES.....12

A. An Individual Does Not Lose the Right to Privacy in CSLI Simply Because It Is Disclosed to a Cell Phone Provider.....12

B. CSLI Is Not Voluntarily Conveyed to a Third Party.....15

III. CSLI IS NOT A BUSINESS RECORD OF THE PROVIDER.....17

A. A Service Provider's Ability to Access CSLI Does Not Defeat the Subscriber's Reasonable Expectation of Privacy.....17

B. Service Providers Were Forced by the Government to Configure Their Networks to Generate CSLI for Law Enforcement Purposes.....19

IV. THE STORED COMMUNICATIONS ACT DID NOT CONTEMPLATE CSLI....21

V. THE SCA GIVES MAGISTRATES DISCRETION TO REQUIRE A WARRANT FOR CSLI.....25

VI. THE GOVERNMENT MAY OBTAIN CSLI WITH A WARRANT BASED ON PROBABLE CAUSE.....29

CONCLUSION.....30

TABLE OF AUTHORITIES

FEDERAL CASES

Almeida-Sanchez v. United States, 413 U.S. 266 (1973).....22

Beck v. Prupis, 529 U.S. 494 (2000)..... 27

Bond v. United States, 529 U.S. 334 (2000)..... 13

California v. Hodari D., 499 U.S. 621 (1991).....26

Clark v. Martinez, 543 U.S. 371 (2005).....28

Donaldson v. United States, 400 U.S. 517 (1971).....19

Ferguson v. City of Charleston, 532 U.S. 67 (2001).....13

In Matter of United States, ___ F. Supp. 2d ___, 2014 WL 1395082 (D. D.C. 2014).....15

In re Application, 724 F.3d 600 (5th Cir. 2013).....*passim*

In re United States, 441 F. Supp. 2d 816 (S.D. Tex. 2006).....22

In re United States, 2006 WL 1876847 (N.D. Ind. 2006).....15

In the Matter of an Application, 736 F. Supp. 2d 578 (E.D. N.Y. 2010).....15

In the Matter of an Application, 809 F. Supp. 2d 113 (E.D. N.Y. 2011)..... 15

In the Matter of the Application, 620 F.3d 304 (3d Cir. 2010).....*passim*

Katz v. United States, 389 U.S. 347 (1967).....5,6

Kyllo v. United States, 533 U.S. 27 (2001).....7,14

Martin v. Franklin Capital Corp., 546 U.S. 132 (2005).....26

Maryland v. King, 133 S. Ct. 1958, (2013).....17

POM Wonderful LLC v. Coca-Cola Co., 132 S. Ct. 2228 (2014).....25

Quon v. Arch Wireless Operating Co. Inc., 529 F.3d 892 (9th Cir. 2008),.....13

Reeb v. Thomas, 636 F.3d 1224 (9th Cir. 2011)..... 25

Riley v. California, 134 S. Ct. 2473 (2014).....*passim*

SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735 (1984).....19

Smith v. Maryland, 442 U.S. 735 (1979).....12

U.S. Telecommunication Association v. FCC, 227 F.3d 450 (D.C. Cir. 2000).....19, 20

United States v. Davis, ___ *F.3d* ___, 2014 WL 2599917 (11th Cir. 2014).....8

United States v. Forrester, 512 F.3d 500 (9th Cir. 2008).....16

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

United States v. Johnson, 457 U.S. 537 (1982).....29

United States v. Johnson, 680 F.3d 1140 (9th Cir. 2012).....5

United States v. Jones, 132 S. Ct. 945 (2012).....*passim*

United States v. Karo, 468 U.S. 705 (1984).....5,7

*United States v. Knotts,*460 U.S. 276 (1983).....5,14

United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010).....12

United States v. Miller, 425 U.S. 435 (1976).....12

United States v. Ressam, 679 F.3d 1069 (9th Cir. 2012).....26

United States v. Taketa, 923 F.2d 665 (9th Cir. 1991).....13

United States v. Williams, 659 F.3d 1223 (9th Cir. 2011).....25

United States v. X-Citement Videos, Inc., 513 U.S. 64 (1994).....28

DOCKETED CASES

American Civil Liberties Union of Northern California v. Department of Justice, No. 12-cv-4008.....4

FEDERAL STATUTES

18 U.S.C. § 1001 19

18 U.S.C. § 3123 27

47 U.S.C. § 1002 ..... 19, 22

OTHER FEDERAL AUTHORITIES

47 C.F.R. § 20.18(h) 24

Communications Assistance For Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) 20

Electronic Communications Privacy Act Reform and the Revolution in Location Based Technologies and Services, Hearing before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary, 111th Cong., 16 (2010) ..... *passim*

Electronic Communications Privacy Act (ECPA) (Part II): Geolocation Privacy and Surveillance, Hearing before the Subcomm. on Crime, Terrorism, Homeland Security, and Investigations, of the H. Comm. on the Judiciary, 113th Cong., 50 (2013) ..... *passim*

Fed. R. Crim. P. 41 ..... 28, 29

H.R. Rep. No. 103-827(I) at 9 (1994) 20

S. Rep. No. 99-541, at 1 (1986) 22

S. Rep. No. 99-541 at, e.g., 2, 4, 9, 10 22

MISCELLANEOUS

Aya Gruber, Garbage Pails and Puppy Dog Tails: Is That What Katz Is Made Of?, 41 13

Micah Sherr, et al., *Can They Hear Me Now? A Security Analysis of Law Enforcement Wiretaps*, Proc. 16th ACM Conf on Computer & Comms. Sec. 512, 514 (Nov. 2009) 20

Thomas A. O'Malley, *Using Historical Cell Site Analysis Evidence in Criminal Trials*, U.S. Att'y Bull., Nov. 2011 ..... 2, 4

INTRODUCTION

The Supreme Court recently, and aptly, noted that cell phones "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Riley v. California*, 134 S. Ct. 2473, 2484 (2014). In addition to acting as cameras, phone books, maps, and computers, cell phones automatically generate a record of when and where they are used – effectively documenting the locations of all cell phone users, everywhere they go, every time of day.

Over the years, the government has obtained the location information of millions of cell phone users from their phone companies, without showing probable cause or obtaining a warrant. However, courts are increasingly recognizing that individuals have a reasonable expectation of privacy in "all [cell phones] contain and all they may reveal," *id.* at 2494, including what they reveal about the user's location. Under established Fourth Amendment principles, the government may not infringe upon these reasonable expectations of privacy unless it first obtains a warrant based on probable cause. Because the government here seeks access to cell site location information without obtaining a warrant or showing probable cause, the Court should deny its application.

BACKGROUND

Ninety percent of American adults have a cell phone.[1] Almost 40% of U.S. households have *only* cell phones.[2] As of December of 2013, there were 335.65 million wireless subscriber

[1] *Device Ownership Over Time*, Pew Research Internet Project, http://www.pewinternet.org/data-trend/mobile/device-ownership/ (last visited July 21, 2014).
[2] *Annual Wireless Industry Survey*, CTIA - The Wireless Association, http://www.ctia.org/your-wireless-life/how-wireless-works/annual-wireless-industry-survey (last visited July 21, 2014).

accounts in the United States,[3] a number that exceeds the total population.[4] In 2013, American cell phone users generated 2.618 trillion minutes of calls and 1.91 trillion text messages.[5] According to a recent survey, nearly three quarters of adults with smartphones reported being within five feet of their phones most of the time.[6] Accordingly, people expect to be able to use their cell phones everywhere they go and, for the most part, they can.

Cell phones operate through the use of radio waves. Cellular service providers maintain a network of radio base stations (also called cell sites or cell towers) throughout their coverage areas. *Electronic Communications Privacy Act (ECPA) (Part II): Geolocation Privacy and Surveillance, Hearing before the Subcomm. on Crime, Terrorism, Homeland Security, and Investigations, of the H. Comm. on the Judiciary*, 113th Cong., 50 (2013) (written testimony of Prof. Matt Blaze, University of Pennsylvania) [hereinafter 2013 ECPA Hearing]. A base station consists of multiple antennas facing in different directions. Typically, there are three antennas, each covering a 120-degree arc, resulting in three pie-shaped sectors. Thomas A. O'Malley, *Using Historical Cell Site Analysis Evidence in Criminal Trials*, U.S. Att'y Bull., Nov. 2011, at 19-20.

Cell phones periodically identify themselves to the closest base station (the one with the strongest radio signal) as they move throughout the coverage area. 2013 ECPA Hearing at 50 (Blaze testimony). Whenever a cell phone user makes or receives a call or text message, his phone connects, via radio waves, to an antenna on a cell site, generating cell site location

---

[3] *Annual Wireless Industry Survey*, CTIA - The Wireless Association, http://www.ctia.org/your-wireless-life/how-wireless-works/annual-wireless-industry-survey (last visited July 21, 2014).

[4] *U.S. and World Population Clock*, U.S. Census Bureau, http://www.census.gov/popclock/ (last visited July 21, 2014) (When visited on July 21, population listed at 318.49 million.)

[5] *Annual Wireless Industry Survey*, *supra* note 2.

[6] Harris Interactive, *2013 Mobile Consumer Habits Study*, Jumio, Inc., 2 (June 2013), http://pages.jumio.com/rs/jumio/images/Jumio%20-%20Mobile%20Consumer%20Habits%20Study-2.pdf

information ["CSLI"]. If a cell phone moves away from the base station with which it started a call and closer to another base station, it connects seamlessly to the next base station. *Id.*

As the number of cell phones has increased, the number of cell sites has had to increase as well:

> A sector can handle only a limited number of simultaneous call connections given the amount of radio spectrum 'bandwidth' allocated to the wireless carrier. As the density of cellular users grows in a given area, the only way for a carrier to accommodate more customers is to divide the coverage area into smaller and smaller sectors, each served by its own base station and antenna. New services, such as 3G and LTE/4G Internet create additional pressure on the available spectrum bandwith, usually requiring, again, that the area covered by each sector be made smaller and smaller.

Id. at 54. Densely populated urban areas therefore have more towers covering smaller sectors. Within one mile of the San Francisco Federal Courthouse, for example, there are 71 towers and 781 separate antennas.[7]

The trend is toward smaller and smaller base stations, called microcells, picocells, or femtocells, which cover a very specific area, such as one floor of a building, the waiting room of an office, or a single home. *Id.* at 43-44. The effect of this proliferation of base stations is that "knowing the identity of the base station (or sector ID) that handled a call is tantamount to knowing a phone's location to within a relatively small geographic area ... sometimes effectively identifying individual floors and rooms within buildings." *Id.* at 55-56. Although the ability of cell providers to track a phone's location within a sector varies based on a number of factors, it is increasingly possible to use CSLI to "calculate users' locations with a precision that approaches that of GPS." *Id.* at 53.

---

[7] Information regarding the concentration of towers in a given geographic area can be found on a public database, available at http://www.antennasearch.com/sitestart.asp

Tools and techniques are constantly being developed to track CSLI with ever-greater precision. Providers can currently triangulate the location of a phone within a sector by correlating the time and angle at which it connects with multiple base stations. *Id.* at 56. Providers also are developing technologies that will track CSLI whenever a phone is turned on, whether or not it is in use. *Id.* at 57. Because this information costs little to collect and store, providers tend to keep it indefinitely. *Electronic Communications Privacy Act Reform and the Revolution in Location Based Technologies and Services, Hearing before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong., 16 (2010) (testimony of Prof. Matt Blaze) [hereinafter 2010 ECPA Hearing].

The ability to track people through their cell phones is, obviously, very appealing to law enforcement. *See* O'Malley, *supra*, at 26 (noting that provider records "contain accurate date, time, and location information" and "unlike a witness' memory, are not prone to impeachment based on their accuracy, reliability, or bias"); 2013 ECPA Hearing at 61 ("These characteristics – ubiquitous and continuous availability, lack of alerting, and high precision – make network-based cellular tracking an extremely attractive and powerful tool for law enforcement surveillance.").

Consequently, each year the United States government seeks CSLI for tens of thousands of people. 2010 ECPA Hearing at 80 (written testimony of United States Magistrate Judge Stephen Wm. Smith). The government almost always seeks this information by way of sealed applications and orders. *Id.* at 87. In this district alone, the Office of the United States Attorney has identified 760 matters in its case management system that were likely to involve applications for location-tracking information between January 1, 2008, and January 3, 2013. Declaration of Patricia J. Kenney in Support of the Department of Justice's Motion for Summary Judgment as to Part 1 of Plaintiff's Freedom of Information Act Request at 10, *American Civil Liberties Union of Northern California v. Department of Justice*, No. 12-cv-4008 MEJ (N.D. Cal. Sept. 23, 2013).

DISCUSSION

I. THE FOURTH AMENDMENT PROHIBITS WARRANTLESS SEARCH AND SEIZURE OF CSLI

A. CSLI Is Protected by the Fourth Amendment Right to Privacy

The Fourth Amendment prohibits the government from collecting an individual's historical location tracking information without a warrant. Since at least 1967, the Supreme Court has recognized that the Fourth Amendment protects an individual's right to privacy, even in public places. *Katz v. United States*, 389 U.S. 347, 351 (1967). *Katz* held that when the government infringes upon a subjective expectation of privacy that society recognizes as reasonable, it effects a search and seizure within the meaning of the Fourth Amendment. *Id.* at 353. Thus, in *Katz*, the government was found to have violated the defendant's Fourth Amendment rights by eavesdropping on his private conversation in a public phone booth. *Id.*

In *United States v. Knotts*, the Court first applied the *Katz* test to electronic surveillance, holding that the Fourth Amendment was not violated when the government used a beeper to track a car from one location to another. 460 U.S. 276, 277 (1983). The beeper tracking in *Knotts* did not implicate the Fourth Amendment because "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." *Id.* at 281. However, the Court left open the possibility that advances in surveillance technology would require a reevaluation of its decision. *Id.* at 283-84.

The following year, in *United States v. Karo*, the Court limited *Knotts* to electronic surveillance *in public places*. 468 U.S. 705, 714 (1984). In *Karo*, the police placed a beeper in a container belonging to the defendant and monitored its location electronically, including while it was inside a private residence. *Id.* at 708-10. The Court held that the continued monitoring of the beeper inside the home was an unconstitutional trespass into the residence by electronic

means – even though the officers could not have known, when they planted the tracking device, that it would end up inside a house. *Id.* at 715; *see also Kyllo v. United States*, 533 U.S. 27, 34 (2001) (holding that the government engages in a search in violation of the Fourth Amendment by using a thermal imager to detect heat signatures inside a house that would be invisible to the naked eye).

More recently, in *United States v. Jones*, five Justices concluded that prolonged, electronic location monitoring by the government impinges upon a legitimate expectation of privacy in violation of the Fourth Amendment. 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring); *id.* at 965 (Alito, J., concurring). In *Jones*, the government placed a GPS tracker on the defendant's car and used it to monitor the car's location – on public thoroughfares – for 28 days. *Id.* at 948. The majority opinion held that the government had violated the Fourth Amendment by the physical trespass of placing the tracker on the vehicle, and it therefore did not need to address whether the location tracking violated a reasonable expectation of privacy. *Id.* at 949. It explicitly noted, however, that "[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis." *Id.* at 953 (emphasis in original).

The five Justices who did engage in a *Katz* analysis concluded that the government's actions in tracking the car's location violated the Fourth Amendment. *Id.* at 964 (Alito, J., concurring); *id.* at 955 (Sotomayor, J., concurring).[8] Despite the fact that the government tracked the car only as it travelled in plain sight on public streets and highways, Justice Alito concluded that the GPS monitoring "involved a degree of intrusion that a reasonable person would not have

[8] Justice Sotomayor, while agreeing with Justices Alito, Ginsburg, Breyer, and Kagan that an analysis under *Katz* was appropriate, nonetheless wrote separately because she also joined the majority in concluding that the physical trespass of placing the tracker on the car was an independent Fourth Amendment violation. *Jones*, 132 S. Ct. at 954-55 (Sotomayor, J., concurring).

anticipated." *Id.* at 964 (Alito, J., concurring). Consequently, he found that "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." *Id.* Notably, this conclusion did not depend upon on the type of technology used to track the car in *Jones*; rather, Justice Alito discussed the proliferation of modern devices that track people's movements, noting that cell phones were "perhaps [the] most significant" among these. *Jones*, 132 S. Ct. at 963 (Alito, J., concurring).

Justice Sotomayor agreed that prolonged electronic surveillance violates the Fourth Amendment. *Id.* at 955 (Sotomayor, J., concurring). She added, however, that "even short-term monitoring" raises concerns under *Katz* because "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *Id.* When governmental actions intrude upon someone's privacy to that degree, a warrant is required. *Id.*

Here, as in *Jones*, the government seeks permission to track individuals, without a warrant, over an extended period of time, by electronic means.[9] CSLI, like GPS, provides the government with a comprehensive, intimate portrait of an individual's life. Most people would not expect that the government can access, without a warrant, records tracking their movements for weeks or months at a time – and that expectation is a reasonable one.

The ability of CSLI to track people inside buildings raises additional Fourth Amendment concerns. *Kyllo* and *Karo* prohibit warrantless intrusions into the home, intended or not, by means of technology. *Kyllo*, 533 U.S. at 34; *Karo*, 468 U.S. at 17. As the Court acknowledged in *Kyllo*, "the rule we adopt must take account of more sophisticated systems that are already in use or in development." *Kyllo*, 533 U.S. at 36. Because CSLI is generated by radio waves, it

[9] This Opposition addresses CSLI in general terms only, because no information was disclosed about the type of location information the government is seeking or the length of time covered by its application.

inevitably collects information from inside buildings, including private homes. Especially as cell sites cover smaller and smaller sectors, cell site location tracking to (or even within) a specific home is inevitable. Even today, the government has no way of restricting its requests for CSLI to public spaces – which is one reason that governmental requests for this information should be supported by probable cause and a warrant.

B. This Court Should Follow the Eleventh Circuit in Holding That Historical Cell Site Location Information Is Protected by the Fourth Amendment

As noted above, the data the government seeks when it requests CSLI is much more comprehensive, and much more apt to reveal intimate information, than the location of someone's car. Accordingly, the Eleventh Circuit recently held that, in light of the *Jones* concurrences, government requests for CSLI are subject to the warrant requirement of the Fourth Amendment. *United States v. Davis*, ___ F.3d ___, 2014 WL 2599917 at *10 (11th Cir. 2014). *Davis* compared the information revealed to the government via a GPS device on a vehicle with that revealed by CSLI and found that the violation of privacy rights implicated by disclosure of CSLI was much more significant:

> One's car, when it is not garaged in a private place, is visible to the public, and it is only the aggregation of many instances of the public seeing it that make it particularly invasive of privacy to secure GPS evidence of its location...In contrast, even on a person's first visit to a gynecologist, a psychiatrist, a bookie, or a priest, one may assume that the visit is private if it was not conducted in a public way. One's cell phone, unlike an automobile, can accompany its owner anywhere. Thus, the exposure of the cell site location information can convert what would otherwise be a private event into a public one. When one's whereabouts are not public, then one may have a reasonable expectation of privacy in those whereabouts.

Id. at *8. Because the location of a cell phone is so apt to reveal private information about its owner, *Davis* concluded, "even one point of cell site location data can be within a reasonable expectation of privacy." *Id.* Indeed, while people are in their cars only while travelling from one

place to another, most Americans are within five feet of their phones most of the time.[10] Especially in urban settings, where cell towers are more plentiful, this means that a cell phone – and, by extension, its owner – can be tracked with disquieting precision.[11]

The government urges this Court to disregard *Davis* and instead follow the Third and Fifth Circuits in holding that the government need not procure a warrant before acquiring CSLI. *See In re Application*, 724 F.3d 600 (5th Cir. 2013); *In the Matter of the Application*, 620 F.3d 304 (3d Cir. 2010). The Third Circuit opinion, which was issued before *Jones* was decided, is based on the proposition that location monitoring does not implicate Fourth Amendment privacy rights.[12] *In the Matter of the Application*, 620 F.3d at 313 ("The *Knotts/Karo* opinions make clear that the privacy interests at issue are confined to the interior of the home."). This reasoning cannot stand in the face of *Jones*, which explains that the government's prolonged surveillance of individuals, even in public places, *does* implicate the Fourth Amendment. *Jones*, 132 S. Ct. at 953; *id.* at 955 (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring).

The Fifth Circuit, on the other hand, held that any disclosure of private information to a third party destroys all privacy interests in the information; *i.e.*, because the cell phone provider collects the CSLI data, the subscriber cannot claim a legitimate interest in its privacy. *In re Application*, 724 F.3d at 610-11. To reach this conclusion, the Fifth Circuit posits that it is

---

[10] Harris Interactive, *2013 Mobile Consumer Habits Study*, Jumio, Inc., 2 (June 2013), http://pages.jumio.com/rs/jumio/images/Jumio%20-%20Mobile%20Consumer%20Habits%20Study-2.pdf

[11] Even cases that disagree on the constitutionality of warrantless CSLI tracking acknowledge that the tracking is precise. *See In re Application*, 724 F.3d 600, 609 (5th Cir. 2013) ("The reason that the Government seeks such information is to locate or track a suspect in a criminal investigation. The data must be precise enough to be useful to the government… it can narrow someone's location to a fairly small area."); *see also* 2013 ECPA Hearing at 61 ("The increasingly high resolution that the cell site tracking can achieve in densely populated areas – and the ability to provide this data even when the handset is indoors – can paint an even richer picture of an individual's movements than can vehicle-based GPS devices.").

reasonable – and constitutional – to force people to choose between preserving their Fourth Amendment rights and owning a cell phone. *Id.* at 613. As discussed in section II, below, the Supreme Court has never taken such an extreme position. Moreover, the Court's recent decision in *Riley v. California* affirms that the protections of the Fourth Amendment extend to information generated by our cell phones even when it is shared with the provider. 134 S. Ct. 2473 (2014).

C. *Riley v. California* Implicitly Recognizes a Privacy Interest in CSLI

After *Riley*, there can be no doubt that individuals have a reasonable expectation of privacy in cell phone location data. In a rare, unanimous Fourth Amendment decision, the Court explained that cell phones "hold for many Americans the privacies of life." *Id.* at 2495 (citation and internal quotation marks omitted). *Riley*'s focus on the wealth of information revealed by an individual's cell phone, and the attendant right to privacy in that information, applies beyond the limited context of searches incident to arrest.[13]

Because cell phones have the capacity to expose such vast amounts of personal information about their owners, the Court refused to engage in a "mechanical application" of precedent. *Id.* at 2484. *Riley* thus rejected the government's efforts to analogize cell phone information to any pre-digital counterpart. *See id.* at 2488 ("The United States asserts that a

---

[12] As discussed in section V, infra, the Third Circuit did hold that 18 U.S.C. § 2703 gives magistrates the discretion to require a warrant for CSLI on a case-by-case basis. *In the Matter of the Application*, 620 F.3d at 319.

[13] Commentators agree that *Riley*'s holding extends well beyond the particular warrant exception at issue. Legal scholars have widely characterized the holding as sweeping, and one that will have broad implications in other areas. *See, e.g.*, Marc Rotenberg & Alan Butler, *Symposium: In* Riley v. California, *A Unanimous Supreme Court Sets Out Fourth Amendment for Digital Age*, SCOTUSblog (June 26, 2014, 6:07 PM), http://www.scotusblog.com/2014/06/symposium-in-riley-v-california-a-unanimous-supreme-court-sets-out-fourth-amendment-for-digital-age/ ("The Court's conclusion that *data is different* will affect not only digital search cases, but also the NSA's bulk record collection program, access to cloud-based data, and the third-party doctrine."); Adam Liptak, *Major Ruling Shields Privacy of Cellphones*, N.Y. Times (June 25, 2014), http://www.nytimes.com/2014/06/26/us/supreme-court-cellphones-search-privacy.html ("While the decision will offer protection to the 12 million people arrested every year, many

search of all data stored on a cell phone is 'materially indistinguishable' from searches of these sorts of physical items. That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together."). The Court declared, without qualification, that "[m]odern cell phones, *as a category*, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse." *Id.* at 2488-89 (emphasis added).

Historical location data generated by cell phones served as one of the Court's chief examples of "the privacies of life" that cell phone metadata exposes. *See id.* at 2490 ("Data on a cell phone can also reveal where a person has been. Historic location information… can reconstruct someone's specific movements down to the minute, not only around town, but within a particular building."). The Court cited with approval Justice Sotomayor's concurrence in *Jones*, in which she concluded that generating and monitoring "a precise, comprehensive record of a person's public movements" infringes upon a reasonable expectation of privacy that is protected by the Fourth Amendment. *Id.* at 2490 (citing *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring)).

Riley also contains echoes of the "mosaic theory" of privacy adopted by Justices Sotomayor and Alito in their *Jones* concurrences, noting that "[a] cell phone collects in one place many distinct types of information… that reveal much more in combination than any isolated record." *Id.* at 2489.[14] The Court explained that aggregating, then analyzing, this data intrudes upon a protected privacy interest: "The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet." *Id; see also Davis*, ___ F.3d

---

for minor crimes, its impact will most likely be much broader.").

___, 2014 WL 2599917 at *6 (noting that the government often relies on mosaic theory to establish that aggregated data is far more revealing than the sum of its parts).

Riley thus stands in direct opposition to the government's position in this case. Cell phones, as the *Riley* court acknowledged, are ubiquitous. *See* 134 S. Ct. at 2490 ("According to one poll, nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower."). The data they collect is "qualitatively different" than that contained in other objects, for purposes of Fourth Amendment analysis. *Id.* *Riley's* discussion of the nature of cell phones and our dependence upon them forecloses any argument that it is "reasonable" to expect that the 90% of American adults who carry cell phones thereby waive their Fourth Amendment right to not be subject to constant government surveillance.

II. CELL PHONE SUBSCRIBERS DO NOT FORFEIT THEIR FOURTH AMENDMENT RIGHTS SIMPLY BECAUSE THEIR CSLI RECORDS ARE MAINTAINED BY THIRD-PARTY CELL PHONE COMPANIES

A. An Individual Does Not Lose the Right to Privacy in CSLI Simply Because It Is Disclosed to a Cell Phone Provider

The government urges this Court to follow the Fifth Circuit by analogizing the CSLI at issue here to the bank records and pen registers at issue in *Smith v. Maryland*, 442 U.S. 735 (1979), and *United States v. Miller*, 425 U.S. 435 (1976). *Smith* and *Miller* held that, by voluntarily sharing dialed numbers with the phone company and banking records with the bank, the consumer waived any right to privacy in those records for purposes of the Fourth Amendment. *Smith*, 442 U.S. at 742; *Miller*, 425 U.S. at 442-43. The fact that the cell phone providers maintain records of individuals' CSLI does not, however, diminish the individuals' privacy interest in those records. Exposing information to a third party does not necessarily

[14] *See also, e.g., United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010) (adopting, in lower court

waive one's expectation of privacy and attendant Fourth Amendment protections.[15]

The third-party doctrine discussed in *Smith* and *Miller* is inapplicable to an era where people routinely and unthinkingly disclose the most intimate details of their lives to their cell phone providers. As Justice Sotomayor recognized in *Jones*, our increasing dependence on technology in daily life requires a re-evaluation of the question of "privacy" in the context of the Fourth Amendment:

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. *E.g., Smith,* 442 U.S., at 742, 99 S. Ct. 2577; *United States v. Miller,* 425 U.S. 435, 443, 96 S. Ct. 1619, 48 L. Ed. 2d 71 (1976). This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.

132 S. Ct. at 957 (Sotomayor, J., concurring); *see also* Aya Gruber, *Garbage Pails and Puppy Dog Tails: Is That What* Katz *Is Made Of?*, 41 U.C. Davis L. Rev. 781 (2008) (arguing that the third-party doctrine is "extremely dangerous in an increasingly technological world" and must be reconsidered in light of actual societal expectations of privacy in digital information).

The Supreme Court has consistently revisited its Fourth Amendment jurisprudence in

---

opinion in *Jones*, the "mosaic" theory to hold that GPS tracking of a car is a "search").

[15] *See Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001) (holding that patients have reasonable expectation of privacy in results of medical tests, despite their voluntary disclosure of those results to hospital personnel); *Bond v. United States*, 529 U.S. 334, 338-39 (2000) (holding that traveler retains reasonable expectation of privacy in bag placed in overhead bin of a bus, despite knowledge that other passengers can handle and move bag); *Quon v. Arch Wireless Operating Co. Inc.*, 529 F.3d 892, 905-07 (9th Cir. 2008) (holding that police officer had reasonable expectation of privacy in contents of text messages sent on phone owned by police department despite fact that third-party server had access to the messages *and* despite department policy stating there was no expectation of privacy in texts), *rev'd on other grounds*, 560 U.S. 746 (2010)); *United States v. Taketa*, 923 F.2d 665, 677 (9th Cir. 1991) (holding that agent had reasonable expectation of privacy in not being secretly videotaped in someone else's office).

light of evolving technology. *See Kyllo*, 533 U.S. at 33-34 ("It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."). *Jones* thus recognized that GPS technology was qualitatively different than its physical surveillance counterpart.[16] 132 S. Ct. at 954. *Riley* similarly rejected any comparison between physical items in an arrestee's possession and his cell phone. *See* 134 S. Ct. at 2485 ("A search of the information on a cell phone bears little resemblance to the type of brief physical search considered in [*United States v. Robinson*, 414 U.S. 218 (1973)]").

Here, as in *Jones* and *Riley*, the realities of modern technology preclude the mechanical application of 35-year-old precedent. In 1979, the year *Smith* was decided, Jimmy Carter was president, *The Dukes of Hazard* premiered on CBS, and telephones travelled only as far as their cords would allow. The Court could not have foreseen that one day the telephone company would be automatically electronically tracking the vast majority of Americans everywhere, all the time, and regularly turning that information over to the government. It is inconceivable that *Smith* and *Miller* intended so far-reaching an abrogation of our Fourth Amendment rights.[17]

The advent of technologies that enable more intrusive police surveillance cannot be permitted to "erode the privacy guaranteed by the Fourth Amendment." *See Kyllo*, 533 U.S. at

---

[16] Even the *Knotts* court acknowledged that its analysis was subject to change with evolving surveillance technology. 460 U.S. at 283-84 ("If such dragnet type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable."); *see also United States v. Pineda-Moreno*, 617 F.3d 1120, 1126 (9th Cir. 2010) (Kozinski, J., dissenting) ("When requests for cell phone location information have become so numerous that the telephone company must develop a self-service website so that law enforcement agents can retrieve user data from the comfort of their desks, we can safely say that 'such dragnet-type law enforcement practices' are already in use.").

[17] Indeed, although the government's concession in *Riley* that a search had occurred enabled the Court to avoid fully reconsidering *Smith*, the Court took the opportunity to explain that the pen register in *Smith* bore little relationship to the phone data being mined by the government. *Riley*, 134 S. Ct. at 2492. The Court noted that, even on an old-fashioned flip phone, a cell phone's call log (and thus its metadata) "contained more than just phone numbers," including substantial personal identifiers, rendering a case about pen registers of little utility in deciding the Fourth Amendment question in the context of cell phones. *Id.* at 2493.

34. This Court should join others across the country in rejecting "the fiction that the vast majority of the American population consents to warrantless government access to the records of a significant share of their movements by 'choosing' to carry a cell phone." *In the Matter of an Application*, 809 F. Supp. 2d 113, 127 (E.D. N.Y. 2011); *see also In the Matter of an Application*, 736 F. Supp. 2d 578, 596 (E.D. N.Y. 2010) ("The Fourth Amendment cannot properly be read to impose on our populace the dilemma of either ceding to the state any meaningful claim to personal privacy or effectively withdrawing from a technologically maturing society."); *cf. In re United States*, 2006 WL 1876847 at **1, 3 (N.D. Ind. 2006) (unpublished) (denying government's appeal from magistrate's order denying prospective and historical CSLI without a warrant); *cf. also In Matter of United States*, ___ F. Supp. 2d ___, 2014 WL 1395082 at *1 (D. D.C. 2014) (noting "serious statutory and constitutional questions" raised by government's application for historical CSLI and ordering amicus and the government to submit "evidence and substantive briefing" before deciding "whether this application should be granted in its current form -- and without a showing of probable cause").

B. CSLI Is Not Voluntarily Conveyed to a Third Party

Even under the third-party doctrine articulated in *Smith* and *Miller*, however, cell phone users would retain a constitutionally protected privacy interest in their CSLI. *Smith* 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. 442 U.S. at 742. The consumer also received a list of numbers dialed on his monthly bill, confirming that the phone company was recording this information. *Id.* Similarly, *Miller* declined to extend Fourth Amendment protection to bank documents (*e.g.*, checks, deposit slips) because these documents were intentionally shared by the consumer with bank employees in order to achieve the consumer's purpose (*e.g.*, transferring

money to another entity, depositing money in an account) and the bank was a party to these transactions. 425 U.S. at 440-43.

CSLI, on the other hand, is not knowingly and intentionally conveyed by the consumer to anyone but rather generated automatically by radio waves. People do not use their cell phones as tracking devices or expect that the government will do so. In contract to *Smith*-era telephone bills, which listed toll calls, cell phone users do not receive a report of their CSLI from their service providers. Nor do providers inform them how long they retain CSLI. Cell phone users do not affirmatively convey CSLI, nor can they control its disclosure. Accordingly, the Third and Eleventh circuits have rejected the argument that CSLI is voluntarily conveyed by cell phone users. *Davis*, ___ F.3d ___, 2014 WL 2599917 at *9; *In the Matter of the Application*, 620 F.3d at 317.

The Ninth Circuit also has rejected the general theory that passive transmission of data to a third party waives a consumer's Fourth Amendment rights. In *United States v. Forrester*, the court held that email and IP addresses were not protected by the Fourth Amendment. 512 F.3d 500, 510 (9th Cir. 2008). Significantly, the court drew a distinction between this information, which the consumer conveys intentionally for purposes of delivering his email or directing his browser to a specific address, and data that is "merely passively conveyed through third party equipment." *Id.* The court thus retained Fourth Amendment protection for information that is not conveyed voluntarily to achieve a purpose of the consumer. *Id.* at 511 ("E-mail, like physical mail, has an outside address 'visible' to the third-party carriers that transmit it to its intended location, and also a package of content that the sender presumes will be read only by the intended recipient.").

Even the *Smith* Court recognized that the voluntary disclosure of information to a third

party does not erase all Fourth Amendment protection.[18] 442 U.S. at 739-40. *Smith* distinguished between records of dialed telephone numbers and the content of telephone conversations, which it acknowledged remained protected by the Fourth Amendment. *Id.* The location information at issue here is more analogous to the content of a communication than to an address. Tracking a person via the location of his cell phone is akin to electronically following him everywhere he goes, inside and outside, day and night, for the period of surveillance. This is far more intrusive than recording the phone numbers he dials, and it warrants greater Fourth Amendment protection. *See Davis*, ___ F.3d ___, 2014 WL 2599917 at *8 ("cell site data is more like communications data than it is like GPS information. That is, it is private in nature rather than being public data that warrants privacy protection only when its collection creates a sufficient mosaic to expose that which would otherwise be private.").

III. CSLI IS NOT A BUSINESS RECORD OF THE PROVIDER

A. A Service Provider's Ability to Access CSLI Does Not Defeat the Subscriber's Reasonable Expectation of Privacy

Relying on the Fifth Circuit's decision, the government argues that it may obtain CSLI because "a historical cell site record 'is clearly a business record' of the cell phone provider," Gov't Application at 5 (quoting *In the Matter of the Application*, 724 F.3d at 612), and, as such, may be obtained by subpoena or similar compulsory process. The government contends that it need not, therefore, establish probable cause before acquiring CSLI and is subject only to the Fourth Amendment's "reasonableness standard for compulsory process." *Id.*

The fundamental flaw in this argument is that it begs the critical question of whether cell

[18] Even if disclosure to a third party diminishes an individual's privacy interest, *Riley* explicitly held that "diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely." 134 S. Ct. at 2488. "To the contrary, when 'privacy-related concerns are weighty enough' a 'search may require a warrant notwithstanding the diminished expectations of privacy.'" *Id.* (quoting *Maryland v. King*, 133 S. Ct. 1958, 1979 (2013)).

phone users have a reasonable expectation of privacy in their location information. *See Smith*, 442 U.S. at 742 ("petitioner's argument that [the pen register] installation and use constituted a 'search' necessarily rests upon a claim that he had a 'legitimate expectation of privacy' regarding the numbers he dialed on his phone"); *Miller*, 425 U.S. at 442 ("We must examine the nature of the particular documents sought to be protected in order to determine whether there is a legitimate 'expectation of privacy' concerning their contents."). If a reasonable expectation of privacy exists, the fact that the record is maintained in the course of business does not strip it of Fourth Amendment protection.

As discussed above, cell phone users do have a reasonable expectation of privacy in their CSLI. Therefore, the government cannot obtain it simply by issuing a subpoena. *See Miller*, 425 U.S. at 444 ("[T]he general rule that the issuance of a subpoena to a third party to obtain the records of that party does not violate the rights of a defendant" applies only when "no Fourth Amendment interests… are implicated.").

A second flaw in the government's argument is that, as discussed above, cell phone users do not knowingly and voluntarily convey their location information to the cell phone provider. The voluntariness question is significant in the business records analysis. *See Smith*, 442 U.S. at 445 (stating that it does not matter "whether or not the phone company in fact elects to make a quasi-permanent record of a particular number dialed" but rather whether "petitioner voluntarily conveyed to it information that it had facilities for recording and that it was free to record"). Two of the three circuits that have addressed whether cell phone users voluntarily share their location information have concluded that they do not. *See Davis*, ___ F.3d ___, 2014 WL 2599917 at *9 (following Third Circuit in rejecting argument that cell phone users knowingly and voluntarily share with providers their historical CSLI); *In the Matter of the Application*, 620 F.3d at 317 ("A cell phone customer has not 'voluntarily' shared his location information with a

cell provider in any meaningful way.").[19]

Once a subscriber has demonstrated a reasonable expectation of privacy in records held by a third party, the question becomes whether the disclosure or some other factor defeats the Fourth Amendment protection otherwise accorded to the records. In *United States v. Warshak*, the Sixth Circuit rejected the argument that an internet service provider's ability and right to access the contents of a subscriber's emails eliminated the subscriber's reasonable expectation of privacy in his emails. 631 F.3d 266, 286-87 (6th Cir. 2010). The ISP's control over and ability to access the emails "will not be enough to overcome an expectation of privacy." *Id.* at 287 (internal quotation marks omitted). There is no reason the Court should reach a different conclusion in this case.

B. Service Providers Were Forced by the Government to Configure Their Networks to Generate CSLI for Law Enforcement Purposes

Moreover, CSLI is not a business record of the provider because the government requires cell phone companies to record CSLI for law enforcement purposes and to give law enforcement access to it. In 1994, Congress enacted the Communications Assistance for Law Enforcement Act ["CALEA"], 18 U.S.C. §§ 1001-1010, which required all cell phone service providers to build into their networks equipment capable of "expeditiously isolating and enabling the government… to access call-identifying information." 47 U.S.C. § 1002(a). "Call-identifying information" includes CSLI. *U.S. Telecomm. Ass'n v. FCC*, 227 F.3d 450, 453 (D.C. Cir. 2000).

CALEA was enacted for the express purpose of allowing law enforcement "to intercept communications involving advanced technologies such as digital or wireless transmission

[19] Other cases that the government cites to support this claim also fail to advance its argument. In *Donaldson v. United States*, 400 U.S. 517 (1971), and *SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735 (1984), the Court found no reasonable expectation of privacy because people had intentionally disclosed the information at issue to someone else. Similarly, in *United States v. Golden Valley Elec. Ass'n*, the

modes." H.R. Rep. No. 103-827(I) at 9 (1994); *see also* Communications Assistance For Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (enacting CALEA "to make clear a telecommunications carrier's duty to cooperate in the interception of communications for law enforcement purposes"). Following the enactment of CALEA, the Telecommunications Industry Association, after extensive negotiations with the FBI, promulgated technical standards outlining the "technical features, specifications, and protocols" a network must incorporate to comply with CALEA. *U.S. Telecomm. Ass'n*, 227 F.3d at 455. These standards are known as the "J-Standard." *Id.* Providers who do not comply with these standards are subject to fines of $10,000.00 per day. *Id.* at 455.

When the J-Standard first was adopted by the FCC, telecommunications industry associations, along with privacy rights groups, challenged it on the grounds that CSLI was outside the scope of CALEA. *Id.* at 455. They objected that the requirement that their networks track and provide CSLI "effectively converts ordinary mobile telephones into personal location-tracking devices, giving law enforcement agencies access to far more information than they previously had." *Id.* at 455-56. The FCC disagreed, and the courts ultimately ruled that CSLI is "call-identifying information" under CALEA and that the providers are, therefore, required to collect it and to make it available to law enforcement. *Id.* at 463.

Today, the J-Standard dictates the default network architecture of every cell phone service provider in the United States. *See* Micah Sherr, et al., *Can They Hear Me Now? A Security Analysis of Law Enforcement Wiretaps*, Proc. 16th ACM Conf on Computer & Comms. Sec. 512, 514 (Nov. 2009) ("This architecture is the only currently fielded standard for complying with CALEA."). It mandates that every cell network include elements that function as "interception

---

reasonableness standard applied because the records at issue were ones in which the consumer had no reasonable expectation of privacy. 689 F.3d 1108, 1116—17 (9th Cir. 2012).

access points" that have the ability to convey CSLI to law enforcement. *Id.* at 514-15. Consequently, cell phone users have no choice but to obtain their cell phone service from a company that is required, by the federal government, to track their CSLI and to make it available to law enforcement.

In light of this history, the government's claim that "[c]ell 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 historical cell site records," Govt. Letter Brief, at 1, is disingenuous, at best. Indeed, when engaged in litigation to force cell phone providers to create networks capable of transmitting CSLI to law enforcement, the Justice Department recognized the privacy interest at stake and conceded, in its brief in *U.S. Telecomm. Ass'n*, that "a pen register order does not by itself provide law enforcement with authority to obtain location information, and we have never contended otherwise." 227 F.3d at 464. The government cannot now claim that CSLI is information that cell phone service providers independently choose to record and preserve that coincidentally happens to be useful to law enforcement.

IV. THE STORED COMMUNICATIONS ACT DID NOT CONTEMPLATE CSLI

The government also argues that Congress determined that it could obtain CSLI based on only a court order, without showing probable cause, when it enacted the Stored Communications Act ["SCA"], including 18 U.S.C. § 2703(d).[20] Because CSLI is protected by the Fourth Amendment, as discussed above, a warrant supported by probable cause is required, and the government may not obtain CSLI based on a lesser showing, even if it complies with the statute. *See Davis*, ___ F.3d ___, WL 2599917 at *3 (holding that "[t]he obtaining of [cell site location]

data without a warrant is a Fourth Amendment violation" even though government obtained information under a § 2703(d) order). "It is clear, of course, that no Act of Congress can authorize a violation of the Constitution." *Almeida-Sanchez v. United States*, 413 U.S. 266, 272 (1973).

Moreover, there is no indication in the SCA or the relevant legislative history that Congress considered, or intended to address, CSLI in promulgating the SCA. *See In re United States*, 441 F. Supp. 2d 816, 833 (S.D. Tex. 2006) ("Hybrid proponents concede that the SCA was not specifically enacted as the mechanism to collect cell site data."). The legislative history of the SCA establishes that Congress enacted it primarily to "'protect against the unauthorized interception of electronic communications.'" *In the Matter of the Application*, 620 F.3d at 313 (quoting S. Rep. No. 99-541, at 1 (1986)). Although the legislative history refers to cell phones, it discusses location information only with respect to "tracking devices" or transponders, which it defines as "one-way radio communication devices that emit a signal on a specific radio frequency" – not cell phones. S. Rep. No. 99-541 at, *e.g.*, 2, 4, 9, 10. The section describing "cellular telephones" does not mention location information. *Id.* at *9.

The SCA was last amended in 1994, by CALEA. That amendment addressed CSLI only by precluding the government from obtaining it based solely on a pen register application. *In the Matter of the Application*, 620 F.3d at 315 n.1 (quoting 47 U.S.C. § 1002(a)(2)(B)); *see also* 2010 ECPA Hearing at 2 (2010) (Rep. Sensenbrenner: "In enacting . . . CALEA, Congress specifically instructed that a person's location information cannot be acquired solely pursuant to a pen register."). In fact, Congress held a series of hearings in 2010 to address CSLI precisely because it had not considered the subject when it enacted or amended the SCA. *See* 2010 ECPA

[20] *See* Govt. Letter Brief at 7 ("In the Stored Communications Act, including § 2703(d), Congress has enacted legislation controlling government access to historical records of cell-phone providers. When

Hearing at 2 (Rep. Sensenbrenner: "Considering that the ECPA was enacted in 1986, well before the proliferation of cell phones and other technologies, I think it is fair to say that the statute does not speak specifically to these issues."); *id.* at 82 (Magistrate Smith: "ECPA does not explicitly refer to 'cell site' or other location information from a cell phone.").

A review of the explosive growth in cell site networks and the proliferation of cell phones over the past 28 years further belies any claim that the 1986 SCA adequately protects cell phone users' privacy interests when the government seeks CSLI today. Indeed, that is one of the reasons the 2010 hearing was necessary:

> [M]obile communication devices have evolved from being little more than a convenience for the wealthy to a basic necessity for most Americans. Cell phones have transformed the way we communicate and work with each other on a daily basis... According to a 2009 Wireless Association report, there were approximately 227 million cell phone services subscribers in the United States last year. That is about 90 percent of the overall population.

Id. at 3-4 (Rep. Johnson); *see also id.* at 3 (Rep. Sensenbrenner: "I think we all know that a 24-year-old original law and a 16-year-old second law is way out of date compared to where the technology is at.").

When the SCA was passed in 1986, there were only 1,000 cell sites in the United States, and fewer than 1% of Americans used cell phones.[21] When the SCA was amended in 1994, fewer than 10% of Americans used cell phones.[22] Today, more than 90% of American adults have one. The increase in the number of cell phones and the uses to which they are put has driven a corresponding increase in the number of base stations, which means CSLI is much more

---

the government seeks historical cell site records using a § 2703(d) order, it complies with this statute.").

[21] Andrea Meyer, 30th Anniversary of the First Commercial Cell Phone Call, Verizon Wireless News Center, (October 11, 2013), http://www.verizonwireless.com/news/article/2013/10/30th-anniversary-cell-phone.html.

accurate now than it was in 1986 or in 1994. 2013 ECPA Hearing at 43 (Blaze testimony). Modern technology allows a cell phone's location to be identified with accuracy close to that of GPS.[23] *Id.* at 56 (Blaze written remarks).

Federal and local law enforcement agencies have taken advantage of the proliferation of cell phones and cell networks, seeking CSLI in more than a million cases a year.[24] The government has sought CSLI almost always in secret and almost always without a warrant, as in this case. *See, e.g.*, 2010 ECPA Hearing at 77 (testimony of Magistrate Smith referring to "regime of secrecy"); Jennifer Valentino-DeVries, Sealed Court Files Obscure Rise in Electronic Serveillance, Wall Street Journal, June 2, 2014[25] (discussing indefinite sealing of most government non-warrant requests for electronic surveillance, including CSLI).

The SCA was not enacted – or amended – to address the proliferation of government requests for CSLI. Since its passage (28 years ago) and most recent amendment (20 years ago), there have been tremendous technical advances in the accuracy of location information. That, along with Americans' widespread dependence on cell phones for an ever-increasing number of

---

[22] Andrew Kupfer, AT&T's $12 Billion Cellular Dream, Fortune, Dec. 12, 1994, at 110, available at http://archive.fortune.com/magazines/fortune/fortune_archive/1994/12/12/80051/index.htm.

[23] FCC regulations require cell phone carriers to provide increasingly accurate location information. *See* 47 C.F.R. § 20.18(h) (setting standards for carriers' ability to locate phones within as little as 100 meters for "network based" calls and as little as 50 meters for "hand-set" based calls for increasingly large percentages of their networks between 2012 and 2019); *see also In re Application*, 620 F.3d at 318 (noting FCC regulation).

[24] According to responses from eight providers to an inquiry from Senator Markey, law enforcement agencies requested "personal mobile phone data" for Americans more than one million times in 2012. For Second Year in a Row, Markey Investigation Reveals more than One Million Requests by Law Enforcement for Americans Mobile Phone Data, Press Release from Ed Markey, (December 9, 2013) available at: http://www.markey.senate.gov/news/press-releases/for-second-year-in-a-row-markey-investigation-reveals-more-than-one-million-requests-by-law-enforcement-for-americans-mobile-phone-data; *see also* 2010 ECPA Hearing at 76, 80 (testimony of Magistrate Smith, estimating that "the total number of electronic surveillance orders issued at the federal level each year substantially exceeds 10,000."). As noted above, in this district alone, the government has identified 760 matters that likely involved applications for location-tracking information from 2008 through 2012.

[25] Available at http://online.wsj.com/articles/sealed-court-files-obscure-rise-in-electronic-surveillance-1401761770.

professional and personal activities and the government's relentless pursuit of location information, requires at least a new assessment of the interests at stake in allowing the government routinely to obtain CSLI without a warrant.

V. THE SCA GIVES MAGISTRATES DISCRETION TO REQUIRE A WARRANT FOR CSLI

Even if the Fourth Amendment did not apply to CSLI, the text of the SCA gives magistrate judges discretion to require the government to establish probable cause supporting a warrant before they authorize the release of this information. *See In the Matter of the Application*, 620 F.3d at 319 ("the statute as presently written gives the [magistrate] the option to require a warrant showing probable cause."). When faced with a question of statutory interpretation, courts must rely on "[a]nalysis of the statutory text, aided by established principles of interpretation." *POM Wonderful LLC v. Coca-Cola Co.*, 132 S. Ct. 2228, 2236 (2014). "'If the plain meaning of the statute is unambiguous, that meaning is controlling.'" *United States v. Johnson*, 680 F.3d 1140, 1144 (9th Cir. 2012) (quoting *United States v. Williams*, 659 F.3d 1223, 1225 (9th Cir. 2011) (ellipses omitted)). Only if the statutory language is ambiguous does a court need to resort to legislative history. *Williams*, 659 F.3d at 1225; *see also Reeb v. Thomas*, 636 F.3d 1224, 1226-67 (9th Cir. 2011) ("When the words of a statute are unambiguous judicial inquiry is complete." (internal quotation marks omitted)).

The SCA sets forth procedures by which the government can obtain both content and subscriber information from a cell phone service provider. 18 U.S.C. § 2703(a), (b), (c). The government generally may obtain non-content information without the customer's consent "only when the governmental entity – (A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure…; [or] (B) obtains a court order for such disclosure under subsection (d) of this section." 18 U.S.C. § 2703(c).

Subsection (d) states,

> [a] court order for disclosure under subsection (b) or (c) *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 contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.

18 U.S.C. § 2703(d) (emphases added). "May be issued" is "the language of permission, rather than mandate." *In the Matter of the Application*, 620 F.3d at 315. Accordingly, the Third Circuit held, the plain language of § 2703 gives magistrates the discretion to require the government to show probable cause supporting a warrant to obtain CSLI.[26] *See id.* at 319 ("If Congress wished that courts 'shall,' rather than 'may,' issue § 2703(d) orders whenever the intermediate standard is met, Congress could easily have said so.").

"At the very least, the use of 'may issue' strongly implies court discretion, an implication bolstered by the subsequent use of the phrase 'only if' in the same sentence." *Id.* at 315. The phrase "only if" indicates that the showing is "a *necessary*, but not a *sufficient*, condition" for issuance of the order. *See California v. Hodari D.*, 499 U.S. 621, 628 (1991) (analyzing phrase in contest of the *Mendenhall* test for determining whether a person has been seized; emphases in original). In other words, § 2703(d) does not require the magistrate to issue the CSLI disclosure order even if the government makes the required showing. S*ee In re Application*, 724 F.3d at 619 (Dennis, J., dissenting) ("The best plain reading of this language is simply that an order *may not issue unless* the standard is met... nowhere does the statute by its terms *require* a court to

[26]As the Third Circuit recognized, even with discretion, magistrates could not act arbitrarily. *In re Application*, 620 F.3d at 316-17. "Discretion is not whim..." *Martin v. Franklin Capital Corp.*, 546 U.S. 132, 139 (2005). A court must have a reason to support its use of discretion, and that reason cannot be based on an error of law or fact. *See United States v. Ressam*, 679 F.3d 1069, 1086 (9th Cir. 2012) (en banc) ("a district court abuses its discretion when it makes an error of law, when it rests its decision on clearly erroneous findings of fact, or when we are left with a definite and firm conviction that the district court committed a clear error of judgment." (internal quotation marks and brackets omitted)).

issue a § 2703(d) order *whenever* the government's application demonstrates reasonable suspicion.") (emphases in original; footnote omitted)).

Reading § 2703(d)'s "shall" as a command rather than a permission would render "only" surplusage: "[T]he difference between 'shall… if'… and 'shall … *only* if'… is dispositive." *In the Matter of the Application*, 620 F.3d at 315. As the Third Circuit stated, "the statute does contain the word 'only' and neither we nor the Government is free to rewrite it." *Id.* at 316; *see also Beck v. Prupis*, 529 U.S. 494, 506 (2000) (referring to "the longstanding canon of statutory construction that terms in a statute should not be construed so as to render any provision of that statute meaningless or superfluous.").

For the "only" in § 2703(d) to have meaning, it must be construed to allow a magistrate the discretion to deny an application for an order under § 2703(d) even if the government has made the necessary showing. To read the statute otherwise, the Third Circuit noted, "could give the Government the virtually unreviewable authority to demand a § 2703(d) order on nothing more than its assertion. Nothing in the legislative history suggests that this was a result Congress contemplated." *In the Matter of the Application*, 620 F.3d at 317. Denying magistrates discretion to decline to issue § 2703(d) orders "would preclude magistrate judges from inquiring into the types of information that would actually be disclosed by a cell phone provider in response to the Government's request, or from making a judgment about the possibility that such disclosure would implicate the Fourth Amendment, as it could if it would disclose location information about the interior of a home."[27] *Id.*

[27] Section 2703(d)'s plain meaning is made all the clearer by comparison to the pen register statute's mandatory language, where there is no "only," and the court simply "shall issue [an order for pen register surveillance] if" the government makes the required certification. 18 U.S.C. § 3123(a)(1); *see also* Fed. R. Crim. P. 41(d)(1) (providing, in mandatory terms, that judge "must issue the warrant if there is probable cause" for search or seizure).

Moreover, the statute explicitly encompasses the possibility that the government would obtain a warrant, supported by probable cause, to obtain non-content information, such as CSLI, from cell phone providers. *See* 18 U.S.C. § 2703(c)(1)(A) (authorizing government to obtain non-content records or information with federal or state warrant). "[I]f magistrate judges were required to provide orders under § 2703(d), then the Government would never be required to make the higher showing required to obtain a warrant under § 2703(c)(1)(A)." *In the Matter of the Application*, 620 F.3d at 316. The Third Circuit correctly rejected the government's argument "that obtaining a warrant to get CSLI is a purely discretionary decision to be made by it, and one that it would make only if a warrant were, in the Government's view, constitutionally required"; "it trivializes the statutory options to read the [warrant] option as included so that the Government may proceed on one paper rather than two." *Id.*

The doctrine of constitutional avoidance offers an additional reason for the Court to hold that magistrates have discretion under the SCA to require the government to obtain a warrant for CSLI. The doctrine "rest[s] on the reasonable presumption that Congress did not intend" any meaning of a statute "which raises serious constitutional doubts," *Clark v. Martinez*, 543 U.S. 371, 381 (2005), and "[i]t is therefore incumbent upon [the Court] to read the statute to eliminate those doubts so long as such a reading is not plainly contrary to the intent of Congress." *United States v. X-Citement Videos, Inc.*, 513 U.S. 64, 78 (1994); *see also Clark*, 543 U.S. at 384 (courts must adopt any "plausible" construction that would avoid serious constitutional concern). There is no indication that Congress intended to deny magistrates the discretion to reject applications for CSLI orders. *In the Matter of the Application*, 620 F.3d at 319. Allowing them the discretion to require the government to show probable cause when there is a risk of infringement upon Fourth Amendment rights does no disrespect to Congress, which explicitly provided for warrants under § 2703(d), and avoids the potential for constitutional violations.

VI. THE GOVERNMENT MAY OBTAIN CSLI WITH A WARRANT BASED ON PROBABLE CAUSE

The Federal Public Defender's position is not that the government may never obtain CSLI, only that it must seek it pursuant to a warrant supported by probable cause. When there are doubts about the constitutionality of a particular type of search, law enforcement officers should err on the side of the Fourth Amendment and get a warrant. *United States v. Johnson*, 457 U.S. 537, 560-61 (1982). Officers already seek court orders under § 2703(d) to obtain CSLI; there will rarely, if ever, be such an urgent need for this information that officers would not have time to get a warrant. *See Riley*, 134 S. Ct. at 2493 ("Recent technological advances...have... made the process of obtaining a warrant itself more efficient."); Fed. R. Crim. P. 41(d)(3) (authorizing magistrates to issue warrant based on information communicated by phone "or other reliable electronic means").

In holding that the Fourth Amendment generally requires police to get a warrant before searching a cell phone seized incident to arrest, the Supreme Court acknowledged that its decision would "have an impact on the ability of law enforcement to combat crime" and that cell phones "can provide valuable incriminating information about dangerous criminals." *Riley*, 134 S. Ct. at 2493. The same is true of CSLI. But in striking the balance between a user's right to privacy in "all [cell phones] contain and all they may reveal," *id.* at 2494, and law enforcement's interest in obtaining this information, the Court chose to protect privacy: "Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple — get a warrant." *Id.* at 2495. "Get a warrant" should be the Court's response when the government seeks cell site location information as well.

CONCLUSION

In *Jones* and *Riley*, the Supreme Court confirmed that the Fourth Amendment continues – and changes – to protect reasonable expectations of privacy in a digital age. We all have a reasonable expectation of privacy in our movements over time in public and, especially, private spaces. Cell phone users reasonably expect that the government will not use their cell phones to track and record their movements, at least without adequate and constitutional justification. This Court should follow the Eleventh Circuit in requiring the government to obtain a warrant when it seeks CSLI.

Dated: July 28, 2014

Respectfully submitted,

STEVEN G. KALAR
Federal Public Defender

/S/ Ellen V. Leonida
ELLEN V. LEONIDA
Assistant Federal Public Defender

United States District Court,
S.D. Texas,
Houston Division.
In the Matter of the Application of the United States of America for an ORDER AUTHORIZING PROSPECTIVE AND CONTINUOUS RELEASE OF CELL SITE LOCATION RECORDS.

Criminal Action No. H:13–1198M.
Signed July 15, 2014.

Background: United States filed application, pursuant to the Stored Communications Act (SCA), for order authorizing prospective and continuous release by phone company of cell-site location records for a targeted cell phone.

Holding: The District Court, Stephen Wm. Smith, United States Magistrate Judge, held that SCA did not authorize continuous monitoring of prospective cell phone location data.

Application denied.

West Headnotes

[1] Telecommunications 372 1475

372 Telecommunications
372X Interception or Disclosure of Electronic Communications; Electronic Surveillance
372X(B) Authorization by Courts or Public Officers
372k1475 k. Carrier's cooperation; pen registers and tracing. Most Cited Cases

Stored Communications Act (SCA) did not authorize continuous monitoring of prospective cell phone location data for a targeted cell phone by means of prospective and continuous release by phone company of cell-site location records; such prospective monitoring of cell site data would convert a cell phone into a "tracking device" within meaning of the Tracking Device Statute, which was subject to warrant requirements that included a showing of probable cause, a duration period, a return to the designated magistrate judge, and notice to the targeted person. U.S.C.A. Const.Amend. 4; 18 U.S.C.A. §§ 2703(d), 3117; Fed.Rules Cr.Proc.Rule 41, 18 U.S.C.A.

[2] Telecommunications 372 1475

372 Telecommunications
372X Interception or Disclosure of Electronic Communications; Electronic Surveillance
372X(B) Authorization by Courts or Public Officers
372k1475 k. Carrier's cooperation; pen registers and tracing. Most Cited Cases

Stored Communications Act (SCA) does not generally empower Government to require providers to create documents.

[3] Federal Civil Procedure 170A 1261

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(A) In General
170Ak1261 k. In general. Most Cited Cases

A limited duty to supplement discovery responses exists only if the party learns that in some material respect the disclosure or response is incomplete or incorrect, but even then the supplementation need not be continuous, but only at appropriate intervals during the discovery period. Fed.Rules Civ.Proc.Rule 26(e)(1)(A), 28 U.S.C.A.

890 *OPINION

STEPHEN WM. SMITH, United States Magistrate Judge.

[1] Recent case law prompts this court to confront yet again an important question of electronic surveillance law: Under what statutory authority is

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

law enforcement permitted to continuously monitor a cell phone's location in (or near) real time?

Background

[2] As part of a drug trafficking investigation, the government has applied for an order under § 2703(d) of the Stored Communications Act (SCA) compelling a phone company to disclose, among other information, cell site data for a target phone "on a continuous basis contemporaneous with" the beginning and end of a call, and if reasonably available, during the call as well.[FN1] In other words, the government seeks to compel continuous and contemporaneous access to cell phone location records not yet created for phone calls not yet made. To be clear, the government does not seek to compel the provider to generate records not ordinarily kept; [FN2] the requested call location data are said to be ***891** ordinary business records. No end-date for the monitoring period is stated.[FN3]

FN1. Sealed Application ¶ 20. The full text of this request reads: "For the Target Device, after receipt and storage, records or other information pertaining to subscriber(s) or customer(s), including the means and source of payment for the service and cell site information, provided to the United States on a continuous basis contemporaneous with (a) the origination of a call from the Target Device or the answer of a call to the Target Device, (b) the termination of the call and (c) if reasonably available, during the progress of the call, but not including the contents of the communications."

FN2. The SCA does not generally empower the government to require providers to create documents. *See In re Application,* 2007 WL 2086663, *1 (S.D.Tex. July 6, 2007).

FN3. Presumably the monitoring would be co-extensive with the 60–day pen register accompanying this request. *See In re Sealing and Non–Disclosure of Pen/Trap/2703(d) Orders,* 562 F.Supp.2d 876, 880 n. 7 (S.D.Tex.2008) (explaining the government's practice in this district of seeking a combined pen/trap and 2703(d) order).

In the past the DOJ has invoked a "hybrid" of several statutes to support its request, but the government's application here relies solely upon the SCA. This court initially denied this part of the government request, but indicated it would consider further briefing on the issue if the government chose to submit it. No such brief was filed.

Analysis

Writing on a mostly clean slate nine years ago, [FN4] this court concluded that prospective monitoring of cell site data converts a cell phone into a "tracking device" under the federal Tracking Device Statute,[FN5] which is subject to the warrant requirements of Rule 41 of the Federal Rules of Criminal Procedure.

FN4. *In re Application,* 396 F.Supp.2d 747 (S.D.Tex.2005). The only other opinion on the topic had been issued a few months earlier by my fellow magistrate judge James Orenstein. *In re Application,* 396 F.Supp.2d 294 (E.D.N.Y.2005).

FN5. 18 U.S.C. § 3117.

Since 2005, other magistrate and district judges have weighed in.[FN6] Some disagreed that a warrant was necessary, holding that such prospective location data is available under the lower, "specific and articulable facts" threshold of the SCA.[FN7] But most published opinions have gone in the other direction, agreeing with this court that the SCA did not apply to real-time monitoring of cell site data. [FN8] The government has yet to appeal these adverse rulings beyond the district level; nevertheless, in this district it routinely requests such authority in its form applications for pen/trap/2703(d) orders. To date no federal appellate court has addressed

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

this particular issue of ongoing surveillance under the SCA.

FN6. For a summary of reported cell site decisions as of June 2010, see *ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary,* 111th Cong. 93 (2010), *available at* ssrn.com/abstract=2173529.

FN7. *See e.g., In re Application,* 632 F.Supp.2d 202 (E.D.N.Y.2008) (Garaufis); *In re Application,* 405 F.Supp.2d 435 (S.D.N.Y.2005) (Gorenstein).

FN8. *See e.g., United States v. Espudo,* 954 F.Supp.2d 1029, 1036–37 (S.D.Cal.2013); *In re Application,* 396 F.Supp.2d at 308–09 (E.D.N.Y.2005) (Orenstein).

Last year a divided Fifth Circuit panel held that orders for historical cell site records under the SCA do not categorically violate the Fourth Amendment. *In re Application of the United States for Historical Cell Site Data,* 724 F.3d 600, 615 (5th Cir.2013). [FN9] The court described its decision as "narrow" and expressly limited to " *historical* cell cite information for specified cell phones at the points at which the user places and terminates a call." [FN10] While the court did assume that historical ***892** cell site records were "covered under the plain text of [SCA] § 2703(c)," [FN11] the opinion was silent about prospective cell site data or continuous monitoring.

FN9. Since that time, two significant cell phone-related decisions have been handed down: *Riley v. California,* —— U.S. ——, 134 S.Ct. 2473, 189 L.Ed.2d 430 (2014) (warrantless search of digital data on a cell phone seized incident to arrest violates Fourth Amendment), and *United States v. Davis,* 754 F.3d 1205 (11th Cir.2014) (obtaining cell site location data without a warrant violates the Fourth Amendment).

FN10. 724 F.3d at 615 (emphasis in original).

FN11. *Id.* at 604. None of the parties before the Fifth Circuit contested the categorization of cell site data as "a record or other information pertaining to a customer or subscriber" within the meaning of the SCA. Nor was the issue raised or decided by the lower court, which confined itself to the constitutional question. *In re Application of United States for Historical Cell Site Data,* 747 F.Supp.2d 827 (S.D.Tex.2010). However, other courts have held that the tracking device exclusion in the ECPA's definition of "electronic communication" removes cell site data from the ambit of the SCA. *See e.g., In re Application,* 2009 WL 159187 (S.D.N.Y., Jan. 13, 2009) (McMahon) (citing cases). Another potentially vexing question is whether the SCA covers cell site information of a phone *user* who is neither "a customer or subscriber." *Cf. In re Application,* 415 F.Supp.2d 663, 666 (S.D.W.Va.2006) (Stanley) (distinguishing between "user" and "subscriber" in the context of a pen register application seeking cell site location data); *see generally* Nathaniel Gleicher, *Neither a Customer Nor a Subscriber Be: Regulating the Release of User Information on the World Wide Web,* 118 YALE L.J. 1945, 1947 (2009) (The SCA "only regulates information pertaining to customers or subscribers of covered information services."). To the extent these questions remain open after the Fifth Circuit's ruling, I leave them for another day.

Even so, given law enforcement persistence in pursuing this authority, it seems appropriate to re-

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

visit our 2005 statutory holding in light of the Fifth Circuit's recent constitutional ruling. The main questions are (1) whether the SCA authorizes ongoing surveillance of cell phone use; (2) whether cell phone tracking is distinguishable from other forms of tracking covered by the Tracking Device Statute and Rule 41; and (3) whether the hybrid theory—a combination of the SCA with other statutes—offers a plausible alternative legal regime for cell phone tracking. The answer to each question is no, for reasons explained below.

1. Distinguishing Historical and Prospective Cell Site Records

The Fifth Circuit's emphasis that its holding was limited to historical cell site information begs the obvious question: what exactly *is* historical cell site information? The SCA does not define the term; in fact, the words "historical" and "cell site" are never used in the SCA. The closest the Fifth Circuit comes to a definition is the following passage: "In the case of such historical cell site information, the Government merely *comes in after the fact* and asks a provider to turn over records the provider has *already created.* " [FN12] In other words, the records sought were historical in the sense that they were created *before* the government's request to the provider.

FN12. 724 F.3d at 612 (emphasis added).

The government's application here exceeds the scope of the one blessed by *Historical Cell Site* in two significant respects. First, the information sought here is "prospective," [FN13] in the sense that law enforcement seeks disclosure of records created in the future, *after* the government's request. Second, and more importantly, the government seeks to impose a *continuing* obligation of disclosure on the provider, thereby enabling law enforcement to monitor the cell phone's call location contemporaneously in (or near) real time. Such monitoring authority is beyond the one-time access apparently contemplated***893** in the Fifth Circuit's decision. Is it also beyond the authority conferred by the SCA?

FN13. Strictly speaking, the term "prospective record" is an oxymoron, because there is no such thing as a record of a future event, at least in ordinary experience. *Cf.* BACK TO THE FUTURE (Universal Pictures 1985). Nevertheless, it will be used here as a convenient shorthand to distinguish those records from the historical records covered by the Fifth Circuit's decision.

Instantaneous storage theory. The government does not think so. In other cases, the government has vigorously challenged the viability of any distinction between "historical" and "prospective" cell site data, arguing that cell phone signaling data becomes a "record" as soon as it is captured and digitally "stored" on the provider's system. This data is historical in one sense and prospective in another: "[T]he same datum that is prospectively created by a disclosure order is a 'record' by the time that it must be turned over to law enforcement." [FN14] Either way, according to the government, cell site data—whenever it is created—is a transaction record subject to production under the SCA.

FN14. Orenstein, 396 F.Supp.2d at 312 (E.D.N.Y.2005) (quoting government's reply brief).

This argument, dubbed the "instantaneous storage" theory by Judge Orenstein in the first reported cell site opinion,[FN15] has found a mixed reception. Some, like Judge Orenstein, have rejected it, citing the SCA's use of the present tense to describe the government's burden of showing that the requested items " *are* relevant and material to an ongoing investigation." [FN16] Other courts have accepted the theory, finding prospective cell site data no different in substance from historical data at the time of its transmission to the government.[FN17]

FN15. *Id.*

FN16. *United States v. Espudo,* 954 F.Supp.2d 1029, 1037 (S.D.Cal.2013); *but*

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

see Dictionary Act, 1 U.S.C. § 1 ("[U]nless the context indicates otherwise, ... words used in the present tense indicate the future as well as the present.").

FN17. *See United States v. Booker,* 2013 WL 2903562, *7 (N.D.Ga. June 13, 2013) ("While this information is 'prospective' in the sense that the records had not yet been created at the time the Order was authorized, it is no different in substance from the historical cell site information ... at the time it is transmitted to the government."); *In re Application,* 632 F.Supp.2d 202, 207 n. 8 (E.D.N.Y.2008) (Garaufis) ("The prospective cell-site information sought by the Government ... becomes a 'historical record' as soon as it is recorded by the provider."); *In re Application,* 460 F.Supp.2d 448, 459 (S.D.N.Y.2006) (Kaplan) ("[T]he information the government requests is, in fact, a stored, historical record because it will be received by the cell phone service provider and stored, if only momentarily, before being forwarded to law enforcement officials."); *In re Application,* 405 F.Supp.2d 435, 444 (S.D.N.Y.2005) (Gorenstein) (nothing in the SCA limits when "information may come into being").

The instantaneous storage argument is not unreasonable, so far as it goes. The SCA does not specify a particular cut-off date for determining which records are to be produced. There are many possibilities: the date of the government's application; the date the order is signed by the judge; the date the order is served on the provider; the date the provider actually produces the records; or a different date specified by the court's order. Absent a clear dividing line to separate present from future data, [FN18] the distinction between historical and prospective cell site data becomes blurred, because digital data can morph into a record within nanoseconds after creation.

FN18. As the poet says, the present is a moving finger that "writes, and having writ, moves on." EDWARD FITZGERALD, THE RUBAIYAT OF OMAR KHAYYAM 71 (William Henry Martin & Sandra Mason, 4th ed. 1879). *See also* TENNESSEE WILLIAMS, THE GLASS MENAGERIE 96 (New Directions 2011) ("The future becomes the present, the present the past."); *cf.* WILLIAM FAULKNER, REQUIEM FOR A NUN 73 (Vintage Books 1950) ("The past is never dead. It's not even past.").

894** ***One-time access vs. continuous monitoring. Even if the government were correct that a 2703(d) order may require the provider to disclose, at some future time, documents not yet in existence when the order is issued, a much larger hurdle remains: Does the SCA impose a *continuing* obligation to disclose customer records, thereby enabling ongoing surveillance, as the government contends? Or is the provider's statutory disclosure obligation satisfied by one-time production of existing records?

The Supreme Court in *Berger v. New York* recognized a fundamental distinction between ongoing electronic surveillance and a one-time search, leading the Court to impose more stringent procedural requirements than those applicable to an ordinary search warrant.[FN19] The focus of the *Berger* opinion was the deficiencies of a state eavesdropping law, but appellate courts have identified similar infirmities with other forms of electronic surveillance: it is intrusive, continuous, indiscriminate, and secret. [FN20] As one respected commentator has elaborated:

FN19. *Berger v. New York,* 388 U.S. 41, 57, 87 S.Ct. 1873, 18 L.Ed.2d 1040 (1967) ("[A]uthorization of eavesdropping for a two-month period is the equivalent of a series of intrusions, searches, and seizures pursuant to a single showing of probable cause.").

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

FN20. *See e.g., United States v. Cuevas–Sanchez,* 821 F.2d 248 (5th Cir.1987) (video surveillance); *United States v. Torres,* 751 F.2d 875, 884–85 (7th Cir.1984) (same).

> The hidden nature of electronic surveillance makes it more likely that an investigation will reveal private information.... Electronic surveillance monitors continuously, increasing the likelihood that people other than the target of the surveillance will have their private information disclosed. Even hardened criminals talk to their mothers and lovers.... Electronic surveillance is "indiscriminate" in the sense that it may obtain information that has no link to criminal activity. Any number of entirely innocent people may either call or be called from a wiretapped phone. Electronic surveillance casts a far wider net than a traditional search for evidence of a crime at a target's home or business.... Finally, electronic surveillance cannot be effective unless it is secret ... Compared to traditional searches, ... law enforcement agents can use electronic surveillance investigations to flout the law without notifying anyone.[FN21]

FN21. Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act,* 56 ALA. L. REV. 9, 18–19 (2004).

[3] Mindful of these dangers, Congress has been attentive to the distinction between ongoing surveillance and one-time access when regulating law enforcement investigative techniques. Continuous search mechanisms like wiretaps, pen registers, and tracking devices are typically hemmed in by duration periods and other prospective features.[FN22] On the other hand, record production regimes have no need for such features because they do not involve ongoing surveillance. An administrative subpoena or a civil discovery request is typically satisfied by a one time production of documents;[FN23] a search warrant***895** for records authorizes one-time access, not repeated searches of the same premises, day after day, week after week, month after month. Real time monitoring of cell site data would mark a radical departure from existing legal regimes for record production. Is there anything in the SCA to support it? The answer is plainly no.[FN24]

FN22. *See In re Application,* 396 F.Supp.2d 747, 760 (S.D.Tex.2005)

FN23. FED.R.CIV.P. 26(e)(1)(A) imposes a limited duty to supplement discovery responses only "if the party learns that in some material respect the disclosure or response is incomplete or incorrect." *See Reed v. Iowa Marine and Repair Corp.,* 16 F.3d 82 (5th Cir.1994). Even then, the supplementation need not be continuous, but only "at appropriate intervals during the discovery period." Advisory Committee Note, 146 F.R.D. at 641; 8A WRIGHT, MILLER & MARCUS, FEDERAL PRACTICE & PROCEDURE § 2049.1 , at 317 (4th ed. 2010).

FN24. Some cases freely concede that the SCA by itself imposes no such obligation, but attempt to derive such an obligation by reading the SCA in combination with the Pen Register Statute, which does authorize prospective surveillance. *See e.g. In re Application,* 460 F.Supp.2d 448, 460 (S.D.N.Y.2006) (Kaplan). This "hybrid" theory is discussed below.

The SCA is part of a comprehensive statute passed in 1986, the Electronic Communications Privacy Act. In separate titles, that law recognizes three different types of ongoing surveillance. Title I amended the Wiretap Act to include interception of electronic communications content. The same title also authorized use of tracking devices outside the district of installation, providing a broad definition of "tracking device" subsequently incorporated into Rule 41.[FN25] Title III authorized pen registers and trap and trace devices. What these schemes have in

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

common are forward-looking mechanisms (e.g. duration period, renewal, reporting, minimization, and sealing) aimed at ongoing activity, not a one-time event.

FN25. See FED. R.CRIM. P 41(a)(2)(E) (" 'Tracking device' has the same meaning set out in 18 U.S.C. 3117."). This definition was part of a 2006 amendment to specify procedures for issuing tracking device warrants.

Title II, referred to as the Stored Communications Act, is different. Modeled after the Right to Financial Privacy Act (RFPA) governing law enforcement access to bank records,[FN26] the SCA is designed to regulate government access to stored electronic communications and transaction records. Just as the RFPA does not authorize law enforcement to monitor bank account transactions as they occur in real time,[FN27] nothing in the SCA imposes a continuing obligation on the provider to disclose account records over time. The SCA has no monitoring periods, no extensions, no minimization requirements, no periodic reporting, no automatic sealing. In short, none of the signature elements of an ongoing surveillance scheme are present.

FN26. S.Rep. No. 99–541, at 3 (1986), 1986 U.S.C.C.A.N. 3555, 3557.

FN27. *See* Susan Freiwald & Sylvain Metille, *Reforming Surveillance Law: The Swiss Model,* 28 BERKELEY TECH. L.J. 1261, 1322–24 (2013) (contrasting the RFPA with Swiss law, which does permit real-time surveillance of bank transac- tions).

The SCA's only nod to prospective data gathering is section 2703(f), which authorizes the government to require a provider "to preserve records and other evidence in its possession pending the issuance of a court order." [FN28] As Judge Orenstein has rightly pointed out,[FN29] this mechanism allows the government to obtain future location records, albeit not contemporaneously, pursuant to a *retrospective* 2703(d) order. By using 2703(f), the government may direct the preservation of records to be disclosed later, in response to a 2703(d) order issued *after* those records are created. This mechanism for one-time access to prospective data is compelling evidence that Congress did not contemplate real-time monitoring of customer data.

FN28. 18 U.S.C. 2703(f).

FN29. *In re Application,* 396 F.Supp.2d 294, 313 (E.D.N.Y.2005).

In sum, as two noted scholars on the ECPA have written, "Congress never intended the Stored Communications Act to ***896** govern ongoing surveillance." [FN30]

FN30. Brief for Center for Democracy and Technology et al., Amicus Curiae Supporting Appellants, *United States v. Councilman,* 418 F.3d 67 (No. 03–1383), 2004 WL 2058257 at *4 (authored by Orin S. Kerr and Peter P. Swire). The case involved an appeal challenging a district court order that emails in momentary electronic storage could be continuously accessed under the SCA as opposed to the Wiretap Act.

2. Tracking Surveillance Under the ECPA

Separate and apart from the SCA's text, a familiar principle of statutory construction compels rejection of the government's surveillance request. As explained above, the SCA is part of a larger statute, the ECPA, and its provisions must be construed in harmony with the rest of that law. *Steve Jackson Games, Inc. v. United States Secret Service,* 36 F.3d 457, 462 (5th Cir.1994) ("[W]hen construing a statute, we do not confine our interpretation to the one portion at issue, but, instead, consider the statute as a whole."). Applying that precept in its first encounter with ECPA, the *Steve Jackson* court found that Congress did not intend

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

substantive overlap between ECPA's various titles, and held that conduct covered by the SCA (Title II) was not simultaneously covered by the wiretap provisions of Title I.[FN31]

FN31. 36 F.3d at 464.

Tracking Device Statute. Similarly here, continuous and contemporaneous monitoring of cell site location data is tantamount to tracking, a form of surveillance Congress separately treated in ECPA.[FN32] As originally drafted, the law expressly paired tracking devices and pen registers in the same title, setting forth procedures for the issuance of court orders allowing their installation and use.[FN33] In its final form, only two provisions dealing with tracking devices were retained: Section 3117(a), which permitted the installation of tracking devices which may move from district to district; and Section 3117(b), which broadly defined tracking device to mean "an electronic or mechanical device which permits the tracking of the movement of a person or object." [FN34] Subsequently, Congress approved amendments to Rule 41 specifying the procedural requirements for a tracking device warrant. Among those requirements are probable cause, a 45–day duration period, return to the designated magistrate judge, and notice to the targeted person.[FN35] Rule ***897** 41(a)(2)(E) expressly incorporates the definition of tracking device from the Tracking Device Statute. Given this detailed regime for location tracking, there is no reason to suspect that Congress ever intended the SCA to open a back door for law enforcement to employ the same surveillance technique under different (and less rigorous) standards.

FN32. 18 U.S.C. § 3117.

FN33. *See* H.R. 3378, 99th Cong., 1st Sess., Title II, § 201. The proposed bill would have required probable cause for a tracking device order, and reasonable cause for a pen register. Legislative history suggests that these tracking devices provisions were later removed due to uncertainty over the proper constitutional standard for tracking device warrants after *U.S. v. Karo,* 468 U.S. 705, 104 S.Ct. 3296, 82 L.Ed.2d 530 (1984). *See Electronic Communications Privacy Act: Hearing on H.R. 3378 Before Subcomm. on Courts, Civil Liberties, and Admin. of Justice of the H. Comm. on the Judiciary,* 99th Cong., 254–274 (1986) (statement of Clifford F. Fishman, Professor of Law, The Catholic University of America School of Law).

FN34. This definition was a shorter version of that originally proposed in H.R. 3378, which read: "an electronic or mechanical device which permits the tracking of the movement of a person or object *in circumstances in which there exists a reasonable expectation of privacy with respect to such tracking.* " H.R. 3378, 99th Cong. § 205 (1985) (emphasis added).

FN35. FED.R.CRIM.P. 41(d)(1), (e)(2)(C), (f)(2). The Advisory Committee Notes observed that the 2006 amendments did not resolve the constitutional issue of the showing required for a tracking warrant, which was left open in *Karo.* The rule simply provides that the magistrate judge must issue the warrant if probable cause is shown, and takes no position whether something less than probable cause would suffice. This court has found no case granting a tracking warrant on less than probable cause, nor has the government ever submitted to this court a Rule 41 tracking warrant application asserting a lesser standard than probable cause.

It might be argued that, in theory, nothing in the SCA prevents an agent from preparing a stack of 2703(d) orders to be served one per hour, day after day, thereby accomplishing the continuous monitoring sought here. Likewise, nothing in the SCA explicitly prohibits an agent from making a similar end run around the Wiretap Act, by lining

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

up a string of § 2703(a) orders for stored emails and serving them seriatim. But, as Professor Kerr has observed, obtaining email content in this way "makes the access the functional equivalent of a wiretap, [and so] should be regulated by the Wiretap Act, not the SCA." [FN36] The same would hold true for serial § 2703(d) orders seeking location data—as the functional equivalent of a tracking warrant, they should be regulated by Rule 41, not the SCA. Careful adherence to the distinction between one-time access and ongoing surveillance will, in the words of Professor Kerr, "ensure that the line between the SCA and the Wiretap Act and Pen Register statute is functional and sensible rather than incoherent and arbitrary." [FN37]

FN36. Orin Kerr, *A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It,* 72 GEO. WASH. L.REV.. 1208, 1232–33 (2004).

FN37. *Id.* at 1233.

Smartphone decision. Some courts have resisted the conclusion that the Tracking Device Statute covers prospective tracking by cell site data. While not disputing that a cell phone is a tracking device in fact,[FN38] these courts contend that a cell phone is not a "tracking device" in law, i.e. the Tracking Device Statute and Rule 41. This conclusion is not derived from the statutory definition of a tracking device, which neatly fits the modern cell phone: "an electronic or mechanical device which permits the tracking of the movement of a person or object." [FN39] Instead, several other justifications are offered, as illustrated by a recent decision, *In re Smartphone Geolocation Data Application,* 977 F.Supp.2d 129 (E.D.N.Y.2013) (Brown).

FN38. One prominent investigative journalist on the technology/privacy beat has described cell phones as "the world's most effective tracking devices, even when they are turned off." JULIA ANGWIN, DRAGNET NATION 141 (2014).

FN39. 18 U.S.C. § 3117(b); FED.R.CRIM.P. 41(a)(2)(E).

First, *Smartphone* argues that the phrase "tracking device" had a plain meaning both prior and extrinsic to the enactment of the ECPA in 1986, [FN40] and points to a Senate Report describing a simple transponder—state of the art tracking technology in 1986, but now obsolete.[FN41] Legislative history has legitimate uses in statutory construction, but this is not one of them. When Congress unambiguously defines a term in the ***898** United States Code, a reviewing court has no power to redefine that term based on extraneous sources of "plain meaning." [FN42] The descriptive passage in the Senate Report could not, and did not purport to, displace the statutory definition of "tracking device" enacted by Congress. As Judge Posner observed in a related context concerning the same report, its description of technology was merely "illustrative, not definitional." [FN43] Nor was Congress unaware that the definition's breadth might encompass cell phones; a prominent telecommunications executive had raised this very possibility in testimony at a committee hearing.[FN44] The ECPA Congress plainly understood the state of tracking technology as it then existed, and, just as plainly, drafted a technology-neutral definition to cover future advances.

FN40. 977 F.Supp.2d at 149.

FN41. S. Rep. 99–541, at 10 (1986), 1986 U.S.C.C.A.N. at 3557. For a discussion of the evolution in tracking technology, see *United States v. Katzin,* 732 F.3d 187, 191–92 (3d Cir.), *reh'g granted,* 2013 WL 7033666 (3d Cir. Dec. 12, 2013).

FN42. *See* 2A N. SINGER & S. SINGER, STATUTES AND STATUTORY CONSTRUCTION § 45.8 at 53 (7th ed. 2014) (noting that popular or received meaning of words in statute may be consulted only "in the absence of a statutory definition").

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

FN43. *United States v. Ramirez,* 112 F.3d 849, 852 (7th Cir.1997).

FN44. *Electronic Communications Privacy Act: Hearing on H.R. 3378 Before Subcomm. on Courts, Civil Liberties, and Admin. of Justice of the H. Comm. on the Judiciary,* 99th Cong. *Hearing on HR 3378,* 99th Cong. 99 (1985). (statement of John W. Stanton, Chairman, Telelocator Network of America, and Executive Vice President, McCaw Communications Co., Inc.).

Next, the *Smartphone* court points to subsection (a) of section 3117 discussing the "installation" of a mobile tracking device, and from this lone word infers that "the statute is aimed at devices installed specifically to track someone or something, as opposed to cell phones which, incidental to their intended purpose, can be tracked or traced." FN45 But an "installation" in our digital age need not entail a physical process, like placing a beeper under a truck bumper; as often as not the term refers to a screen tap or keystroke by which new software is electronically "installed" on digital devices.FN46 Nor is it correct to assume that cell phones have a single intended purpose. As the Supreme Court recently observed in its landmark cell phone search case:

FN45. 977 F.Supp.2d at 150.

FN46. The Pen/Trap Statute repeatedly uses the same word, even though the modern pen register is installed electronically rather than physically. 18 U.S.C. §§ 3121–3125; *see also* Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act,* 69 S. CAL. L. REV. 949, 982–89 (1996) (describing the evolution of the pen register from mechanical device to computer system).

The term "cell phone" is itself misleading shorthand: many of these devices are in fact minicomputers that also have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.FN47

FN47. *Riley v. California,* —— U.S. ——, 134 S.Ct. 2473, 2489, 189 L.Ed.2d 430 (2014).

Or, just as easily, "the world's most effective tracking devices." FN48

FN48. *See supra* note 38.

Finally, the *Smartphone* opinion worries that taking the "tracking device" definition literally would lead to warrants in "illogical and unworkable" circumstances, such as bicycle tire tracks in a muddy field, or an automobile taillight, or the transmitter of a pirate radio station. But these examples are not particularly troublesome,FN49 and far ***899** less so than the consequences of the opinion's own crabbed reading. Accepting *Smartphone's* premise that Congress intended § 3117(b) to refer only to 1986–vintage beepers, not only would cell phones be excluded, but also current tracking technology like GPS devices. And Rule 41's tracking warrant provisions would be similarly obsolete, because they adopt the same definition of "tracking device" that Congress enacted in 1986.FN50

FN49. A bicycle wheel rut may provide evidence that something has passed, but it is no more a "mechanical or electronic device" than a footprint or the wake of a ship. A bicycle and a taillight may be devices, but neither intrinsically reveals "movement" except through direct observation, unlike a beeper or a cell phone. As for the pirate radio, the transmitter revealing its location is functionally indistinguishable from the beeper planted in the container of contraband in *Karo,* and could just as easily qualify as a tracking device.

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

FN50. See FED.R.CRIM.P. 41(a)(2)(E) (" 'Tracking device' has the meaning set out in 18 U.S.C. § 3117(b).").

Smartphone does not address these anomalies, nor the larger question they pose: why, instead of a uniform and coherent legal regime for tracking devices, would Congress prefer a fragmented scheme with varying standards dependent upon the type of technology used? Multiple standards for tracking technologies (most of which rely on radio waves in some form anyway) would seem to accomplish very little for law enforcement,[FN51] other than to generate confusion and opportunity for manipulation, goals unworthy of Congress.

FN51. In this district the government's practice is to invoke at least three different legal mechanisms to track a target: a SCA 2703(d) order for tracking a cell phone by single tower cell data; a "precise location" warrant based on probable cause for tracking a cell phone's precise location by GPS or triangulation; and a Rule 41 tracking warrant for GPS tracking by device other than a cell phone.

These considerations compel me to respectfully disagree with my colleague from New York, and to reject the SCA as stand-alone authority for prospective, continuous, and contemporaneous cell site monitoring. Both in fact and in law, this type of surveillance converts a smartphone into a tracking device, and it is governed by the standards of Rule 41, not the SCA.

3. Hybrid Theory

If the prior analysis is correct, then the SCA is not a proper vehicle to compel continuous disclosure of *any* type of records, including cell site data. In other cases, the government has argued, with limited success, that cell site data is a special category of business records, accessible by a unique combination of statutory authorities. This "hybrid theory" posits that a 1994 law (CALEA) [FN52] implicitly authorized the acquisition of prospective cell site data under the combined authority of the SCA and the Pen/Trap Statute. The most thorough elaboration of this theory to date is the 2005 opinion by Judge Gorenstein.[FN53] A minority of published decisions have accepted the hybrid theory, [FN54] relying almost entirely upon the arguments initially laid out by Judge Gorenstein. Those decisions largely ignore subsequent criticisms of his opinion,[FN55] so the debate has advanced very little in recent years.

FN52. Communications Assistance to Law Enforcement Act, 47 U.S.C. § 1002(a)(2).

FN53. 405 F.Supp.2d 435 (S.D.N.Y.2005).

FN54. *See supra* note 6.

FN55. *See e.g., In re Application,* 441 F.Supp.2d 816 (S.D.Tex.2006).

Unlike the Western Front commanders of a century ago, I will resist the temptation to launch yet another sortie over the same ground slogged by these competing opinions. Instead, a short summary of the main unanswered questions for the hybrid theory will suffice:

***900** • *Missing exception.* How does the hybrid theory escape the SCA's general prohibition against divulging customer records "to any governmental entity"? [FN56] None of the listed exceptions to that prohibition cite the Pen/Trap Statute, an omission that effectively sinks the hybrid theory. [FN57]

FN56. 18 U.S.C. § 2702(a)(3) ("Except as provided in subsection (b) or (c), ... a provider of remote computing service or electronic communications service to the public shall not knowingly divulge a record or other information pertaining to a subscriber or customer of such service ... to any governmental entity.").

FN57. 18 U.S.C. § 2702(c)(1)–(6). Significantly, the prohibition on divulging customer records was first added to the SCA

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

in 2001, the same time the pen/trap definitions were expanded to include "dialing, routing, addressing, and signaling information." 18 U.S.C. § 3127.

• *Paternity.* If the SCA and the Pen/Trap Statute were indeed the parents of a new form of surveillance, why don't they seem to know each other? Neither statute mentions such a symbiotic relationship with the other, nor do their respective legislative histories hint at such a pairing.[FN58]

FN58. 441 F.Supp.2d at 834–35.

• *Birthday.* Even if these statutes had a covert one-night stand, when did the rendezvous occur? The relevant statutory provisions were passed at various times over 15 years. On none of those occasions did anyone in Congress, DOJ, industry, or academia announce (or even notice) that a new breed of electronic surveillance had been spawned. [FN59]

FN59. *Id.* at 835.

• *Congressional clairvoyance.* How did Congress know in 1994, when CALEA was passed, that seven years later the Patriot Act would amend the pen/trap definitions to include signaling information such as cell site data? Until 2001, the Pen/Trap Statute had covered only phone numbers dialed, not call location information.[FN60]

FN60. 396 F.Supp.2d at 765.

• *Hidden elephant.* Why would Congress by a wink and a nod create an alternative legal regime for an investigative technique—mobile tracking devices—already the subject of a specific statute and established procedures? Justice Scalia's memorable phrase is apt: "Congress, we have held, does not alter the fundamental details of a regulatory scheme in vague terms or ancillary provisions—it does not, one might say, hide elephants in mouseholes." [FN61]

FN61. *Whitman v. Am. Trucking Ass'n,* 531 U.S. 457, 468, 121 S.Ct. 903, 149 L.Ed.2d 1 (2001) (refusing to find implicit in ambiguous sections of a statute an authorization that was expressly stated elsewhere).

Lacking persuasive responses to questions such as these, the hybrid theory remains a highly implausible adventure in statutory interpretation.

Conclusion

To summarize, even if the Fifth Circuit's *Historical Cell Site* holding should survive post-*Riley* challenges, nothing in that opinion undermines this court's 2005 ruling that the SCA is not an appropriate vehicle for continuous monitoring of prospective cell phone location data. The same holds true for recent decisions in other districts, like *Smartphone.* Whether or not cell site data is ultimately held worthy of Fourth Amendment protection, the Tracking Device Statute and Rule 41 of the Federal Rules of Criminal Procedure have already struck a fair balance between law enforcement and privacy concerns, and that balance is entitled to ungrudging respect by courts and prosecutors.

***901** Because the government's application seeks to bypass the only legitimate route Congress has mapped out for location tracking surveillance, it is denied.

S.D.Tex.,2014.
In re Order Authorizing Prospective and Continuous Release of Cell Site Location Records
31 F.Supp.3d 889, 60 Communications Reg. (P&F) 1482

END OF DOCUMENT

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

Westlaw.

42 F.Supp.3d 511
(Cite as: 42 F.Supp.3d 511)

C

United States District Court,
S.D. New York.
In the Matter of the APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER PURSUANT TO 18 U.S.C. §§ 2703(C) and 2703(D) DIRECTING AT & T, SPRINT/NEXTEL, T–MOBILE, METRO PCS and VERIZON WIRELESS to Disclose Cell Tower Log Information.

No. M–50.
Signed May 30, 2014.

Background: United States filed petition seeking order pursuant to Stored Communications Act (SCA) requiring cellular telephone service providers to disclose historical cell site data from cell towers located near specified address for particular time period.

Holdings: The District Court, James C. Francis IV, United States Magistrate Judge, held that:
(1) Fourth Amendment did not preclude government from requiring providers to disclose historical cell site data, and
(2) United States was not required to obtain warrant prior to issuance of order.

Ordered accordingly.

West Headnotes

[1] Searches and Seizures 349 28

349 Searches and Seizures
349I In General
349k25 Persons, Places and Things Protected
349k28 k. Abandoned, surrendered, or disclaimed items. Most Cited Cases

For Fourth Amendment purposes, person has no legitimate expectation of privacy in information he voluntarily turns over to third parties. U.S.C.A. Const.Amend. 4.

[2] Telecommunications 372 1475

372 Telecommunications
372X Interception or Disclosure of Electronic Communications; Electronic Surveillance
372X(B) Authorization by Courts or Public Officers
372k1475 k. Carrier's cooperation; pen registers and tracing. Most Cited Cases

Cell phone users had no reasonable expectation of privacy in cell site information communicated for purpose of making and receiving calls in ordinary course of provision of cellular phone service, and thus Fourth Amendment did not preclude government from requiring cellular telephone service providers to disclose historical cell site data from cell towers located near specified address for particular time period; it was common knowledge that communications companies regularly collected and maintained all types of non-content information regarding cell-phone communications, including cell-site tower data, for cell phones for which they provided service. U.S.C.A. Const.Amend. 4.

[3] Searches and Seizures 349 25.1

349 Searches and Seizures
349I In General
349k25 Persons, Places and Things Protected
349k25.1 k. In general. Most Cited Cases
(Formerly 349k192.1)

Searches and seizures inside home without warrant are presumptively unreasonable. U.S.C.A. Const.Amend. 4.

[4] Searches and Seizures 349 33

349 Searches and Seizures
349I In General
349k31 Persons Subject to Limitations; Governmental Involvement
349k33 k. Private persons. Most Cited Cases

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

Voluntary disclosure doctrine, pursuant to which Fourth Amendment does not prohibit obtaining of information revealed to third party and conveyed by him to government authorities, applies even where disclosures are made from protected space of home. U.S.C.A. Const.Amend. 4.

[5] Telecommunications 372 1475

372 Telecommunications
372X Interception or Disclosure of Electronic Communications; Electronic Surveillance
372X(B) Authorization by Courts or Public Officers
372k1475 k. Carrier's cooperation; pen registers and tracing. Most Cited Cases

United States would not be required to obtain warrant prior to issuance of order pursuant to Stored Communications Act (SCA) requiring cellular telephone service providers to disclose historical cell site data from cell towers located near specified address for particular time period, where government only sought to determine numbers that were used at multiple locations, as well as numbers that matched those that law enforcement had learned were associated with certain persons under investigation, and there was no possibility that widespread tracking of locations of individuals could ensue if application was granted. U.S.C.A. Const.Amend. 4; 18 U.S.C.A. § 2703(d).

***512** JAMES C. FRANCIS IV, United States Magistrate Judge.

The United States of America (the "Government") seeks an order pursuant to the Stored Communications Act ("SCA") requiring various cellular telephone service providers to disclose historical cell site data from cell towers located near a specified New York City address for a particular four-and-one-half hour time period. I asked that the Government provide me with a memorandum supporting its position that the requested information was obtainable, and further invited the New York Civil Liberties Union and American Civil Liberties Union (collectively, the "ACLU") to submit their views on the question as *amici curiae.*[FN1]

FN1. I am grateful to the ACLU for its thorough and helpful submission, which was of considerable assistance in resolving the Government's application. The ACLU's work is especially impressive, given that counsel were unable to review the actual application at issue, which is not publicly available.

Information Sought

The Government explains that there are two ways to obtain historical cell site data. In the typical case, the Government requests information connected to a particular cell phone number and (if the application is granted) retrieves "a list of all calls to and from the telephone number, along with the locations and sectors (or 'faces') of the cell towers through which each call originated and terminated," thus providing information helpful in determining the "approximate locations of cellular telephones during the sending and receipt of calls." (Letter of Jason A. Masimore dated May 7, 2014 ("Masimore 5/7/14 Letter") at 1–2).

This application, on the other hand, centers not on a particular cell phone number, but on the cell towers in the area of an identified location. The information sought "consists of a list for a particular cell tower from the specified date and time period of the subscribers' cellular telephone numbers connecting to that tower, along with the times of the calls and the digits dialed or the call numbers of the telephones calling into the subscribers' cellular telephones connecting through the tower," information that can help establish "that the listed cellular telephones were somewhere in the vicinity of that particular cell tower during that time period." (Masimore 5/7/14 Letter at 2). The information gathered here—specifically, the telephone numbers that connected to the cell towers during the pertinent time period—will be compared to similar information gathered from other locations relevant to

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

the investigation to determine numbers that were used at multiple locations, as well as numbers that match those that law enforcement has learned are associated with certain persons under investigation for the series of crimes at issue.

Discussion

A. *Authorization under the Stored Communications Act*

The SCA permits the Government to obtain an order requiring "a provider of ***513** electronic communication service ... to disclose a record or other information pertaining to a subscriber or customer of such service (not including the contents of communications)" when the Government offers "specific and articulable facts showing that there are reasonable grounds to believe that the ... records ... sought[ ] are relevant and material to an ongoing criminal investigation." 18 U.S.C. §§ 2703(c)(1), (d).

The ACLU argues that a cell tower dump is not authorized under the statute because "Congress phrased the disclosure provision of § 2703(c) in the singular: ' *a* subscriber or customer of such service.' " (Letter of Nathan Freed Wessler, *et al.* dated May 20, 2014 ("Wessler 5/20/14 Letter"), at 7). Although this argument has some intuitive appeal, it is easily refuted: "[i]n determining the meaning of any Act of Congress, unless the context indicates otherwise[,] words importing the singular include and apply to several persons, parties, or things." 1 U.S.C. § 1. The ACLU argues that the "use of the singular article ... is part of Congress's comprehensive scheme to strictly limit permissible government intrusions into the privacy of cell phone users." (Wessler 5/20/14 Letter at 8). However, this generalized "context" is insufficient to overrule "the default rule of statutory construction that words importing the singular include the plural meaning." *Carrow v. Merit Systems Protection Board,* 564 F.3d 1359, 1366 (Fed.Cir.2009) (examining legislative history for indication that statutory term "an Executive agency" was intended to preclude plural meaning).[FN2]

FN2. The ACLU also contends that the view "that the government may obtain an order under § 2703(c) *about* a subscriber of service A *from* service B" ignores the statutory text authorizing disclosure of a record " 'pertaining to a subscriber or customer of *such* service.' " (Wessler 5/20/14 Letter at 8 (quoting 18 U.S.C. 2703(c))). Under the order sought, the only information that service A could provide about a service B subscriber is that subscriber's phone number, either because a service A subscriber dialed it or because a service B subscriber dialed a service A phone number. This is the same information available from a conventional pen register, which captures outgoing "dialing, routing, addressing, or signaling information" from a cell phone or other electronic or wire communication device, or a trap and trace device, which captures "incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication." 18 U.S.C. § 3127(a)(3)-(4).

The ACLU further contends that even if the SCA as a whole does not prohibit cell tower dumps, they can never be obtained under § 2703(d): the Government "cannot possibly meet th[e] [statute's] standard because it seeks vast quantities of irrelevant and immaterial—yet extraordinarily sensitive—information about hundreds or thousands of wholly innocent parties." (Wessler 5/20/14 Letter at 8). Noting that courts have described § 2703(d)'s standard as akin to "reasonable suspicion," *In re Application of the United States of America for Historical Cell Site Data,* 724 F.3d 600, 616 (5th Cir.2013) (Dennis, J. dissenting) (hereinafter *In re Fifth Circuit Application*) (denominating the standard "reasonable suspicion"); *In re Application of*

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

the United States of America for an Order Pursuant to 18 U.S.C. § 2703(D), 707 F.3d 283, 287 (4th Cir.2013) ("This is essentially a reasonable suspicion standard."), the ACLU cites cases regarding so-called *Terry* stops to support its argument that "the 'reasonable suspicion' standard requires an evaluation of the facts pertinent to the individual being searched or seized." (Wessler 5/20/14 Letter at 9 (citing *Ybarra v. Illinois,* 444 U.S. 85, 94, 100 S.Ct. 338, 62 L.Ed.2d 238 (1979))).

***514** While clever, this argument ignores the actual language of the statute, which does not use the phrase "reasonable suspicion," but requires only "specific and articulable facts showing that there are reasonable grounds to believe that the ... records ... sought[ ] are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). Thus there is no indication in the text (or in the legislative history) that Congress intended to import the standards guiding *Terry* stops into the SCA. Nor is it likely that the courts using this shorthand intended to graft onto the statutory language the doctrine arising out of the limited investigation stop cases. A better interpretation is that, when used in connection with the SCA, the phrase merely indicates that the standard "is a lesser one than probable cause." *In re Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government,* 620 F.3d 304, 313 (3d Cir.2010) (hereinafter *In re Third Circuit Application*).

Accordingly, the type of order sought here is authorized by the statute.

B. *The Warrant Requirement*

The Fourth Amendment can, of course, trump statutory authorization either by requiring the Government to show probable cause to obtain the information sought here or, perhaps, by prohibiting such searches altogether. That amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const., amend. IV. It requires law enforcement to obtain a warrant before executing a search, thus "interpos[ing] a magistrate between the citizen and the police ... to ensure that an objective mind might weigh the need to invade that privacy in order to enforce the law." *United States v. Voustianiouk,* 685 F.3d 206, 211 (2d Cir.2012) (internal quotation marks omitted). Justice Harlan's concurrence in *Katz v. United States,* 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967), a touchstone of Fourth Amendment jurisprudence, formulated a "two-fold requirement" for determining whether government action constitutes a search: "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.' " *Id.* at 361, 88 S.Ct. 507 (Harlan, J. concurring); *see also United States v. Jones,* ——U.S. ——, ——, 132 S.Ct. 945, 950, 181 L.Ed.2d 911 (2012) ("Our [ ] cases have applied the analysis of Justice Harlan's concurrence in [*Katz*], which said that a violation occurs when government officers violate a person's 'reasonable expectation of privacy.' " (quoting *Katz,* 389 U.S. at 360, 88 S.Ct. 507 (Harlan, J. concurring))). The ACLU argues that there is a reasonable expectation of privacy in cell tower records from which individuals' location can be determined.[FN3] (Wessler 5/20/14 Letter at 13).

FN3. The Government asserts that the records it seeks will enable it to determine "that the listed cellular telephones were somewhere in the vicinity of that particular cell tower during that time period" (Masimore 5/7/14 Letter at 2), and it appears that the information will allow the Government only to determine whether a particular subscriber's cell phone is in proximity to the subject cell tower and to identify the sector of the tower to which the cell phone connected. The Government indicates that it will not be using additional tools to further pinpoint location. (Letter of Jason A. Masimore dated May 23, 2014, at 2 n. 1); *see In re Smartphone Geolocation Data Application,* 977 F.Supp.2d 129, 137

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

(E.D.N.Y.2013) ("Cell-site location is arguably the least precise of the three methods currently used, though that precision can be substantially enhanced through triangulation of signals from multiple towers."); *In re Application of the United States of America for an Order Pursuant to 18 U.S.C. § 2703(d) Directing Providers to Provide Historical Cell Site Locations Records,* 930 F.Supp.2d 698, 701 (S.D.Tex.2012) (hereinafter *In re S.D. Tex. Application*) ("[R]efinements in location technology regarding cell site information" actually "enables [the Government] to plot with great precision where the cell phone user has been during a given time peri- od.").

***515** 1. *"Dragnet Type" Surveillance*

In *United States v. Knotts,* 460 U.S. 276, 103 S.Ct. 1081, 75 L.Ed.2d 55 (1983), the Supreme Court approved the warrantless use of a beeper to track a vehicle's movements on public roads. *Id.* at 281–82, 103 S.Ct. 1081. Noting the respondent's fear that the holding could usher in " 'twenty-four hour surveillance of any citizen of this country ... without judicial knowledge or supervision,' " the Court observed that, "if such dragnet type law enforcement practices ... should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable." *Id.* at 283–84, 103 S.Ct. 1081. The ACLU contends that cell tower dumps violate reasonable expectations of privacy "because they involve just th[is] sort of 'dragnet type' surveillance of hundreds or thousands of innocent people." (Wessler 5/20/14 Letter at 13).

I cannot agree that the Government's application here raises the spectre of "wholesale surveillance" suggested in *Knotts* and some of the cases following it. Such concerns center on the possibility of the Government tracking an individual's (or a number of individuals') every movement over a period of time. *See Knotts,* 460 U.S. at 284, 103 S.Ct. 1081 (mentioning "twenty-four hour surveillance of any citizen of this country"); *United States v. Katzin,* 732 F.3d 187, 191–92, 205 (3d Cir.2013) (holding warrantless GPS tracking of vehicle for several days generating "highly accurate record of the tracker's whereabouts throughout its period of operation" unjustified), *vacated on grant of reh'g en banc,* 2013 WL 7033666 (3d Cir. Dec. 12, 2013); *United States v. Pineda–Moreno,* 617 F.3d 1120, 1125–26 (9th Cir.2010) (Kozinski, C.J., dissenting from denial of rehearing en banc) (equating GPS tracking device that continuously recorded car's location with "dragnet-type law enforcement practices" of *Knotts* and worrying that "[b]y tracking and recording the movements of millions of individuals the government can use computers to detect patterns and develop suspicions"); *United States v. Marquez,* 605 F.3d 604, 610 (8th Cir.2010) ("It is imaginable that a police unit could undertake 'wholesale surveillance' by attaching [electronic tracking] devices to thousands of random cars and then analyzing the volumes of data produced for suspicious patterns of activity."); *United States v. Garcia,* 474 F.3d 994, 998 (7th Cir.2007) ("The new technologies enable, as the old (because of expense) do not, wholesale surveillance. One can imagine the police affixing GPS tracking devices to thousands of cars at random, recovering the devices, and using digital search techniques to identify suspicious driving patterns."). That is not at issue here. Rather, the Government seeks to retrieve phone numbers used during a particular time period in a particular area to be cross-referenced with data generated from other areas relevant to the investigation during other relevant time periods." [FN4] There is no ***516** possibility that widespread tracking of the locations of individuals could ensue if the application is granted. *See In re Application of the United States of America for an Order Authorizing the Release of Historical Cell–Site Information,* 809 F.Supp.2d 113, 122, 126–27 (E.D.N.Y.2011) (hereinafter *In re E.D.N.Y. Application*) (holding that " *cumulative* cell-site—location records" require a warrant because of the significant "governmental intrusion into inform-

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

ation which is objectively recognized as highly private"—that is, the Government's "surveillance of [one's] movements over a considerable time period"); *cf. Commonwealth v. Augustine,* 467 Mass. 230, 254–55, 4 N.E.3d 846 (2014) ("[T]he tracking of the defendant's movements ... for two weeks was more than sufficient to intrude upon the defendant's expectation of privacy safeguarded [by the Massachusetts Constitution].").

FN4. The ACLU supposes an extremely broad search, which it characterizes as a "fishing expedition." (Wessler 5/20/14 Letter at 14). However, as explained above, the order sought is more like what the ACLU calls a "typical tower dump" intended to cross-reference numbers acquired with numbers that the Government has determined to be relevant in its investigation. (Wessler 5/20/14 Letter at 14). The ACLU recognizes that this type of request does not raise the "especially acute constitutional concerns" that would have been implicated by its more expansive hypothetical search. (Wessler 5/20/14 Letter at 14).

2. *The Voluntary Disclosure Doctrine*

In *United States v. Miller,* 425 U.S. 435, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976), the petitioner sought to suppress certain documents connected with his bank accounts, which had been obtained without a warrant. *Id.* at 437–38, 96 S.Ct. 1619. The Supreme Court held that the documents did not fall "within a protected zone of privacy," and therefore the Fourth Amendment was not implicated in law enforcement's acquisition of them. *Id.* at 440, 96 S.Ct. 1619. It noted that the information contained in the records, which included checks, financial statements, and deposit slips, was "voluntarily conveyed to the banks." *Id.* at 442, 96 S.Ct. 1619.

> The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. This Court 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 and the confidence placed in the third party will not be betrayed.

Id. at 443, 96 S.Ct. 1619 (internal citations omitted).

[1] Three years later, in *Smith v. Maryland,* 442 U.S. 735, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979) the Court applied the reasoning of *Miller* and the cases on which it relied to "the question whether the installation and use of a pen register constitutes a 'search' within the meaning of the Fourth Amendment." *Id.* at 736, 99 S.Ct. 2577 (footnote omitted). It held that the petitioner had no "legitimate expectation of privacy regarding the numbers he dialed on his phone" 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 742–43, 99 S.Ct. 2577. This was true even though the defendant had " 'us[ed] the telephone *in his house* to the exclusion of all others,' " because "[a]lthough [his] conduct may have been calculated to keep the contents of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed." *Id.* (first alteration in original) (emphasis omitted). *Smith* thus reaffirmed what the Court has consistently held: "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Id.* at 743– ***517** 44, 99 S.Ct. 2577. *Smith* and *Miller* remain the "prevailing case law." *United States v. Pascual,* 502 Fed.Appx. 75, 80 & n. 6 (2d Cir.2012).

[2] Many courts have held that this voluntary disclosure doctrine (also known as the "third-party disclosure doctrine") compels the conclusion that the Government's acquisition of cell site location

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

data is not a "search" within the meaning of the Fourth Amendment. *See, e.g., United States v. Caraballo,* 963 F.Supp.2d 341, 359–60 (D.Vt.2013) (" *Smith* and *Miller* thus support a conclusion that a cell phone user generally has no reasonable expectation of privacy in cell site information communicated for the purpose of making and receiving calls in the ordinary course of the provision of cellular phone service."); *In re Smartphone Geolocation Data Application,* 977 F.Supp.2d at 146 ("Under existing law [ ] a user does not have a reasonable expectation of privacy as to geolocation data."); *United States v. Madison,* No. 11–60285–CR, 2012 WL 3095357, at *9 (S.D.Fla. July 30, 2012) ("[T]he third-party disclosure doctrine relied upon by *Smith* requires the finding that society is not prepared to recognize as legitimate any subjective expectation that Defendant might have had in the cell-tower location data for his cell-phone usage."); *United States v. Graham,* 846 F.Supp.2d 384, 389, 400 (D.Md.2012) ("Based on clear Supreme Court ... precedent, this Court finds the third-party doctrine applicable to historical cell site location information."). These courts have noted that "[a]s part of the ordinary course of business, cellular phone companies collect information that identifies the cell towers through which a person's calls are routed." *Graham,* 846 F.Supp.2d at 400. Contrary to the ACLU's contention (Wessler 5/20/14 Letter at 17), this is information that cell phone users voluntarily disclose—"[a]fter all, if the phone company could not locate a particular cell phone, there would be no means to route a call to that device, and the phone simply would not work." *In re Smartphone Geolocation Data Application,* 977 F.Supp.2d at 146; *see also Madison,* 2012 WL 3095357, at *8 ("All cell users are aware that cell telephones do not work when they are outside the range of the communication company's cell-tower network.... Thus, ... cell-phone users have knowledge that when they place or receive calls, they, through their cell phones, are transmitting signals to the nearest cell tower, and, thus, to their communications service providers."). And it is "common knowledge that communications companies regularly collect and maintain all types of non-content information regarding cell-phone communications, including cell-site tower data, for cell phones for which they provide service." *Madison,* 2012 WL 3095357, at *8; *see also In re Fifth Circuit Application,* 724 F.3d at 611–12, 613–14 (noting that "[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" and that users voluntarily convey information about their location when they place a call, even if they do not "directly inform [the] service provider of the location of the nearest cell phone tower"); *In re Smartphone Geolocation Data Application,* 977 F.Supp.2d at 137–42 (discussing widespread public knowledge of ability and practice of cell phone service providers to track customers' locations); *In re E.D.N.Y. Application,* 809 F.Supp.2d at 121 (calling it a "doubtful proposition" that cell phone users are unaware that location data is collected and stored by service providers). *But see In re Third Circuit Application,* 620 F.3d at 317 ("[I]t is unlikely that cell phone customers are aware that their cell phone providers *collect* and ***518** store historical location information."). I agree that *Smith* and *Miller* dictate the outcome here, where the subscribers are aware that use of their cell phones necessitates disclosure of the information sought.

The ACLU cites *United States v. Warshak,* 631 F.3d 266 (6th Cir.2010) for the proposition that "the fact that cell phone location information is handled by a third party is not dispositive." (Wessler 5/20/14 Letter at 18). But *Warshak* dealt with the disclosure of the *contents* of a defendant's e-mails. *Warshak,* 631 F.3d at 283. And the Court in *Smith* noted an exception to the voluntary disclosure doctrine for the content of communications that are routed through a third party. *Smith,* 442 U.S. at 741, 99 S.Ct. 2577; *see also Madison,* 2012 WL 3095357, at *9 n. 11 (noting "content exception to the third-party-disclosure doctrine as it relates to communications providers"); *In re E.D.N.Y. Application,* 809 F.Supp.2d at 122–25

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

(discussing "content exception [ ] incorporated, by dicta, into Fourth Amendment telephonic communications case law in *Smith* "). *Warshak* is therefore inapposite here, where the Government does not seek the contents of communications.

3. *Constitutionally Protected Spaces*

To be sure, much of the information the Government seeks will have been generated by people using their cell phones in their own homes. The ACLU argues that the cell tower dump therefore constitutes a Fourth Amendment search of "constitutionally protected spaces." (Wessler 5/20/14 Letter at 14–15).

[3] The Supreme Court has "not deviated from th[e] basic Fourth Amendment principle" that "[s]earches and seizures inside a home without a warrant are presumptively unreasonable." *United States v. Karo,* 468 U.S. 705, 714–15, 104 S.Ct. 3296, 82 L.Ed.2d 530 (1984). Accordingly, the Court held in *Karo* that law enforcement monitoring of a beeper on a can of ether while the can was in a private residence was a Fourth Amendment search requiring a warrant because it revealed "critical fact[s] about the interior of the premises" that the Government could not have obtained through visual surveillance. *Id.* at 715, 104 S.Ct. 3296. Similarly, in *Kyllo v. United States,* 533 U.S. 27, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001), the warrantless use of a "thermal-imaging device aimed at a private home from a public street" was held to be unconstitutional because "obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area constitutes a search." *Id.* at 29, 34, 121 S.Ct. 2038 (citation omitted) (internal quotation marks omitted). Thus, it is certainly correct that the Supreme Court has repeatedly recognized that government intrusion into the home without a warrant intrudes on a reasonable expectation of privacy.

[4] Nonetheless, *Karo* and *Kyllo* do not alter the analysis here. As *Smith* makes clear, the voluntary disclosure doctrine applies even where the disclosures are made from the protected space of the home. *Smith,* 442 U.S. at 743, 99 S.Ct. 2577 ("But the site of the call is immaterial for the purposes of analysis in this case.... The fact that he dialed the number on his home phone rather than on some other phone could make no conceivable difference...."); *see also In re Smartphone Geolocation Data Application,* 977 F.Supp.2d at 143–45 (finding location of origination of communication "not ... useful" in deciding whether to issue authorization for cell site data and therefore applying voluntary disclosure doctrine); *Caraballo,* 963 F.Supp.2d at 356 (stating, in case regarding Government ***519** "pinging" target cell phone, that "[a] Fourth Amendment analysis entirely dependent upon the fortuity of a criminal defendant entering his or her own home during the pinging process is likely to prove [ ] unworkable...."). *But see In re Application of the United States of America for Historical Cell Site Data,* 747 F.Supp.2d 827, 835–37 (S.D.Tex.2010) (denying request for historical cell site data based, in part, on location of phone in non-public places), *vacated by In re Fifth Circuit Application,* 724 F.3d at 615.

4. *Discretion*

Finally, the ACLU argues that, even if the SCA and the Constitution permit issuance of the requested order on a less stringent showing than probable cause, it is within my discretion to require that the Government meet the higher standard. (Wessler 5/20/14 Letter at 10–12). I agree that a judge has such discretion.

The operative statutory language states that "a court order for disclosure ... may be issued by any court that is a court of competent jurisdiction and shall issue only if" the standard is met. 18 U.S.C. § 2703(d). The Third Circuit has observed that the phrase "may be issued" is "the language of permission, rather than mandate." *In re Third Circuit Application,* 620 F.3d at 315. Additionally, the direction that an order "shall issue only if" the standard is met "describe[s] a necessary condition, not a suf-

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

ficient condition." *Id.* at 316 (internal quotation marks omitted). *But see In re Fifth Circuit Application,* 724 F.3d at 606–08 (rejecting Third Circuit's interpretation). If Congress meant otherwise, it could have excised the word "only" from the statute; however, "the statute does contain the word 'only' and neither [I] nor the Government is free to rewrite it." *In re Third Circuit Application,* 620 F.3d at 315.

Under the voluntary disclosure doctrine, an individual's privacy interest in shared information is attenuated but not necessarily eviscerated altogether. *See, e.g., Smith,* 442 U.S. at 741, 99 S.Ct. 2577 (voluntary disclosure doctrine does not extend to contents of communications). Certain searches by the Government of information that is voluntarily but selectively disclosed may be so invasive that it would be prudent to require a showing of probable cause. With emerging and as-yet-unknown technologies, such searches are likely to become easier, cheaper, and more prevalent; it may, then, be time to scrutinize the voluntary disclosure doctrine more closely. *See Jones,* ——U.S. at ——, 132 S.Ct. at 957 (Sotomayor, J. concurring) ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.").

[5] Nevertheless, I will not require a warrant here because the information voluntarily disclosed—the telephone numbers associated with communications in a general location—does not implicate privacy interests to the same degree as, for example, the content of those communications. I will, however, require the Government to submit an amended application that (1) provides more specific justification for the time period for which the records will be gathered and (2) outlines a protocol to address how the Government will handle the private information of innocent third-parties whose data is retrieved. *See In re S.D. Tex. Application,* 930 F.Supp.2d at 702 ("[I]n order to receive such data, the Government at a minimum should have a protocol to address how to handle this sensitive private information."); *see also In the Matters of the Search of Cellular Telephone Towers,* 945 F.Supp.2d 769, 771 (S.D.Tex.2013) (issuing warrant for cell ***520** tower records but requiring, among other things, that "any and all original records and copies ... determined not to be relevant to the ... investigation" be returned to cell service providers).

Conclusion

The Government is directed to submit, within seven days of the date of this order, an amended application that (1) re-evaluates and justifies the time period for which the cell tower records are requested and (2) provides a plan to address the protection of private information of innocent third-parties whose data is disclosed to the Government. If that information satisfies me that the privacy rights of subscribers are adequately protected, the requested order will issue.

SO ORDERED.

S.D.N.Y.,2014.
In re Application of the U.S.A. for an Order Pursuant to 18 U.S.C. 2703(c), 2703(d) Directing AT & T, Sprint/Nextel, T-Mobile, Metro PCS, Verizon Wireless
42 F.Supp.3d 511

END OF DOCUMENT

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

[Editor's note: portions of the following opinion not related to use of a cell-site simulator have been omitted as noted.]

United States District Court,
D. Arizona.
UNITED STATES of America, Plaintiff,
v.
Daniel David RIGMAIDEN, Defendant.

No. CR 08–814–PHX–DGC.
May 8, 2013.

ORDER

DAVID G. CAMPBELL, District Judge.

***1** The government has indicted Defendant Daniel Rigmaiden on 74 counts of mail and wire fraud, aggravated identity theft, and conspiracy. Doc. 200. The charges arise from a scheme to obtain fraudulent tax refunds by filing electronic tax returns in the names of hundreds of deceased persons and third parties. The government located and arrested Defendant, in part, by tracking the location of an aircard connected to a laptop computer that allegedly was used to perpetrate the fraudulent scheme. Defendant argues that the technology and methods used to locate the aircard violated his Fourth Amendment rights. He also argues that the government violated the Fourth Amendment by obtaining various documents and data through Court orders, relying on warrants that lacked particularity and probable cause, and exceeding the scope of the warrants.

Defendant has filed a motion to suppress and many related motions and memoranda.[FN1] Although Defendant Rigmaiden represents himself and has no formal training in the law, his motions and memoranda are thoroughly researched and factually detailed. The Court and its staff have read hundreds of pages of briefing and exhibits, and oral argument was held on March 28, 2013. After thorough consideration of the parties' arguments, Defendant's motion to suppress will be denied.

FN1. These include Defendant's Motion to Suppress (Doc. 824); Supplement Memorandum re 4th Amendment Violations (Doc. 830–1); Supplement Memorandum re Destruction of Evidence (Doc. 830–2); Motion for Order Requiring Government to Comply with Data Deletion Requirements (Doc. 847); Motion for Discovery re: Digital Evidence Search (Doc. 890); Motion for Leave to Place Additional Evidence on the Record (Doc. 897); Motion for Leave to File First Supplement to Motion for Order Requiring Government to Comply with Data Deletion Requirements (Doc. 926); Motion to Suppress All Digital Data Evidence as a Sanction for Failure to Preserve Evidence (Doc. 931); Motion for Sanctions for Discovery Violations re: Digital Evidence Search (Doc. 932); Motion to Amend/Correct (Doc. 934).

I. Background.

The government alleges that in 2007 and 2008, using the identities of deceased and living individuals, including their social security numbers, Defendant e-filed more than 1,200 fraudulent tax returns claiming more than $3,000,000 in tax refunds. Doc. 873 at 3.[FN2] In reliance on the fraudulent filings, the IRS deposited hundreds of thousands of dollars in bank accounts and debit cards maintained by Defendant and his co-conspirators. This order will describe only the most relevant portions of the year-long investigation that led to Defendant's arrest.

FN2. Citations in this order are to page numbers affixed to the top of documents by the Court's CMECF system, not to pages numbers in the documents themselves.

In June 2007, an IRS e-file provider notified the IRS that a large volume of tax returns had been filed

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

through its website by an unknown person using an automated process. IRS agents subpoenaed the subscriber information for one of the IP addresses from which a return was filed and learned that the IP address was associated with a Verizon Wireless broadband access card provided to a Travis Rupard in San Jose, California. This access card, which was used to make a wireless connection between a computer and the Internet, became a key focus in the investigation. The access card will be referred to in this order as "the aircard."

In March of 2008, the IRS Fraud Detection Center in Austin, Texas ("AFDC") identified a number of recently-filed fraudulent tax returns which directed that refunds be sent to various debit cards connected with a single Meridian Bank account. Doc. 873 at 9–10. IRS agents subpoenaed subscriber information for these fraudulent filings and found that some of the IP addresses ultimately traced back to the Verizon aircard and the related account maintained by Travis Rupard. Investigators also found the name "Travis Rupard" to be a false identity—the aircard account subscriber information provided by "Travis Rupard" listed a non-existent address, and the California driver's license number provided by "Travis Rupard" was in fact assigned to a female with a different name.

***2** On April 15, 2008, as a result of various investigative efforts, agents executed a search warrant on a co-conspirator's computer and obtained e-mail correspondence between the coconspirator and an individual known to the co-conspirator as "the Hacker." The coconspirator had never personally met the Hacker, but had communicated with the Hacker by encrypted e-mail and had, at the Hacker's direction, established bank accounts to receive refunds from the fraudulent tax return scheme. Following his arrest, the co-conspirator agreed to work with the government as a confidential informant, and is referred to by the government as "CI–2."

On April 17, 2008, the Hacker contacted CI–2 through a secure e-mail account and provided detailed encrypted instructions for delivering $68,000 in proceeds from the taxrefund scheme to the Hacker. The Hacker directed CI–2 to wash the $68,000 of cash in lantern fuel to avoid drug detection dogs, double vacuum seal the currency, place the sealed cash inside a stuffed animal, and mail the animal in a gift-wrapped box with a birthday card addressed to a dying child. The Hacker instructed CI–2 to send the package to "Patrick Stout" at a FedEx/Kinko's store in Palo Alto, California. Investigators found "Patrick Stout" to be another false identity—it was traced to a post office box in Sacramento, California, opened through the use of a fraudulent California driver's license bearing a number assigned to yet another female with a different name.

The package containing $68,000 in currency was delivered to the FedEx/Kinko's store on May 6, 2008. The next day, at approximately 5:00 a.m., a white male wearing a dark jacket and hood entered the store, presented identification in the name of Patrick Stout, and retrieved the package. The individual opened the package outside the store, removed the cash, discarded the shipping box, and then proceeded to a nearby train station where he eluded agents who had him under surveillance. The Hacker e-mailed CI–2 on May 8, 2008, and confirmed receipt of the money.

On June 25, 2008, the government obtained Verizon transaction logs for the aircard and compared them with transaction information for other activities of the Hacker, including his e-mail communications with CI–2. The IP addresses accessed by the aircard and the date/time stamps shown for its connections were consistent with activities of the Hacker, suggesting that the Hacker was in fact using the Travis Rupard aircard. In addition, the AFDC reported that more than 100 fraudulent tax refund claims were filed between May 22 and June 5, 2008. Doc. 873 at 16–23. The times when these false filings were made corresponded with activity on the Travis Rupard aircard. Although the false filings were made from different IP

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

addresses, investigators believed the Hacker was using the aircard to access proxy computers or other anonymous tools on the Internet to mask his IP address. Consistent with this theory, the Hacker had stated in an April 15, 2008 e-mail to CI–2 that he used a different IP address for each fraudulent tax return in order to avoid detection. *Id.* at 26. Through these and other investigative efforts, investigators became convinced that the Hacker was using the Travis Rupard aircard and that locating the aircard would lead them to the Hacker.

***3** As discussed in more detail below, in June and July of 2008 the government obtained historical cell-site records from Verizon that reflected communications from the aircard. These cell-site records showed that the aircard communicated regularly with several cell towers in the area of Santa Clara, California. Using the cell-tower information, a map, and various calculations, a government agent was able to narrow the location of the aircard to an area of 6,412,224 square feet, or just under one-quarter of a square mile. Doc. 824–1 at 167. The government obtained an order from a Federal Magistrate Judge in the Northern District of California that authorized the installation of a pen register and trap and trace device to obtain additional cell site information, and a warrant authorizing the use of a mobile tracking device to communicate with the aircard. On July 16, 2008, agents used this mobile device to track the aircard's location to unit 1122 of the Domicilio apartment complex in Santa Clara. The government then obtained information from the apartment complex indicating that unit 1122 was rented in the name of Steven Travis Brawner. The rental application listed a fake California driver's license bearing a number that belonged to a female with a different name, and the handwriting of “Steve Brawner” on the apartment application was found by a handwriting expert to be similar to the handwriting of “Patrick Stout” on a post office box application. In addition, “Steve Brawner” had provided a fraudulent 2006 tax return when he applied to rent the apartment. Using this and other information generated during the investigation, the government obtained a warrant to search apartment 1122.

To ascertain the arrival and departure habits of the apartment's occupant, agents obtained gate access data from the Domicilio apartment's alarm company. This information showed when the occupant of unit 1122 used his fob to enter or leave the complex. Agents conducted surveillance of the apartment through the rest of July 2008 without observing the occupant. On the night of July 22, 2008, an undercover FBI agent used the ruse of a fast food delivery to knock on the apartment's door, but nobody answered.

Finally, on August 3, 2012, at approximately 4:15 p.m., agents observed a person matching the description of Steven Brawner walking near the apartment. The person began to act suspiciously when he saw the agents, and then began running to evade the agents. After a foot chase through the surrounding area, Defendant was apprehended by local police officers who happened to be on the scene. Agents searched the suspect incident to his arrest and found a set of keys in his pocket. An agent took the keys to unit 1122 and confirmed that they fit and turned the door lock. The agent waited for the arrival of other agents with the search warrant before entering the apartment.

Once in the apartment, agents found identification bearing the suspect's photograph and the name Patrick Stout, along with many of the pre-recorded $100 bills that were part of the $68,000 delivery in May. Agents also found the aircard, a laptop computer, and computer storage devices that eventually were found to contain much incriminating evidence. Fingerprints identified the suspect as Defendant Daniel Rigmaiden.

***4** Following his arrest and indictment in this case, Defendant elected to represent himself after he became dissatisfied with five successive defense attorneys. Defendant sought extensive discovery from

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

the government, including detailed discovery about the nature and operation of the mobile tracking device used to locate the aircard. The Court held several hearings, received substantial briefing, and ultimately concluded that some information regarding the mobile tracking device was protected by the qualified law enforcement privilege recognized in *Roviaro v. United States,* 353 U.S. 53, 77 S.Ct. 623, 1 L.Ed.2d 639 (1957). Doc. 723. The Court also concluded, however, that Defendant was fully able to make his Fourth Amendment arguments in light of the extensive disclosures provided by the government, detailed stipulations of fact agreed to by the government, and information Defendant was able to obtain through his own investigations with the aid of investigators, legal assistants, and a laptop computer provided by the Court. *Id.* Having now read Defendant's 355—page motion to suppress, and having reviewed his thousands of pages of supporting materials, the Court confirms this conclusion. Defendant has been placed at no disadvantage by the government's withholding of sensitive law enforcement information. Unless otherwise specified in this order, the Court will assume that Defendant's factual assertions are true.

II. Discussion.

Defendant's motion to suppress and related memoranda and motions (*see* footnote 1) contain a highly detailed and granular statement of his arguments. Defendant divides the government's actions into 21 different searches and provides detailed explanations as to how they functioned, why they were covered by the Fourth Amendment, and why they were not authorized by the orders and warrants obtained by the government. The Court has reviewed these many arguments individually, but will not attempt to address them separately in this written order. The Court instead will use the following categories to address Defendant's challenges and the government's responses: whether Defendant had a legitimate expectation of privacy in the location of the aircard; the government's collection of historical cell-site information, destination IP addresses, and data from the Domicilio apartment's alarm company; the search for the aircard using the mobile tracking device; the searches of Defendant's apartment and computer; and whether the Fourth Amendment's good faith exception applies.

A. Legitimate Expectation of Privacy.

[*Discussion omitted because it does not pertain to cell-site simulators. The court held that the defendant lacked a reasonable expectation of privacy in his aircard, computer, or apartment because they were obtained fraudulently using the identities of other persons.]*

B. Collection of Historical Records.

[*Discussion omitted as it does not pertain to cell-site simulators. The court held that the defendant had no reasonable expectation of privacy in historical cell-site information, IP address information, and apartment security system information obtained by the government via compulsory process.*]

C. Mobile Tracking Device Search for the Aircard.

Defendant claims that use of the mobile tracking device to locate his aircard violated the Fourth Amendment. The government argues that it obtained a warrant to use the tracking device. Defendant contends that the warrant was deficient and that the government exceeded its scope when carrying out the investigation. The ACLU has filed an amicus brief making similar arguments in support of Defendant's motion to suppress. Doc. 920.

1. Facts.

On July 11, 2008, the government obtained order CR–08–90330 (the “Tracking Warrant”) from United States Magistrate Judge Richard Seeborg of the Northern District of California. Doc. 470–1 at 28. The Tracking Warrant was issued under Rule 41(b) of the Federal Rules of Criminal Procedure and other stat-

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

utes. *Id.* Judge Seeborg found that the application for the warrant established "probable cause to believe that the use and monitoring of a mobile tracking device" would "lead to evidence of" several specific crimes, including conspiracy to defraud the government, fraud relating to identity information, aggravated identity theft, and wire fraud, "as well as to the identification of individuals who are engaged in the commission of these offenses." *Id.* at 29. This finding was based on a 17–page affidavit signed by FBI Special Agent William Ng. *Id.* at 10–17.

The Tracking Warrant precisely identifies the aircard to be located as "the Verizon Wireless broadband access card/cellular telephone assigned Telephone Number (415) 264–9596 and Electronic Serial Number (ESN) 005–00717190." *Id.* at 1. The warrant limited the duration of the authorized tracking to "a period not to exceed thirty (30) days," and ordered that monitoring of transmissions related to the aircard were "limited to transmissions needed to ascertain the physical location of [the aircard]." *Id.* at 2, 3.

Defendant raises several challenges to the Tracking Warrant. He asserts, among other arguments, that the warrant is not supported by probable cause, that it lacks particularity, that the government's searches and seizures exceeded the warrant's scope, and that agents executed the warrant unreasonably because they failed to comply with inventory and return requirements. Doc. 824–1 at 288–311. In its amicus brief, the ACLU argues that the search exceeded the scope of the warrant because the warrant authorized Verizon, not the government, to locate the aircard, and that the warrant was misleading and incomplete because it failed adequately to describe the technology involved in the search. Doc. 920.

***15** As noted above, the government has stipulated to several specific facts for purposes of this order. *See* Doc. 723 at 13–14. The Court accordingly will assume these facts to be true:

• The mobile tracking device used by the FBI to locate the aircard functions as a cell-site simulator. The device mimicked a Verizon Wireless cell tower and sent signals to, and received signals from, the aircard.

• The FBI used the device in multiple locations. The FBI analyzed signals exchanged between the mobile tracking device and the aircard. The FBI would take a reading, move to a new location, take another reading, move to another location, etc. The FBI never used more than a single piece of equipment at any given time.

• The device was used by government agents on foot within Defendant's apartment complex.

• The device generated real time data during the tracking process.

• All data generated by the mobile tracking device and received from Verizon as part of the locating mission was destroyed shortly after Defendant's arrest on August 3, 2008.

• The device used to simulate a Verizon cell tower is physically separate from the pen register trap and trace device used to collect information from Verizon.

• Signals sent by the mobile tracking device to the aircard are signals that would not have been sent to the aircard in the normal course of Verizon's operation of its cell towers.

• The mobile tracking device caused a brief disruption in service to the aircard.

• During the tracking operation, the FBI placed telephone calls to the aircard.

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

• The tracking operation was a Fourth Amendment search and seizure.

• The government will rely solely on the Tracking Warrant to authorize the use of equipment to communicate directly with Defendant's aircard and determine its location. The government will rely on a separate order (CR08–90331–MISC–RS) to justify obtaining cell-site and other non-content information from Verizon, but will base its defense of the use of the mobile tracking device solely on the Tracking Warrant.

• At the conclusion of the July 16, 2008, search efforts, the mobile tracking device had located the aircard precisely within Defendant's apartment.

With these assumed facts in mind, the Court will turn to an analysis of arguments made by Defendant and the ACLU.

2. Probable Cause.

Defendant argues that the actions authorized by the Tracking Warrant "were not supported by an applicable finding of probable cause." Doc. 824 at 301. As noted above, however, Judge Seeborg specifically found "probable cause to believe that the use and monitoring of a mobile tracking device for the [aircard] will lead to evidence of" several specific crimes and "to the identification of individuals who are engaged in the commission of these offenses." Doc. 470–1 at 29.

To establish probable cause for a search warrant, the government need only show "a fair probability that contraband or evidence of a crime will be found." *Illinois v. Gates,* 462 U.S. 213, 238, 103 S.Ct. 2317, 76 L.Ed.2d 527 (1983). The Court reviews Judge Seeborg's probable cause finding with deference, asking only whether he had a "substantial basis" for the probable cause determination. *Id.* at 238–29 *see also Ewing v. City of Stockton,* 588 F.3d 1218, 1223 (9th Cir.2009) (issuance of a search warrant is upheld "if the issuing judge 'had a substantial basis' for concluding [that] probable cause existed based on the totality of the circumstances"); *United States v. Gil,* 58 F.3d 1414, 1418 (9th Cir.1995) (magistrate judge's determination of probable cause is accorded significant deference).

***16** Special Agent Ng's affidavit supports Judge Seeborg's probable cause determination. Doc. 470–1 at 10–17. The affidavit describes the fraudulent tax-refund scheme in detail (*id.*, ¶¶ 3–21), how it was connected to the Hacker (referred to in the affidavit as the "Target Subject") (*id.*, ¶¶ 13–21), various confidential informant contacts with the Target Subject that confirmed his direct involvement in the fraudulent tax-refund scheme (*id.*), the Target Subject's receipt of funds from the scheme (*id.*, ¶¶ 22–30), and that the scheme and some of its fraudulent refund filings were connected to the aircard (referred to in the affidavit as the "Target Broadband Access Card/Cellular Telephone") (*id.*, ¶¶ 1, 34, 42). The affidavit clearly establishes a "fair probability" that locating the aircard would lead to evidence of a crime. Judge Seeborg's probable cause finding satisfies the Fourth Amendment. *See Dalia v. United States,* 441 U.S. 238, 255, 99 S.Ct. 1682, 60 L.Ed.2d 177 (1979).

Defendant disputes the language of the Tracking Warrant, arguing that Judge Seeborg's probable cause finding applied only to information provided by Verizon and not to locating the aircard. But Judge Seeborg's expressly found "probable cause to believe that the use and monitoring of a mobile tracking device for the [aircard]" would lead to evidence of various crimes. Doc. 470–1 at 29.

Defendant also argues that the phrase "mobile tracking device" describes a device attached to a vehicle and not the device used by agents to locate the aircard. The Court concludes, however, that "mobile tracking device" is a reasonable description of the

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

mobile device used by the government to track the aircard. The Tracking Warrant authorized "the use and monitoring of a mobile tracking device for the Target Broadband Access Card/Cellular Telephone," while "the agents are stationed in a public location and the Target Broadband Access Card/Cellular Telephone is ... inside private residences, garages, and/or other locations not open to the public or visual surveillance[.]" *Id.* at 28–29. The affidavit of Agent Ng stated that the mobile tracking device would monitor the aircard and would "ultimately generate a signal that fixes the geographic position of the [aircard]." *Id.* at 26. These statements foreclose any possible confusion that the device was to be attached to a vehicle.

3. Particularity.

Defendant argues that the search exceeded the scope of the warrant because the warrant did not specifically authorize the FBI to use a cell-site simulator. He also argues that the warrant's reference to a "mobile tracking device," its description of the place to be searched, and its use of the phrase "all data, information, facilities, and technical assistance" lack particularity. The government counters that the warrant was not required to provide greater specificity concerning the methods by which the aircard was to be located.

There is no legal requirement that a search warrant specify the precise manner in which the search is to be executed. *Dalia,* 441 U.S. at 257; *see Maryland v. Garrison,* 480 U.S. 79, 84, 107 S.Ct. 1013, 94 L.Ed.2d 72 (1987). "The Fourth Amendment ... does not set forth some general 'particularity requirement.' It specifies only two matters that must be 'particularly describ[ed] in the warrant: 'the place to be searched' and 'the persons or things to be seized.' " *United States v. Grubbs,* 547 U.S. 90, 97, 126 S.Ct. 1494, 164 L.Ed.2d 195 (2006) (citing *Dalia,* 441 U.S. at 257).

***17** *Dalia* involved a warrant that authorized the placement of a hidden listening device in the defendant's office, but did not specify that the police would break into the office to install the device. 441 U.S. at 254–56. The Supreme Court rejected the particularity challenge, holding that authorization of the break-in was not necessary because nothing in the Fourth Amendment requires search warrants to "include a specification of the precise manner in which they are to be executed." *Id.* at 257. The Supreme Court's explanation applies to this case:

> Nothing in the language of the Constitution or in this Court's decisions interpreting that language suggests that ... search warrants also must include a specification of the precise manner in which they are to be executed. On the contrary, it is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant—subject of course to the general Fourth Amendment protection "against unreasonable searches and seizures."
>
> [Dalia's] view of the Warrant Clause parses too finely the interests protected by the Fourth Amendment. Often in executing a warrant the police may find it necessary to interfere with privacy rights not explicitly considered by the judge who issued the warrant. For example, police executing an arrest warrant commonly find it necessary to enter the suspect's home in order to take him into custody, and they thereby impinge on both privacy and freedom of movement. Similarly, officers executing search warrants on occasion must damage property in order to perform their duty.
>
> *Id.* at 257–58.

In *United States v. Brooks,* 427 F.3d 1246, 1251 (10th Cir.2005), the Tenth Circuit similarly explained that while a search warrant must describe with particularity the objects of the search, "the methodology used to find those objects need not be described: this court has never required warrants to contain a partic-

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

ularized computer search strategy." *See also United States v. Blake,* No. 1:08–cr–0284–OWW, 2010 WL 702958, at *4 (E.D.Cal. Feb.25, 2010) ("There is no legal requirement that a search warrant include a specification of the precise manner in which the search is to be executed.").

The Court concludes that the Tracking Warrant was sufficiently particular. It precisely identified the aircard to be located by description, telephone number, and ESN number. Doc. 470–1 at 28. It stated that the aircard was to be located using a "mobile tracking device," which, as noted above, reasonably describes the mobile equipment used to track signals from the aircard. *Id.* And it stated that FBI agents would be located in a public place while the aircard would be located in a private residence. *Id.* Although the warrant did not describe the precise means by which the mobile tracking device would operate, what signals it would send to the aircard, what signals it would capture, or the fact that it would cause some of Defendant's electricity to be consumed in the process, these and the many other details of the device's operation described in Defendant's motion clearly concern the manner in which the search was to be executed, something that need not be stated with particularity in the warrant. *Dalia,* 441 U.S. at 257–58; *Grubbs,* 547 U.S. at 97–98. The objective of the warrant—locate the aircard—was clearly stated, as was the use of a mobile tracking device to make the location. Defendant's efforts to parse the warrant requirement further are no more persuasive here than were the defendants' similar efforts in *Dalia* and *Brooks.*[FN7]

FN7. This analysis also applies to Defendant's many arguments about things not specified in the warrant: that the mobile tracking device would force the aircard to change its cell tower connection to an emulated cell tower, would temporarily interrupt Defendant's Internet connection, would write data to the aircard and laptop, would disable encryption for aircard signals, and would download data from the aircard. These details concerned the manner of the search and were less intrusive than the physical break-in that did not have to be specified in the warrant in *Dalia.* Under *Dalia, Grubbs,* and related cases, the Court concludes that these methodology details were not required in the warrant.

4. Scope and Terms of the Warrant.

***18** Defendant and the ACLU argue that the aircard locating mission exceeded the scope of the Tracking Warrant because the warrant suggests that Verizon, not the FBI, was authorized to search for the aircard. The warrant states that Verizon is "to *assist* agents of the Federal Bureau of Investigation (FBI) by providing all information, facilities, and technical assistance needed to ascertain the physical location of the [aircard] through the use and monitoring of a mobile tracking device[.]" Doc. 470–1 at 28. This language sufficiently states that the FBI was to ascertain the location of the aircard by using a mobile tracking device and that Verizon was being ordered to provide assistance. The warrant further orders that Verizon "shall provide to agents of the FBI data and information ... while the agents are stationed in a public location and the [aircard] is ... inside private residences, garages and/or other locations not open to the public or visual surveillance[.]" *Id.* at 2. The plain and common sense reading of these words is that Verizon was to assist the FBI by providing information and other services while the FBI used a mobile tracking device in a public location to find the aircard. *See, e.g., United States v. Gorman,* 104 F.3d 272, 275 (9th Cir.1996) ("Plain meaning and common sense are landmarks for the execution and interpretation of the language of a search warrant.") (citations omitted).

The ACLU argues that the "most sensible reading" of the Tracking Warrant is that it authorized Verizon to install a pen register, not that it authorized the government to use a mobile tracking device. Doc. 985 at 3. Again the Court disagrees. Two orders were

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

signed by Judge Seeborg on July 11, 2008. The Tracking Warrant was sought "pursuant to an Application under Federal Rule of Criminal Procedure 41(b); Title 18, United States Code, Sections 2703 and 3117, and Title 28, United States Code, Section 1651[.]" Doc. 470–1 at 28. As already noted, the warrant found "probable cause to believe that the use and monitoring of a mobile tracking device for the [aircard] will lead to evidence of" specific crimes, "as well as to the identification of individuals who are engaged in the commission of these offenses." *Id.* at 29.

Separate order CR–08–90331 ("the Pen and Trap Order"), also dated July 11, 2008, states that it is an "Application under 18 U.S .C. §§ 2703(c), 2703(d), 3122, and 3123 ... requesting an Order authorizing the installation of a pen register and trap and trace device on the instrument or facility currently utilizing the following subject telephone number[.]" Doc. 470–2 at 6. The Pen and Trap Order then states that "Applicant has offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information identifying subscribers or customers ... for Target Device are relevant and materials to an ongoing criminal investigation of the specified offenses." *Id.* at 7. This is the statutory standard for obtaining information under the SCA.

***19** A common-sense reading of these two documents shows that the Tracking Warrant was granted under Rule 41, upon a finding of probable cause, and authorized use of a mobile tracking device to locate the aircard. The Pen and Trap Order was authorized under various statutes, upon a finding under the SCA, and authorized installation of a pen and trap device. The Court cannot agree that the Tracking Warrant authorized only a pen and trap device.

The Court agrees that the Tracking Warrant is not a model of clarity. But it contains the essential elements of a warrant. The Supreme Court has made clear that the Fourth Amendment imposes only three requirements on warrants: "First, warrants must be issued by neutral, disinterested magistrates. Second, those seeking the warrant must demonstrate to the magistrate their probable cause to believe that the evidence sought will aid in a particular apprehension or conviction for a particular offense. Finally, warrants must particularly describe the things to be seized, as well as the place to be searched." *Dalia,* 441 U.S. at 255 (citations and quotation marks omitted); *see also Grubbs,* 547 U.S. at 97–98. The Tracking Warrant satisfied each of these requirements. It was issued by Judge Seeborg, a neutral magistrate; the judge found probable cause; and the thing to be located (the aircard) was precisely identified. The place to be searched could not be specified because it was unknown, but the warrant did note the likelihood that the aircard would be located "inside private residences, garages and/or other locations not open to the public or visual surveillance[.]" Doc. 470–1 at 29. The Tracking Warrant satisfied the essential requirements of the Fourth Amendment. Nothing more is required. *Dalia,* 441 U.S. at 257–58.[FN8]

FN8. In a supplemental brief, the ACLU attaches internal e-mail communications from the North District of California suggesting that magistrates judges in that district recently have become concerned about the use of pen and trap orders to authorize the kind of aircard locating mission that occurred in this case. Doc. 985–1. The e-mails do not persuade the Court that suppression is required here. Prosecutors in this case obtained the Tracking Warrant in addition to the Pen and Trap Order. Moreover, the e-mail communications appear to reflect an evolving understanding about the use of technology, with prosecutors in the Northern District of California attempting to be responsive to concerns expressed by magistrate judges. The e-mails occurred some three years after the aircard locating mission in this case, and provide no basis to conclude that prosecutors

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

knew or should have known their practices in 2008 were deficient.

5. New Technology and the Duty of Candor.

Defendant and the ACLU insist that because cell-site simulators are a new and potentially invasive technology, the government was required to include a more detailed description in its warrant application. The ACLU cites cases in which a magistrate denied the government's application to use a cell-site simulator, but in each of those cases the applications were made pursuant to statutory authority and not, as here, pursuant to a warrant based on probable cause. *See In re Application for an Order Authorizing Installation and Use of a Pen Register and Trap and Trace Device (In re Stingray),* 890 F.Supp.2d 747, 2012 WL 2120492, at *5 (S.D.Tex. June 2, 2012) (distinguishing *Rigmaiden*, with its stipulation that a Fourth Amendment search occurred, and explaining that "[h]ere, the application seeks an order authorizing the use of this equipment as a pen register as opposed to seeking a warrant."); *In re Application for an Order Pursuant to 18 U.S.C. § 2703(d) (In re Cell Tower Dump),* ——F.Supp.2d ——, 2012 WL 4717778, at *3–4 (S.D.Tex. Sept.26, 2012) (rejecting application under SCA "for cell tower dump," stating that a warrant supported by probable cause was required).

***20** In support of the argument that the government violated a "duty of candor" in applying for the warrant, Defendant and the ACLU cite *United States v. Rettig,* 589 F.2d 418 (9th Cir.1978), and *United States v. Comprehensive Drug Testing, Inc. ("CDT"),* 621 F.3d 1162 (9th Cir.2010). These cases offer little support for Defendant's position.

In *Rettig,* drug enforcement agents asked a federal magistrate to issue an arrest warrant for the defendant on cocaine importation charges and a search warrant for the defendant's residence. 589 F.2d at 420. The judge issued the arrest warrant, but denied the search warrant because information provided in support of the warrant was stale. *Id.* The agents arrested the defendant. *Id.* During the arrest, they caught the defendant trying to flush marijuana down the toilet. *Id.* Defendant was taken into custody while another agent attempted to obtain a search warrant for marijuana evidence, this time from a state judge, without informing the judge of the agents' unsuccessful attempt to obtain a search warrant from the federal magistrate judge the day before. *Id.* The state marijuana warrant was obtained, and agents then spent several hours searching for evidence relating to the cocaine conspiracy as to which the federal search warrant had been denied. *Id.* at 421. They ultimately seized more than 2,000 items. *Id* .

Not surprisingly, the Ninth Circuit suppressed the evidence. The court found that agents used the state search warrant "as an instrument for conducting the search for which permission had been denied on the previous day, a search that pertained to evidence of the cocaine charge, not to the possession of marijuana," and that "the search was for purposes and objects not disclosed to the magistrate." *Id.* The court clarified, however, that the agents' failure to apprise the state judge of their previous attempt to secure a search warrant for the cocaine conspiracy evidence "would not necessarily invalidate the search warrant or proscribe a search and incident seizures confined to the terms of the warrant." *Id.* Instead, the court found suppression necessary because "the agents did not confine their search in good faith to the objects of the [state marijuana] warrant," and "substantially exceeded any reasonable interpretation of its provisions." *Id.* at 423. It was not the agents' lack of candor with respect to the prior warrant application that required suppression, but their failure "to disclose an intent to conduct a search the purposes and dimensions of which are beyond that set forth in the affidavits." *Id.*

In this case, the application seeking authority to use a mobile tracking device did not mislead Judge Seeborg as to the purpose of the search, which was to locate the aircard. Although it is true, as the ACLU emphasizes, that the application did not disclose that

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

the mobile tracking device would capture signals from other cell phones and aircards in the area of Defendant's apartment, the Court regards this as a detail of execution which need not be specified under *Dalia.* 441 U.S. at 258. Significantly, the agents in this case did not seek to capture third-party cell phone and aircard information so they could use it in a criminal investigation, nor is there any evidence that they used the third-party information in that manner. To the contrary, the evidence presented by the government and Defendant shows that the third-party information was deleted from the mobile tracking device immediately after the aircard was located. Thus, this was not a case like *Rettig* where agents intentionally searched for and sought to use cocaine evidence that was well beyond the scope of the marijuana search warrant.

***21** Defendant and the ACLU also cite *CDT,* and in particular the concurring opinion by Chief Judge Kozinski. *CDT* involved a federal investigation of a business that was suspected of providing steroids to professional baseball players. *Id.* at 1166. During the investigation, the government learned of 10 players who had tested positive for steroid use. *Id.* It secured a grand jury subpoena in the Northern District of California seeking all records pertaining to Major League Baseball in the possession of CDT. *Id.* CDT moved to quash the subpoena. *Id.* The day the motion to quash was filed, the government obtained a warrant in the Central District of California to search CDT's facilities. *Id.* The warrant was limited to the 10 players as to whom the government had probable cause, but when the government executed the warrant it "seized and promptly reviewed the drug testing record for hundreds of players in Major League Baseball (and a great many other people)." *Id.* The government also obtained a warrant from the District of Nevada for the urine samples on which drug tests had been performed. *Id.*

CDT and the players' union moved for return of seized property in the Central District of California and the District of Nevada, and moved to quash the subpoenas in the Northern District of California. *Id.* at 1166–67. The district courts granted these motions, expressing "grave dissatisfaction with the government's handling of the investigation" and accusing the government of "manipulation and misrepresentation." *Id.* at 1167. The Ninth Circuit affirmed. *Id.*

In his concurrence, Chief Judge Kozinski criticized federal authorities for submitting a warrant application that omitted information concerning CDT's agreement to keep the sought-after data intact pending a ruling on its motion to quash in the Northern District of California, an agreement that was accepted by the United States Attorney's Office. *Id.* at 1178. This omission "created the false impression that, unless the data were seized at once, it would be lost." *Id.* Chief Judge Kozinski wrote that "omitting such highly relevant information altogether is inconsistent with the government's duty of candor in presenting a warrant application. A lack of candor in this or any other aspect of the warrant application must bear heavily against the government in the calculus of any subsequent motion to return or suppress the seized data." *Id.*

The Court cannot conclude that the omissions identified by Defendant and the ACLU in this case were "highly relevant." They were not material to the probable cause determination, nor did they mislead Judge Seeborg as to the object of the search. Instead, they implicated only the question of "how the search would be conducted." *United States v. Mittelman,* 999 F.2d 440, 444 (9th Cir.1993) (holding that "misstatements regarding the manner of a search do not bear on the issue of whether the search itself was justified"). Therefore, any omission of the fact that the mobile tracking device would also capture information from other cell phones and aircards in the area does not weigh heavily against the government.

***22** Moreover, the warrant specifically required the government to "expunge all of the data" at the conclusion of the tracking mission. Doc. 470–1 at 30. The government explained that this was done pre-

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

cisely because the device captured information from cell phones and aircards unrelated to this investigation. There is no suggestion that the government's failure to disclose that the device would capture third-party information somehow allowed it to retain and review such data.

6. Other Arguments.

Defendant argues that the warrant was invalid because Agent Ng's affidavit was not incorporated in or attached to the warrant when the search was executed. Like the defendant in *United States v. Smith,* 424 F.3d 992 (9th Cir.2005), Defendant apparently "confuses the well-settled principle that a warrant's overbreadth can be cured by an accompanying affidavit that more particularly describes the items to be seized with the contention ... that an affidavit incorporated by reference must always be attached for the search warrant to be valid—even if the warrant is not overbroad without the attachment." *Id.* at 1007 (citation and quotation marks omitted). As in *Smith,* Defendant's argument is "unsupported by case law." *Id.*

Nor is the warrant invalid because it fails to describe the place to be searched. A warrant to locate an item need not specify the place to be searched. In such cases the particularity requirement can be satisfied if the warrant provides other information. In *United States v. Karo,* 468 U.S. 705, 104 S.Ct. 3296, 82 L.Ed.2d 530 (1984), the government contended that it would be impossible to describe the place to be searched "because the location of the place is precisely what is sought to be discovered through the search." *Id.* at 718. The Supreme Court rejected that argument: "However true that may be, it will still be possible to describe the object into which the beeper is to be placed, the circumstances that led agents to wish to install the beeper, and the length of time for which beeper surveillance is requested." *Id.* The Tracking Warrant precisely identified the object to be located, found probable cause to believe that location of the aircard would produce evidence of the crimes identified in the warrant and the identification of individuals involved in those crimes, and placed a time limit on the location effort. As noted, the warrant also specifically recognized that the aircard may be located in a private residence. The affidavit of Agent Ng provided detailed information about the alleged tax-refund scheme and how location of the aircard could aid in the investigation of that scheme. These specifics satisfy the requirements of *Karo.*

Finally, Defendant notes that the Tracking Warrant did not require the FBI to make a return or serve a copy of the warrant on Defendant, and argues that this failure violated Rule 41(f)(2). The government concedes this flaw in the warrant, but correctly notes that suppression is not the appropriate remedy. There is no causal connection between the failure to serve the warrant and the government's location of the aircard. *See United States v. Hector,* 474 F.3d 1150, 1155 (9th Cir.2007) (holding that suppression is inappropriate remedy for failure to serve copy of search warrant) (citing *Hudson v. Michigan,* 547 U.S. 586, 592, 126 S.Ct. 2159, 165 L.Ed.2d 56 (2006)); *United States v. Motz,* 936 F.2d 1021, 1025 (9th Cir.1991) (holding that where defendants "were not prejudiced by the agents' failure to perform the ministerial requirements" of return and inventory, "[t]he district court was correct in refusing to suppress the evidence"). Defendant argues that he would have fled and never been found if the warrant had been served, but the Court cannot conclude that his inability to evade capture is the kind of prejudice referred to in the case law.

D. Search of Apartment and Computer.

[*Discussion omitted as it does not pertain to cell-site simulators. The court rejected challenges to the physical search of defendant's apartment and computer.*]

E. Good Faith Exception.

[*Discussion omitted. The court held that even if*

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

there had been a Fourth Amendment violation, agents had relied in good faith on warrants and suppression would not be an appropriate remedy.]

III. Related Motions.

[*Discussion omitted as it does not pertain to cell-site simulators*.]

IV. Conclusion.

Defendant has not shown that he had a legitimate expectation of privacy in his apartment, laptop, or aircard. Defendant has not shown that his Fourth Amendment rights were violated or, if a violation did occur, that suppression is the appropriate remedy. The good faith exception applies to the contested areas of the government's investigation, including its use of the mobile tracking device pursuant to a Rule 41 warrant.

***34** Defendant has filed literally dozens of motions in this case, many of them seeking suppression or some other form of sanction against the government. The Court has patiently sought to address each motion filed by pro se Defendant, but the time has come to resolve the government's allegations on the merits. Defendant should file no further motions to suppress or for sanctions based on the government's searches in this case or its pretrial production of discovery to Defendant.

IT IS ORDERED.

1. Defendant's Motion to Suppress (Doc. 824) is **denied.**

[*Additional omitted do not pertain to cell-site simulators and are omitted.*]

D.Ariz.,2013.
U.S. v. Rigmaiden
Not Reported in F.Supp.2d, 2013 WL 1932800 (D.Ariz.)

END OF DOCUMENT

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

United States Court of Appeals,
Fifth Circuit.
In re Application of the UNITED STATES of America FOR HISTORICAL CELL SITE DATA.
United States of America, Appellant.

No. 11–20884.
July 30, 2013.

Background: Government brought applications, under the Stored Communications Act (SCA), in three separate criminal investigations, seeking to compel cell phone service providers to produce cell site information for targeted cell phones that would track the phones over a two-month period. The United States District Court for the Southern District of Texas, Lynn N. Hughes, J., 747 F.Supp.2d 827, denied applications. Government appealed.

Holdings: The Court of Appeals, Edith Brown Clement, Circuit Judge, held that:
(1) issue was ripe for review;
(2) denial of applications was final appealable order;
(3) magistrate judge did not have discretion to require government to seek warrant rather than order; and
(4) court orders authorized by Stored Communications Act under "specific and articulable facts" standard, rather than Fourth Amendment probable cause standard, to compel cell phone service providers to produce the historical cell site information of their subscribers were not per se unconstitution- al.

Vacated and remanded.

Dennis, Circuit Judge, filed dissenting opinion.

West Headnotes

[1] Criminal Law 110 1139

110 Criminal Law
110XXIV Review
110XXIV(L) Scope of Review in General
110XXIV(L)13 Review De Novo
110k1139 k. In general. Most Cited Cases

The Court of Appeals reviews constitutional challenges to federal statutes de novo.

[2] Criminal Law 110 1158.1

110 Criminal Law
110XXIV Review
110XXIV(O) Questions of Fact and Findings
110k1158.1 k. In general. Most Cited Cases

The Court of Appeals reviews a district court's findings of fact for clear error.

[3] Criminal Law 110 1158.1

110 Criminal Law
110XXIV Review
110XXIV(O) Questions of Fact and Findings
110k1158.1 k. In general. Most Cited Cases

A finding of fact is clearly erroneous when although there is evidence to support it, the reviewing court on the entire evidence is left with a firm and definite conviction that a mistake has been committed.

[4] Criminal Law 110 1153.2

110 Criminal Law
110XXIV Review
110XXIV(N) Discretion of Lower Court
110k1153 Reception and Admissibility of Evidence
110k1153.2 k. Judicial notice. Most Cited Cases

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

The Court of Appeals reviews the use of judicial notice for abuse of discretion. Fed.Rules Evid.Rule 201, 28 U.S.C.A.

[5] Telecommunications 372 1479

372 Telecommunications
372X Interception or Disclosure of Electronic Communications; Electronic Surveillance
372X(B) Authorization by Courts or Public Officers
372k1479 k. Review of proceedings; standing. Most Cited Cases

Issue of whether court orders authorized by Stored Communications Act (SCA) under "specific and articulable facts" standard to compel cell phone service providers to produce historical cell site information of their subscribers were per se unconstitutional was ripe for review, where magistrate judge denied government's applications on basis that SCA's authorization of such orders for cell site information violated Fourth Amendment, district court adopted magistrate judge's decision, government's claim that denial was improper and deprived it of legitimate investigatory tool was question of law, amenable to judicial resolution, and current appeal was only time that government could challenge denial of its order. U.S.C.A. Const. Art. 3, § 1 et seq.; U.S.C.A. Const.Amend. 4; 18 U.S.C.A. § 2703(d).

[6] Telecommunications 372 1479

372 Telecommunications
372X Interception or Disclosure of Electronic Communications; Electronic Surveillance
372X(B) Authorization by Courts or Public Officers
372k1479 k. Review of proceedings; standing. Most Cited Cases

District court's denial of government's applications under Stored Communications Act (SCA) for court to issue orders to compel cell phone service providers to produce historical cell site information of their subscribers, on basis that SCA's authorization of such orders for cell site information under "specific and articulable facts" standard violated Fourth Amendment, was final appealable order; application for that type of order was independent proceeding, not tied to any current criminal case, and denying or granting order finally disposed of proceeding. U.S.C.A. Const.Amend. 4; 18 U.S.C.A. § 2703(d); 28 U.S.C.A. § 1291.

[7] Telecommunications 372 1475

372 Telecommunications
372X Interception or Disclosure of Electronic Communications; Electronic Surveillance
372X(B) Authorization by Courts or Public Officers
372k1475 k. Carrier's cooperation; pen registers and tracing. Most Cited Cases

Magistrate judge did not have discretion under Stored Communications Act (SCA) to require government to seek warrant rather than order under "specific and articulable facts" standard to compel cell phone service providers to produce historical cell site information of their subscribers, as long as government met statutory requirements. 18 U.S.C.A. § 2703(d).

[8] Telecommunications 372 1475

372 Telecommunications
372X Interception or Disclosure of Electronic Communications; Electronic Surveillance
372X(B) Authorization by Courts or Public Officers
372k1475 k. Carrier's cooperation; pen registers and tracing. Most Cited Cases

Under the Stored Communications Act (SCA), to obtain an order for the historical cell site records of a particular cell phone owner, the government may apply to a court that has jurisdiction, and that court must grant the order if the government seeks an order (1) to require a provider of electronic communication service or remote computing service (2)

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

to disclose a non-content record or other information pertaining to a subscriber to or customer of such service when the government (3) meets the specific and articulable facts standard. 18 U.S.C.A. § 2703(d).

[9] Telecommunications 372 1475

372 Telecommunications
372X Interception or Disclosure of Electronic Communications; Electronic Surveillance
372X(B) Authorization by Courts or Public Officers
372k1475 k. Carrier's cooperation; pen registers and tracing. Most Cited Cases

Court orders authorized by Stored Communications Act under "specific and articulable facts" standard, rather than Fourth Amendment probable cause standard, to compel cell phone service providers to produce historical cell site information of their subscribers were not per se unconstitutional, since cell site information was business record of transactions to which it was party, government did not require service providers to record that information or store it, users knew that they conveyed information about their location to their service providers, and use of phones was entirely voluntary. U.S.C.A. Const.Amend. 4; 18 U.S.C.A. § 2703(d).

[10] Searches and Seizures 349 25.1

349 Searches and Seizures
349I In General
349k25 Persons, Places and Things Protected
349k25.1 k. In general. Most Cited Cases

What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. U.S.C.A. Const.Amend. 4.

[11] Searches and Seizures 349 25.1

349 Searches and Seizures
349I In General
349k25 Persons, Places and Things Protected
349k25.1 k. In general. Most Cited Cases

When a person communicates information to a third party, even on the understanding that the communication is confidential, he cannot object under the Fourth Amendment if the third party conveys that information or records thereof to law enforcement authorities. U.S.C.A. Const.Amend. 4.

[12] Searches and Seizures 349 26

349 Searches and Seizures
349I In General
349k25 Persons, Places and Things Protected
349k26 k. Expectation of privacy. Most Cited Cases

The Fourth Amendment, safeguarded by the courts, protects only reasonable expectations of privacy. U.S.C.A. Const.Amend. 4.

***601** Nathan Paul Judish (argued), U.S. Department of Justice, Washington, DC, James Lee Turner, Assistant U.S. Attorney, U.S. Attorney's Office, Houston, TX, for Appellant.

Matthew Zimmerman, Esq., Hanni Meena Fakhoury, Esq. (argued), Attorney, San Francisco, CA, for Amicus Curiae, Electronic Frontier Foundation.

Catherine Newby Crump, American Civil Liberties Union Foundation of New York, New York, NY, for Amicus Curiae, American Civil Liberties Union Foundation.

Rebecca L. Robertson, Attorney, Houston, TX, for Amicus Curiae, American Civil Liberties Union Foundation of Texas.

***602** Susan Allison Freiwald (argued), San Francisco, CA, pro se.

Marc Rotenberg, Washington, DC, for Amicus Curiae, Electronic Privacy Information Center.

Appeal from the United States District Court for the Southern District of Texas.

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

Before REAVLEY, DENNIS, and CLEMENT, Circuit Judges.

EDITH BROWN CLEMENT, Circuit Judge:

We are called on to decide whether court orders authorized by the Stored Communications Act to compel cell phone service providers to produce the historical cell site information of their subscribers are per se unconstitutional. We hold that they are not.

I. FACTUAL AND PROCEDURAL BACKGROUND

In early October 2010, the United States filed three applications under § 2703(d) of the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701–2712, seeking evidence relevant to three separate criminal investigations. Each application requested a court order to compel the cell phone service provider for a particular cell phone to produce sixty days of historical cell site data and other subscriber information for that phone. The Government requested the same cell site data in each application: "the antenna tower and sector to which the cell phone sends its signal." It requested this information for both the times when the phone sent a signal to a tower to obtain service for a call and the period when the phone was in an idle state.[FN1] *In re Application of the United States for Historical Cell Site Data,* 747 F.Supp.2d 827, 829 (S.D.Tex.2010).

FN1. According to the Government, it now believes that cell phone service providers do not create cell site records when a phone is in an idle state, and it is willing to exclude such information from the scope of its applications.

For each application, the magistrate judge granted the request for subscriber information but denied the request for the historical cell site data, despite finding that the Government's showing met the "specific and articulable facts" standard set by the SCA for granting an order to compel the cell site data. Shortly thereafter, the magistrate judge invited the Government to submit a brief justifying the cell site data applications. Four days after the Government submitted its brief, the magistrate judge issued a written opinion taking judicial notice of a host of facts about cell phone technology, primarily derived from the testimony of a computer science professor at a congressional hearing, but also including information from published studies and reports and service provider privacy policies. He concluded his opinion by declaring that, based on these facts viewed in light of Supreme Court precedent, "[c]ompelled warrantless disclosure of cell site data violates the Fourth Amendment." *Id.* at 846.

The Government filed objections with the district court to the magistrate judge's ruling on the constitutionality of the SCA and his judicial notice of facts. Although there was no party adverse to the Government's ex parte application, the ACLU and Electronic Frontier Foundation ("EFF"), among others, participated as amici curiae. As part of its submissions, the Government provided the court with additional evidence in the form of an affidavit from one of the service providers detailing its cell site records. After the parties submitted their briefs, the district judge issued a single-page order. He concluded:

> When the government requests records from cellular services, data disclosing the location of the telephone at the time ***603** of particular calls may be acquired only by a warrant issued on probable cause. The records would show the date, time called, number, and location of the telephone when the call was made. These data are constitutionally protected from this intrusion. The standard under the Stored Communications Act is below that required by the Constitution.

The Government appealed once again, and the ACLU and EFF,[FN2] along with Professor Orin Kerr and others, requested and were granted leave to participate as amici.

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

FN2. These two amici, which filed jointly, are referred to as "the ACLU" for simplicity.

II. STANDARD OF REVIEW

[1][2][3][4] This court reviews constitutional challenges to federal statutes de novo. *United States v. Pierson,* 139 F.3d 501, 503 (5th Cir.1998). It reviews a district court's findings of fact for clear error. *United States v. Keith,* 375 F.3d 346, 348 (5th Cir.2004). "A finding of fact is clearly erroneous 'when although there is evidence to support it, the reviewing court on the entire evidence is left with a firm and definite conviction that a mistake has been committed.' " *In re Missionary Baptist Found. of Am., Inc.,* 712 F.2d 206, 209 (5th Cir.1983) (quoting *United States v. U.S. Gypsum Co.,* 333 U.S. 364, 395, 68 S.Ct. 525, 92 L.Ed. 746 (1948)). The court reviews use of judicial notice under Federal Rule of Evidence 201 for abuse of discretion. *Taylor v. Charter Med. Corp.,* 162 F.3d 827, 829 (5th Cir.1998). Although the Federal Rules of Evidence may not apply to applications for § 2703(d) orders, Rule 201 "embodies 'the traditional view' of judicial notice ... 'consistent with' the common law," WRIGHT, MILLER & COOPER, 21B FED. PRAC. & PROC. EVID. § 5102 (2d ed.), so the court will apply the same standard to common law judicial notice.

III. DISCUSSION

The Government raises two issues on appeal. First, it challenges the district court's adoption of the magistrate judge's conclusion that the SCA unconstitutionally lowers the standard the Government must meet to compel disclosure of historical cell site information below that required by the Fourth Amendment. Second, it claims that the magistrate judge's judicial notice of certain facts, to the extent they were adopted by the district court, was improper. To these merits issues presented by the Government, amicus Professor Orin Kerr adds two threshold issues: whether this case is ripe and whether 28 U.S.C. § 1291 gives the court appellate jurisdiction over it.

A. Jurisdiction

1. Ripeness

[5] Professor Kerr claims that this controversy is not ripe. He asserts that the issue of whether a court order complies with the Fourth Amendment must be addressed after officers execute the order, not before. According to Professor Kerr, exclusively ex post review of such orders is "essential because Fourth Amendment law is extremely fact-specific." Although we agree that this approach is preferable in most cases, *see Warshak v. United States,* 532 F.3d 521, 528 (6th Cir.2008) (en banc) ("The Fourth Amendment is designed to account for an unpredictable and limitless range of factual circumstances, and accordingly it *generally* should be applied after those circumstances unfold, not before." (emphasis added)), we also agree that, as he says, here we are presented with the unusual circumstance of "an abstract question of [Fourth Amendment] law with no connection to a genuine factual record." Because the district court concluded that ***604** the § 2703(d) order provision was categorically unconstitutional with respect to an entire class of records—historical cell site information—that is covered under the plain text of § 2703(c), our review of its decision addresses only whether the fact that the Government's request was for such records is, by itself, sufficient to make its applications for § 2703(d) orders unconstitutional. [FN3]

FN3. For our review, it does not matter how any eventual search would be carried out. Of course, if the Government executed the order in an unconstitutional manner, any evidence it obtained might be subject to suppression. But that is not the issue presented here.

This issue satisfies our test for ripeness. Such cases are ripe when they meet two criteria. "First, they are fit for judicial decision because they raise pure questions of law. Second, [the plaintiff] would suffer hardship if review were delayed." *Opulent*

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

Life Church v. City of Holly Springs, Miss., 697 F.3d 279, 287–88 (5th Cir.2012). Here, the Government applied for three § 2703(d) orders, and the magistrate judge denied its applications on the basis that the SCA's authorization of such orders for cell site information violates the Constitution. The district court adopted the magistrate judge's decision to deny the applications on constitutional grounds. The Government's claim that this denial is improper and deprives it of a legitimate investigatory tool is a question of law, amenable to judicial resolution. Moreover, this is the only time that the Government can challenge the denial of its order. It cannot wait until after it executes the order, because there is no order to execute. The dispute is ripe for review.

The cases cited by Professor Kerr do not alter this conclusion. He points out that in *Warshak,* the Sixth Circuit, sitting en banc, discussed how expectations of privacy, particularly in the context of "ever-evolving technologies," typically turn on concrete, case-by-case determinations of a "limitless range of factual circumstances." 532 F.3d at 527–28. However, we are only asked to decide whether every instance of one particular factual circumstance— § 2703(d) orders for historical cell site information—is unconstitutional. If we conclude that such orders are not categorically unconstitutional, specific orders within that category certainly may be unconstitutional because of additional facts involved in the case. But we do not need such facts to determine if orders for historical cell site records are per se unconstitutional.

Moreover, *Warshak* involved a plaintiff who sought an injunction against the United States to prevent it from obtaining and executing any § 2703(d) order against him in the future. *Id.* at 524–25. Because no order existed, or might ever exist, the Sixth Circuit held that his claim was too speculative to be ripe for adjudication. *Id.* at 525–31. Similarly, Professor Kerr notes that we dismissed, sua sponte, as unripe a pre-enforcement challenge brought by two unions against a state railway safety law, which they claimed authorized drug testing of railroad employees without probable cause. *See United Transp. Union v. Foster,* 205 F.3d 851, 857–59 (5th Cir.2000). We held that the unions' claims were speculative and, thus, premature. *Id.* But to trigger the drug tests in the law challenged in *Foster:*

> [T]he following train of events would necessarily have to occur: First, a train must be involved in a collision at a Louisiana railroad crossing ... Second, even assuming that such a collision occurs, ... a law enforcement officer must have "reasonable grounds to believe the person to have been operating or in physical control of the locomotive engine while under the influence" of alcohol or other illegal controlled substances.... Third, "reasonable grounds to believe" would have to be interpreted to mean ***605** something other than "probable cause." ... Finally, a Louisiana officer would have to order such testing without actually having "probable cause."

Id. at 858; *see also Chandler v. Miller,* 520 U.S. 305, 309–10, 318–22, 117 S.Ct. 1295, 137 L.Ed.2d 513 (1997) (invalidating a state law mandating drug testing for political candidates without requiring the candidates to wait until after they were tested to challenge the law). Unlike the plaintiffs in *Warshak* and *Foster,* the Government's claims are not speculative. It has already been denied the use of § 2703(d) orders for historical cell site information by the district court.

2. Appellate jurisdiction

[6] Professor Kerr does not believe that the order denying the Government's application is a final order over which this court has appellate jurisdiction under 28 U.S.C. § 1291.[FN4] He argues instead that the Court must treat the Government's appeal as a petition for a writ of mandamus. But federal appellate courts have long treated denials of similar orders under the Wiretap Act as appealable final orders, basing their jurisdiction to review them expressly on § 1291. *See Application of the United States,* 563 F.2d 637, 641 (4th Cir.1977); *Application of the United States,* 427 F.2d 639, 642 (9th

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

Cir.1970). The Third Circuit also appears to have based its jurisdiction to review a denial of a § 2703(d) order on § 1291. *See In re Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't,* 620 F.3d 304 (3d Cir.2010); *see also* WRIGHT, MILLER & COOPER, 15B FED. PRAC. & PROC. § 3919.9 (2d ed.) ("Denial of a government application for a search warrant concludes the only matter in the district court.... Appeal is available as from a final decision."). *But see United States v. Savides,* 658 F.Supp. 1399, 1404 (N.D.Ill.1987), *aff'd sub nom. United States v. Pace,* 898 F.2d 1218 (7th Cir.1990) ("[T]he government has no right to appeal if it believes the magistrate erred in denying the warrant."). We proceed under § 1291, recognizing that an application for this type of order is an independent proceeding, not tied to any current criminal case, and that denying or granting the order finally disposes of the proceeding.[FN5]

FN4. Professor Kerr also alleges that there is an Article III problem with allowing magistrate judges to address constitutional questions. But, because the order is appealable under § 1291, the magistrate judge's opinion is subject to de novo review by a district judge. *See* FED.R.CRIM.P. 59(b)(3); *see also id.* advisory committee note (explaining that the task of clarifying whether a matter is "dispositive" and therefore subject to de novo review is left to courts, and also that "the district judge retains the authority to review any magistrate judge's decision or recommendation whether or not objections are timely filed [by the losing party]"). This plenary review of the magistrate judge's conclusions by an Article III judge satisfies the constitutional requirements of Article III. *See Peretz v. United States,* 501 U.S. 923, 939, 111 S.Ct. 2661, 115 L.Ed.2d 808 (1991); *Thomas v. Arn,* 474 U.S. 140, 154–55, 106 S.Ct. 466, 88 L.Ed.2d 435 (1985).

FN5. Particularly in the case where a court denies the Government's application despite finding that the Government has met its evidentiary burden, in contrast to a case where the court finds that the application is not supported by evidence that satisfies the relevant standard, the order is final, because in such a case the Government cannot return to the court with additional evidence sufficient to convince the court to grant its application. *Cf. Savides,* 658 F.Supp. at 1404 (" *A probable cause determination* on an application for a search warrant by a magistrate is not a final order." (emphasis added)).

B. Fourth Amendment challenge

The district court held that the SCA violates the Fourth Amendment because the Act allows the United States to obtain a court order compelling a cell phone company to disclose historical cell site records ***606** merely based on a showing of "specific and articulable facts," rather than probable cause. [FN6] We review this ruling, applying *Katz v. United States* and its progeny to determine whether the Government's acquisition of these electronic records constitutes a search or a seizure subject to the Fourth Amendment's probable cause. 389 U.S. 347, 353, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967).

FN6. Amicus Susan Freiwald expresses concern that the SCA allows executive branch officials to police themselves. We have difficulty understanding this fear. An official must prove to a neutral magistrate that his application for a § 2703(d) order meets the "specific and articulable facts" standard set by Congress. Moreover, if the official executes the order improperly, an injured party may seek judicial review of his actions. These safeguards adequately protect against executive overreaching.

The SCA regulates disclosure of stored electronic communications by service providers. With

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

regard to compelled disclosure of non-content records or other subscriber information, the Act requires the Government to, as relevant here, secure either a warrant or a court order for the records. 18 U.S.C. § 2703(c).[FN7] If the Government seeks a court order, such an order:

FN7. The Government is not required to provide notice to the subscriber. § 2703(c)(3).

> [M]ay 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 contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.
> § 2703(d). The "specific and articulable facts" standard is a lesser showing than the probable cause standard that is required by the Fourth Amendment to obtain a warrant. U.S. CONST. amend. IV; *see In re Application of the United States,* 620 F.3d at 315 (holding that "§ 2703(d) creates a higher standard than that required by the pen register and trap and trace statutes" but "a less stringent [standard] than probable cause"); *Warshak,* 631 F.3d at 291.

1. Discretion

[7] The ACLU contends that we can avoid the constitutional issue by holding that the magistrate judge had discretion under the SCA to require the Government to seek a warrant rather than a § 2703(d) order to obtain historical cell site information. In support of its argument, the ACLU relies on a Third Circuit decision in which the majority of the panel held that the SCA "gives the [magistrate judge] the option to require a warrant showing probable cause." *In re Application of the United States,* 620 F.3d at 319. The majority reached this conclusion after analyzing the text of the statute. First, it noted that an order "may be issued" by any court with jurisdiction, which is "language of permission, rather than mandate." *Id.* at 315. It concluded that Congress's use of this phrase "strongly implies court discretion." *Id.* Second, it observed that this implication was "bolstered by the subsequent use of the phrase 'only if' in the same sentence." *Id.; see* § 2703(d) ("[An order] shall issue only if the governmental entity offers specific and articulable facts that there are reasonable grounds to believe [that the records] sought, are relevant and material to an ongoing criminal investigation."). The majority explained that both the Third Circuit and the Supreme Court had determined that " 'only if' describe[s] a necessary condition, not a sufficient condition." *In re Application of the United States,* 620 F.3d at 316 (quoting *Twp. of Tinicum v. U.S. Dep't of Transp.,* 582 F.3d 482, 488 (3d Cir.2009)); *see California v.* ****607*** *Hodari D.,* 499 U.S. 621, 628, 111 S.Ct. 1547, 113 L.Ed.2d 690 (1991). Therefore it held that the specific and articulable facts standard was necessary to allow, but not sufficient to require, the magistrate judge to issue a § 2703(d) order.

This construction of the SCA, however, ignores the intervening "shall" in the provision. "The word 'shall' is ordinarily 'the language of command.' " *Alabama v. Bozeman,* 533 U.S. 146, 153, 121 S.Ct. 2079, 150 L.Ed.2d 188 (2001) (quoting *Anderson v. Yungkau,* 329 U.S. 482, 485, 67 S.Ct. 428, 91 L.Ed. 436 (1947)); *see Lexecon Inc. v. Milberg Weiss Bershad Hynes & Lerach,* 523 U.S. 26, 35, 118 S.Ct. 956, 140 L.Ed.2d 62 (1998) ("The Panel's instruction comes in terms of the mandatory 'shall,' which normally creates an obligation impervious to judicial discretion."). Including this "shall" in our interpretation of the SCA, as we should, *see Kaltenbach v. Richards,* 464 F.3d 524, 528 (5th Cir.2006) ("It is 'a cardinal principle of statutory construction' that 'a statute ought, upon the whole, to be so construed that, if it can be prevented, no clause, sentence, or word shall be superfluous, void, or insignificant.' " (quoting *TRW Inc. v. Andrews,* 534 U.S. 19, 21, 122 S.Ct. 441, 151 L.Ed.2d 339 (2001))), we reach a different conclusion from that of the Third Circuit.

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

[8] Reading the provision as a whole, we conclude that the "may be issued" language is permissive—it grants a court the authority to issue the order—and the "shall issue" term directs the court to issue the order if all the necessary conditions in the statute are met. These conditions include both the requirements specified by § 2703(b) (for orders seeking the contents of electronic communications) or those specified by § 2703(c) (for orders seeking non-content records of such communications) and the "specific and articulable facts standard" laid out in § 2703(d) itself. Therefore, to obtain an order for the historical cell site records of a particular cell phone owner, the Government may apply to a court that has jurisdiction. And that court must grant the order if the Government seeks an order (1) to "require a provider of electronic communication service or remote computing service" (2) "to disclose a [non-content] record or other information pertaining to a subscriber to or customer of such service" when the Government (3) meets the "specific and articulable facts" standard. If these three conditions are met, the court does not have the discretion to refuse to grant the order.[FN8] *See In re Application of the United States for an Order Pursuant to 18 U.S.C. § 2703(d),* 830 F.Supp.2d 114, 148 (E.D.Va.2011) ("The fact that 'only if' creates a necessary but not sufficient condition ... does not automatically create a gap in the statute that should be filled with judicial ***608** discretion. The Court considers it more likely that the 'only if' language in § 2703(d) clarifies that any conditions established by (b) and (c) are cumulative with respect to the standard set forth in paragraph (d). The default rule remains that the judicial officer 'shall issue' an order when the government meets its burden.").

FN8. The Third Circuit observed that "Congress would, of course, be aware that such a statute mandating the issuance of a § 2703(d) order without requiring probable cause and based only on the Government's word may evoke protests by cell phone users concerned about their privacy. The considerations for and against such a requirement would be for Congress to balance. A court is not the appropriate forum for such balancing." *In re Application of the United States,* 620 F.3d at 319. While we disagree with the Third Circuit that the Government need only give its word to obtain a § 2703(d) order—rather, the Government must show "specific and articulable facts"—we agree with the Third Circuit's statement of Congress's authority. But we believe Congress has weighed these considerations and set this balance. The text of the statute shows that Congress does not want magistrate judges second-guessing its calculus. *See id.* at 320 (Tashima, J., concurring) ("Granting a court unlimited discretion to deny an application for a court order, even after the government has met statutory requirements, is contrary to the spirit of the statute.").

Even if the text of the statute supported the ACLU's argument that magistrate judges have discretion to require the Government to secure a warrant for cell site information, such discretion would be beside the point here. The district court did not simply decide that the Government must secure a warrant in this case. It held, adopting the magistrate judge's conclusion, that "[w]hen the government requests records from cellular services, data disclosing the location of the telephone at the time of particular calls may be acquired only by a warrant issued on probable cause.... The standard under the Stored Communications Act is below that required by the Constitution." *See also Historical Cell Site Data,* 747 F.Supp.2d at 846 (concluding that "[c]ompelled warrantless disclosure of cell site data violates the Fourth Amendment," despite the fact that historical cell site information clearly falls within a category of data for which the SCA requires only a § 2703(d) order); *cf. In re Application of the United States,* 620 F.3d at 307–08. Thus, the district court held that all § 2703(d) orders for cell site information were unconstitutional, so it had no

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

discretion to grant such an order. *See In re Application of the United States,* 620 F.3d at 319 (holding, in a case where the magistrate judge below had not ruled on the constitutionality of the SCA, that a magistrate judge has discretion under the statute to require the Government to seek a warrant). Therefore, we cannot avoid the question of whether the SCA's authorization of § 2703(d) orders under a "specific and articulable facts" standard is constitutional.

2. The constitutional question

[9] The Government and the ACLU focus their analysis of the constitutionality of the SCA as applied to historical cell site data on distinct questions. The ACLU focuses on what information cell site data reveals—location information—and proceeds to analyze the § 2703(d) orders under the Supreme Court's precedents on tracking devices. In contrast, the Government focuses on who is gathering the data—private cell service providers, not government officers—and analyzes the provision under the Court's business records cases.

The ACLU contends that individuals have a reasonable expectation of privacy in their location information when they are tracked in a space, like the home, that is traditionally protected or when they are tracked for a longer period of time and in greater detail than society would expect.[FN9] The ACLU relies on the concurrences in *United States v. Jones,* —— U.S. ——, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012), which concluded that prolonged GPS monitoring of a vehicle could constitute a search, *id.* at 964 (Alito, J., concurring in the judgment) (joined by Justices Ginsburg, Breyer, and Kagan); *see id.* at 955 (Sotomayor, J., concurring) (expressly agreeing with Justice Alito's concurrence on this point).[FN10] ***609** The ACLU points out that individuals are only in vehicles for discrete periods, but most people carry cell phones on their person at all times, making the tracking more detailed and invasive. The Government responds that cell site data are only collected when a call is made, which is a discrete event, just like a car ride.

FN9. The ACLU argues that the extended time period—sixty days—for which the Government sought historical cell site records contravenes privacy expectations. But the Supreme Court has upheld a court order for records that included three monthly statements, or roughly ninety days of records. *United States v. Miller,* 425 U.S. 435, 438, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976).

FN10. The ACLU, as well as the magistrate judge's opinion, *Historical Cell Site Data,* 747 F.Supp.2d at 841–43, also cite the protections in the Wireless Communication and Public Safety Act of 1999 as evidence that society recognizes a privacy interest in location information, though the ACLU recognizes that, under Supreme Court precedent, statutory protections are not determinative. *See City of Ontario v. Quon,* 560 U.S. 746, 130 S.Ct. 2619, 2632, 177 L.Ed.2d 216 (2010) ("Respondents point to no authority for the proposition that the existence of statutory protection renders a search *per se* unreasonable under the Fourth Amendment. And the precedents counsel otherwise."). But the SCA is a statute as well, and there is little reason to think that absence of statutory protection for a certain type of information is any less evidence of society's *lack* of a privacy interest in that information than presence of legal protection is evidence of such an interest.

Moreover, the Government argues that cell site information is less precise than GPS location information. It contends that these data are not sufficiently accurate to reveal when someone is in a private location such as a home. But the ACLU points out that the reason that the Government seeks such information is to locate or track a suspect in a criminal investigation. The data must be precise enough to be useful to the Government,

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

which would suggest that, at least in some cases, it can narrow someone's location to a fairly small area. *See* FCC Commercial Mobile Services, 47 C.F.R. § 20.18(h)(1) (2012) (requiring cell phone carriers to have, by 2012, the ability to locate phones within 100 meters of 67% of calls and 300 meters for 95% of calls for network based calls, and to be able to locate phones within 50 meters of 67% of calls and 150 meters of 95% of calls for hand-set based calls). And the Supreme Court held in *United States v. Karo* that without a warrant the Government cannot determine by means of a beeper whether a particular article (in that case a cannister of ether) is in an individual's home at a particular time. 468 U.S. 705, 719, 104 S.Ct. 3296, 82 L.Ed.2d 530 (1984). In response, the Government argues that a pen register can similarly locate someone to his home. If a person makes a call from his home landline, he must be located in his home at the landline's receiver. Yet the Court in *Smith v. Maryland* nevertheless sanctioned the warrantless use of pen registers, installed by the phone company at the request of police, to record the numbers dialed from particular landlines. 442 U.S. 735, 745–46, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979).

[10] This argument highlights the difference between the Government's and the ACLU's approaches to this issue. Both *Karo* and *Smith* involved the Government's acquisition of information about the interior of a home: that a particular canister was located in the home or that a person was calling particular numbers from a phone in the home. But in *Karo* (as in *Jones*), the Government was the one collecting and recording that information. And this is the distinction on which the Government's affirmative argument turns. The Government recognizes that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." *Katz,* 389 U.S. at 351, 88 S.Ct. 507; *see also id.* at 350–51, 88 S.Ct. 507 ("[T]he Fourth Amendment cannot be translated into a general constitutional 'right to privacy.' That Amendment protects individual privacy against certain kinds of *governmental intrusion*.... But the protection of a person's general right to privacy—his right to be let alone by *other people* —is, like the protection of his property and of his very life, left largely to the law of the individual States." (emphasis added)).

***610** Therefore, the Government, when determining whether an intrusion constitutes a search or seizure, draws a line based on whether it is the Government collecting the information or requiring a third party to collect and store it, or whether it is a third party, of its own accord and for its own purposes, recording the information. Where a third party collects information in the first instance for its own purposes, the Government claims that it can obtain this information later with a § 2703(d) order, just as it can subpoena other records of a private entity. *Compare Smith,* 442 U.S. at 743, 99 S.Ct. 2577 (finding significant that "the phone company does in fact record this information *for a variety of legitimate business purposes* " (emphasis added)), *with Jones,* 132 S.Ct. at 964 (Alito, J., concurring in the judgment) (expressing concern over the application of existing Fourth Amendment doctrine to "the use of GPS tracking technology *for law enforcement purposes* " (emphasis added)). We agree.

[11] This question of *who* is recording an individual's information initially is key because:

> [T]he individual must occasionally transact business with other people. When he does so, he leaves behind, as evidence of his activity, the records and recollections of others. He cannot expect that these activities are his private affair. To the extent an individual knowingly exposes his activities to third parties, he surrenders Fourth Amendment protections, and, if the Government is subsequently called upon to investigate his activities for possible violations of the law, it is free to seek out these third parties, to inspect their records, and to probe their recollections for evidence.

Reporters Comm. for Freedom of Press v. Am. Tel. & Tel. Co., 593 F.2d 1030, 1043

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

(D.C.Cir.1978). Moreover, "[t]he fortuity of whether or not the [third party] in fact elects to make a quasi-permanent record" of information conveyed to it "does not ... make any constitutional difference." *Smith,* 442 U.S. at 745, 99 S.Ct. 2577. The third party can store data disclosed to it at its discretion. And once an individual exposes his information to a third party, it can be used for any purpose, as "[i]t is established that, when a person communicates information to a third party *even on the understanding that the communication is confidential,* he cannot object if the third party conveys that information or records thereof to law enforcement authorities." *SEC v. Jerry T. O'Brien, Inc.,* 467 U.S. 735, 743, 104 S.Ct. 2720, 81 L.Ed.2d 615 (1984) (emphasis added).[FN11]

FN11. Although the ACLU contends that this sort of compulsory process requires notice and an opportunity to litigate the order's validity before it is executed, the Government notes that it is the party who owns the records, not the party whose information is recorded, that has this right to challenge the order. *See Jerry T. O'Brien,* 467 U.S. at 743, 104 S.Ct. 2720 (concluding that Supreme Court precedents "disable respondents from arguing that notice of subpoenas issued to third parties is necessary to allow a target to prevent an unconstitutional search or seizure of his papers"). The SCA provides that "[a] governmental entity receiving records or information [of non-content data] is not required to provide notice to a subscriber or customer" before or after government officials obtain this information. § 2703(c)(3). Insofar as the ACLU believes that the SCA is constitutionally problematic because it does not require these officials to ever disclose to the subscriber that they sought and obtained his non-content records—whether or not information gleaned from the records led to a criminal prosecution, *cf. Jones,* 132 S.Ct. at 964 (showing special concern for situations where government officials " *secretly* monitor" individuals (emphasis added))—we note that nothing in the non-content records provisions of the SCA prevents cell service providers from informing their subscribers of such government requests.

***611** The Government does concede that the subpoenaed third party must have possession of—the right to control—the records before officials can require it to turn them over. The Government, therefore, distinguishes cases where a landlord or hotel manager merely has the right to enter the apartment or room of another. The Government acknowledges that "the government may not subpoena the landlord to produce the tenant's personal papers from her apartment." However, it contrasts these situations from the one presented in *United States v. Miller,* 425 U.S. 435, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976). In *Miller,* the Court rejected a bank depositor's Fourth Amendment challenge to a subpoena of bank records because, as the bank was a party to the transactions, the records belonged to the bank. *Id.* at 440–41, 96 S.Ct. 1619 ("[T]he documents subpoenaed here are not respondent's private papers.... [R]espondent can assert neither ownership nor possession. Instead, these are the business records of the bank[ ].... [They] pertain to transactions to which the bank was itself a party." (citation and internal quotation marks omitted)).

This qualification that the right to possession hinges on whether the third party created the record to memorialize its business transaction with the target, rather than simply recording its observation of a transaction between two independent parties, recently gained context and support from a case decided by the Sixth Circuit. In that case, *United States v. Warshak,* the court of appeals held that the "government may not compel a commercial [internet service provider] to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause." 631 F.3d 266, 288 (6th Cir.2010). The court reasoned that the

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

emails were communications between two subscribers, not communications between the service provider and a subscriber that would qualify as business records. The provider was merely the "intermediary." *Id.* at 286.

Defining business records as records of transactions to which the record-keeper is a party also fits well with the historical and statutory distinction between communications content and addressing information. *See United States v. Forrester,* 512 F.3d 500, 511 (9th Cir.2008) ("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.") (collecting cases); *see, e.g.,* 18 U.S.C. § 2703(b)-(c). Communications content, such as the contents of letters, phone calls, and emails, which are not directed to a business, but simply sent via that business, are generally protected. However, addressing information, which the business needs to route those communications appropriately and efficiently are not. *See Smith,* 442 U.S. at 741, 99 S.Ct. 2577 (finding significant that pen registers, unlike the listening device employed in *Katz,* "do not acquire the *contents* of communications" and do not require a warrant); *Forrester,* 512 F.3d at 511 ("The government's surveillance of e-mail addresses also may be technologically sophisticated, but it is conceptually indistinguishable from government surveillance of physical mail.... E-mail, like physical mail, has an outside address 'visible' to the third-party carriers that transmit it to its intended location, and also a package of content that the sender presumes will be read only by the intended recipient.").

Under this framework, cell site information is clearly a business record. The cell service provider collects and stores historical cell site data for its own business purposes, perhaps to monitor or optimize service***612** on its network or to accurately bill its customers for the segments of its network that they use. The Government does not require service providers to record this information or store it. The providers control what they record and how long these records are retained. The Government has neither "required [n]or persuaded" providers to keep historical cell site records. *Jones,* 132 S.Ct. at 961 (Alito, J., concurring in the judgment). In the case of such historical cell site information, the Government merely comes in after the fact and asks a provider to turn over records the provider has already created.

Moreover, these are the providers' own records of transactions to which it is a party. The caller is not conveying location information to anyone other than his service provider. He is sending information so that the provider can perform the service for which he pays it: to connect his call. And the historical cell site information reveals his location information for addressing purposes, not the contents of his calls.[FN12] The provider uses this data to properly route his call, while the person he is calling does not receive this information.

FN12. The Ninth Circuit has similarly concluded that "e-mail to/from addresses and IP addresses constitute addressing information and do not necessarily reveal any more about the underlying contents of communication than do phone numbers." *Forrester,* 512 F.3d at 510. It noted that:

> Like IP addresses, certain phone numbers may strongly indicate the underlying contents of the communication; for example, the government would know that a person who dialed the phone number of a chemicals company or a gun shop was likely seeking information about chemicals or firearms. Further, when an individual dials a pre-recorded information or subject-specific line, such as sports scores, lottery results or phone sex lines, the phone number may even show that the caller had access to specif-

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

> ic content information. Nonetheless, the Court in *Smith* and *Katz* drew a clear line between unprotected addressing information and protected content information that the government did not cross here.
>
> *Id.* These observations are equally applicable to historical cell site data.

The ACLU points out that this conveyance of location information to the service provider nevertheless must be voluntary in order for the cell phone owner to relinquish his privacy interest in the data. The ACLU asserts that here it is not. According to the ACLU, "[w]hen a cell phone user makes or receives a call, there is no indication to the user that making or receiving that call will ... locate the caller." A user cannot voluntarily convey something which he does not know he has.

The Government disputes the assertion that cell phone users do not voluntarily convey location information. It contends that the users know that they convey information about their location to their service providers when they make a call and that they voluntarily continue to make such calls. We agree.

In *Smith,* the Supreme Court recognized that:

> All telephone users realize that they must "convey" phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills.

442 U.S. at 742, 99 S.Ct. 2577. Furthermore, it observed that "[m]ost phone books tell subscribers, on a page entitled 'Consumer Information,' that the company 'can frequently help in identifying to the authorities the origin of unwelcome and troublesome calls.' " *Id.* at 742–43, 99 S.Ct. 2577.

***613** A cell service subscriber, like a telephone user, understands that his cell phone must send a signal to a nearby cell tower in order to wirelessly connect his call. *See United States v. Madison,* No. 11–60285–CR, 2012 WL 3095357, at *8 (S.D.Fla. July 30, 2012) (unpublished) ("[C]ell-phone users have knowledge that when they place or receive calls, they, through their cell phones, are transmitting signals to the nearest cell tower, and, thus, to their communications service providers."). Cell phone users recognize that, if their phone cannot pick up a signal (or "has no bars"), they are out of the range of their service provider's network of towers. And they realize that, if many customers in an area attempt to make calls at the same time, they may overload the network's local towers, and the calls may not go through. Even if this cell phone-to-tower signal transmission was not "common knowledge," *California v. Greenwood,* 486 U.S. 35, 40, 108 S.Ct. 1625, 100 L.Ed.2d 30 (1988), the Government also has presented evidence that cell service providers' and subscribers' contractual terms of service and providers' privacy policies expressly state that a provider uses a subscriber's location information to route his cell phone calls. In addition, these documents inform subscribers that the providers not only use the information, but collect it. *See also Madison,* 2012 WL 3095357, at *8 ("Moreover, the cell-phone-using public knows that communications companies make and maintain permanent records regarding cell-phone usage, as many different types of billing plans are available.... Some plans also impose additional charges when a cell phone is used outside its 'home area' (known commonly as 'roaming' charges). In order to bill in these different ways, communications companies must maintain the requisite data, including cell-tower information."). Finally, they make clear that providers will turn over these records to government officials if served with a court order. Cell phone users, therefore, understand that their service providers record their location information when they use their phones at least to the same extent that the landline users in *Smith* understood that the phone company recorded the numbers they dialed.

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

Their use of their phones, moreover, is entirely voluntary. *See United States v. Skinner,* 690 F.3d 772, 777 (6th Cir.2012) ("There is no Fourth Amendment violation because Skinner did not have a reasonable expectation of privacy in the data given off by his voluntarily procured pay-as-you-go cell phone."). The Government does not require a member of the public to own or carry a phone. As the days of monopoly phone companies are past, the Government does not require him to obtain his cell phone service from a particular service provider that keeps historical cell site records for its subscribers, either. And it does not require him to make a call, let alone to make a call at a specific location.

Nevertheless, the ACLU argues that, while an individual's use of his phone may be voluntary, he does not voluntarily convey his cell site information because he does not *directly* convey it to his service provider. The only information he directly conveys is the number he dials. *See In re Application of the United States,* 620 F.3d at 317 ("[W]hen a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed."). This crabbed understanding of voluntary conveyance would lead to absurd results. For example, if a user programmed a contact's telephone number into his phone's speed dial memory, he would only need to dial the speed dial reference number to make the call. Would that mean that the Government would be unable to obtain the contact's actual telephone number from his service provider? Clearly not. The contact's***614** telephone number is necessary for the service provider to connect the call; the user is aware of this fact; therefore, he is aware that he is conveying that information to the service provider and voluntarily does so when he makes the call. [FN13] A similar analysis for cell site information leads to the conclusion that a user voluntarily conveys such information when he places a call, even though he does not directly inform his service provider of the location of the nearest cell phone tower. Because a cell phone user makes a choice to get a phone, to select a particular service provider, and to make a call, and because he knows that the call conveys cell site information, the provider retains this information, and the provider will turn it over to the police if they have a court order, he voluntarily conveys his cell site data each time he makes a call.

FN13. In an analogous context, when a customer makes a credit card purchase at a store or restaurant, he does not *directly* convey the location of the transaction to his credit card company. Nevertheless, law enforcement officers can obtain his credit card records from the company with a subpoena, *see, e.g., United States v. Maturo,* 982 F.2d 57, 59 (2d Cir.1992) (DEA agents obtained a subpoena for the credit card records of an investigatory target.), and use them to track his location, *see, e.g., United States v. Kragness,* 830 F.2d 842, 865 (8th Cir.1987) ("The government introduced credit-card records and an airline-ticket stub which show that [the defendant] traveled from Minneapolis/St. Paul to Miami on August 16, 1980."); *see also* 12 U.S.C. §§ 3402, 3407, 3409 (prescribing that federal officials can obtain an individual's financial records, such as credit card statements, pursuant to judicial subpoena served on his financial institution if "there is reason to believe that the records sought are relevant to a legitimate law enforcement inquiry," and, subject to certain exceptions, the individual has notice and an opportunity to object to the disclosure before it occurs).

Finally, the ACLU argues that advances in technology have changed society's reasonable expectations of privacy in information exposed to third parties. *See Jones,* 132 S.Ct. at 963–64 (Alito, J., concurring in the judgment) ("In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but prac-

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

tical.... Devices like the one used in the present case, however, make long-term monitoring relatively easy and cheap."); *see also id.* at 957 (Sotomayor, J., concurring). We agree that technological changes can alter societal expectations of privacy. *See id.* at 962 (Alito, J., concurring) ("Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes. New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable."). At the same time, "[l]aw enforcement tactics must be allowed to advance with technological changes, in order to prevent criminals from circumventing the justice system." *Skinner,* 690 F.3d at 778 (citing *United States v. Knotts,* 460 U.S. 276, 284, 103 S.Ct. 1081, 75 L.Ed.2d 55 (1983)). Therefore, "[i]n 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 in the judgment).

Congress has crafted such a legislative solution in the SCA. The statute conforms to existing Supreme Court Fourth Amendment precedent. This precedent, as it now ***615** stands, does not recognize a situation where a conventional order for a third party's voluntarily created business records transforms into a Fourth Amendment search or seizure when the records cover more than some specified time period or shed light on a target's activities in an area traditionally protected from governmental intrusion. We decline to create a new rule to hold that Congress's balancing of privacy and safety is unconstitutional.[FN14]

FN14. The Government also argues on appeal that the district court erred by overruling the Government's objections to the magistrate judge's judicially-noticed findings of fact. Because we hold that the magistrate judge had no discretion to deny the Government's application for a § 2703(d) order, we need not reach the issue of whether its judicial notice of facts was improper.

[12] We understand that cell phone users may reasonably want their location information to remain private, just as they may want their trash, placed curbside in opaque bags, *Greenwood,* 486 U.S. at 40–41, 108 S.Ct. 1625, or the view of their property from 400 feet above the ground, *Florida v. Riley,* 488 U.S. 445, 451, 109 S.Ct. 693, 102 L.Ed.2d 835 (1989), to remain so. But the recourse for these desires is in the market or the political process: in demanding that service providers do away with such records (or anonymize them) or in lobbying elected representatives to enact statutory protections. The Fourth Amendment, safeguarded by the courts, protects only reasonable *expectations* of privacy.

Recognizing that technology is changing rapidly, we decide only the narrow issue before us. Section 2703(d) orders to obtain *historical* cell site information for specified cell phones at the points at which the user places and terminates a call are not categorically unconstitutional. We do not address orders requesting data from all phones that use a tower during a particular interval, orders requesting cell site information for the recipient of a call from the cell phone specified in the order, or orders requesting location information for the duration of the calls or when the phone is idle (assuming the data are available for these periods). Nor do we address situations where the Government surreptitiously installs spyware on a target's phone or otherwise hijacks the phone's GPS, with or without the service provider's help.

IV. CONCLUSION

Cell site data are business records and should

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

be analyzed under that line of Supreme Court precedent. Because the magistrate judge and district court treated the data as tracking information, they applied the wrong legal standard. Using the proper framework, the SCA's authorization of § 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. Moreover, as long as the Government meets the statutory requirements, the SCA does not give the magistrate judge discretion to deny the Government's application for such an order. Therefore, we VACATE district court's order and REMAND with instructions to grant the Government's applications.

DENNIS, Circuit Judge, dissenting:

In my view, this appeal should be decided by adhering to the Supreme Court's constitutional question avoidance doctrine and construing the applicable ambiguous provisions of the Stored Communications Act to require that the government must obtain a warrant in order to secure an order requiring an electronic communications provider to disclose data potentially protected by the Fourth Amendment, such ***616** as the historical cell site location data sought in this case. Because the government did not apply for a warrant, but instead sought such data based only on a showing of reasonable suspicion, the district court reached the correct result in denying the government's request for an order for the provider to disclose that data. Accordingly, I would affirm the result reached by the district court, and I respectfully dissent from the majority opinion's contrary interpretation of the Stored Communications Act and its unnecessary interpretation of the Fourth Amendment as not affording individuals protection of their historical cell site location data.

This appeal properly turns on construction of a statute, rather than on interpretation of the Fourth Amendment. Provisions of the 1986 Stored Communications Act codified at 18 U.S.C. § 2703 authorize the government to require a cellular service provider to disclose a customer's call records, "not including the contents of communications," without the customer's consent, "only when the government[ ] ... obtains a warrant" or "obtains a court order for such disclosure under subsection [2703](d)." 18 U.S.C. § 2703(c)(1)(A)-(B). A § 2703(d) order, in turn, "may be issued by any court ... of competent jurisdiction and shall issue only if the government[ ]" demonstrates reasonable suspicion "that ... the records ... are relevant and material to an ongoing criminal investigation." *Id.* § 2703(d). Critically, the statute is ambiguous as to when the government is to follow "warrant procedures" under § 2703(c)(1)(A).

The government argues that the statute nonetheless should be read as requiring courts to grant every § 2703(d) application that meets the statutory reasonable suspicion standard, regardless of the type of customer records sought. In the government's view, it need never follow "warrant procedures," notwithstanding that such procedures are the first mechanism provided for in the statute. *See id.* § 2703(c)(1)(A).

The majority adopts the government's interpretation of the statute, creating a circuit split with the only other Court of Appeals that has considered the interpretive question. *See In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't,* 620 F.3d 304, 315–17 (3d Cir.2010). By doing so, the majority is forced to confront the serious and debatable constitutional question of whether cellular customers have a legitimate Fourth Amendment privacy interest in the "cell site location information" generated when we use our phones. The substantial difficulty of this question is reflected in the Supreme Court's conscientious avoidance of similar questions regarding the Fourth Amendment implications of modern telecommunications technologies. *See United States v. Jones,* —— U.S. ——, 132 S.Ct. 945, 953–54, 181 L.Ed.2d 911 (2012); *City of Ontario v. Quon,* 560 U.S. 746, 130 S.Ct. 2619, 2629–30, 177 L.Ed.2d 216 (2010). The majority ad-

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

opts the government's position on this issue as well, holding that cellular customers do not have a Fourth Amendment privacy interest in historical cell site location information. On this point too, the majority splits from the Third Circuit, the only other Court of Appeals to have considered the issue. *See In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't,* 620 F.3d at 317–18. This divergence of authority illustrates the difficulty and uncertainty of the constitutional issue.

Respectfully, I believe that the majority's approach contravenes Supreme Court precedent applying the canon of constitutional avoidance, "[']a cardinal principle' of ***617** statutory interpretation." *See Zadvydas v. Davis,* 533 U.S. 678, 689, 121 S.Ct. 2491, 150 L.Ed.2d 653 (2001). "[T]he canon of constitutional avoidance ... is a tool for choosing between competing plausible interpretations of a statutory text, resting on the reasonable presumption that Congress did not intend the alternative which raises serious constitutional doubts." *Clark v. Martinez,* 543 U.S. 371, 381, 125 S.Ct. 716, 160 L.Ed.2d 734 (2005). Here, because the government's interpretation "give[s] rise to [a] substantial constitutional question[ ]," *see INS v. St. Cyr,* 533 U.S. 289, 300, 121 S.Ct. 2271, 150 L.Ed.2d 347 (2001), precedent requires that we "first ascertain whether a construction of the statute is fairly possible by which the constitutional question may be avoided," *United States v. Sec. Indus. Bank,* 459 U.S. 70, 78, 103 S.Ct. 407, 74 L.Ed.2d 235 (1982) (internal quotation marks omitted) (quoting *Lorillard v. Pons,* 434 U.S. 575, 577, 98 S.Ct. 866, 55 L.Ed.2d 40 (1978)).

Here, such an "alternative interpretation" is not only "fairly possible," *see St. Cyr,* 533 U.S. at 299–300, 121 S.Ct. 2271, but indeed better accords with the statute's text, structure, and purpose than the interpretation advanced by the government and adopted by the majority. Section 2703(c) may be fairly construed to provide for "warrant procedures" to be followed when the government seeks customer records that may be protected under the Fourth Amendment, including historical cell site location information. *See* 18 U.S.C. § 2703(c)(1)(A). This construction gives meaning and effect to all of the statute's words and provisions without rendering any superfluous. It also accords with the enacting Congress's intent to create a statutory framework flexible enough to permit "the law [to] advance with the technology to ensure the continued vitality of the [F]ourth [A]mendment." S.Rep. No. 99–541, at 5 (1986), 1986 U.S.C.C.A.N. 3555, 3559. Moreover, this construction effectuates a workable framework that does not require magistrates to speculate on societal expectations in ex parte application proceedings devoid of the concrete investigative facts upon which Fourth Amendment analysis depends.

Based on this analysis, I would hold that the government must obtain a warrant pursuant to § 2703(c)(1)(A) in order to compel disclosure of the cell site location records it seeks here, which may be protected from disclosure or seizure absent a warrant. Thus, I would hold that the magistrate judge and district court erred in pronouncing upon the constitutional question and therefore would vacate the constitutional ruling below. However, the magistrate and the district court reached the right result by denying the government's application for an order compelling disclosure of cell site data without a showing of probable cause. I would affirm on statutory grounds the order denying the government's § 2703(d) application with respect to historical cell site location data.

I

The Stored Communications Act was enacted as Title II of the Electronic Communications Privacy Act of 1986, P.L. 99–508 (1986). The legislation's purpose was "to update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies." S.Rep. No. 99–541, at 1 (1986), 1986 U.S.C.C.A.N. 3555, 3555. Section 2703 "details the procedures the government may

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

employ to obtain stored information from a third-party provider, depending upon whether the government is seeking the contents of a stored communication, or non-content information." *In re Application of U.S. for an Order Pursuant to 18 U.S.C. Section 2703(d),* 707 F.3d 283, 296 (4th Cir.2013) (Wilson, J., concurring) (citing 18 U.S.C. ***618** § 2703(a)-(c)). Subsection 2703(c)(1) provides in relevant part:

> 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 or customer of such service (not including the contents of the communications) only when the governmental entity—
>
> **(A)** obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; [or]
>
> **(B)** obtains a court order for such disclosure under subsection (d)....

18 U.S.C. § 2703(c)(1)(A)-(B). Subsection 2703(d) provides in pertinent part:

> A court order for disclosure under subsection (b) or (c) 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 contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.

Id. § 2703(d). The "specific and articulable facts" standard set forth in § 2703(d), *id.,* "is essentially a reasonable suspicion standard," *In re Application of U.S. for an Order Pursuant to 18 U.S.C. Section 2703(d),* 707 F.3d at 287.[FN1]

FN1. *See, e.g., United States v. Khanalizadeh,* 493 F.3d 479, 483 (5th Cir.2007) ("Officers must base their reasonable suspicion on 'specific and articulable facts,' not merely 'inarticulate hunches' of wrongdoing."); *see also Terry v. Ohio,* 392 U.S. 1, 21, 88 S.Ct. 1868, 20 L.Ed.2d 889 (1968).

The government and the majority maintain that these provisions unambiguously mean that a magistrate *must* issue a § 2703(d) order *whenever* the government's application meets the statutory reasonable suspicion standard. Under this reading, the statute never requires the government to follow the warrant procedures provided for in subsection 2703(c)(1)(A), regardless of the type of non-content records the government seeks.

Contrary to the government's argument, however, the statute is ambiguous as to when the "warrant procedures" described in subsection 2703(c)(1)(A) are to be followed. Thus, we must apply the avoidance canon, a "rule[ ] for resolving textual ambiguity," *Spector v. Norwegian Cruise Line Ltd.,* 545 U.S. 119, 140, 125 S.Ct. 2169, 162 L.Ed.2d 97 (2005), "counseling that ambiguous statutory language be construed to avoid serious constitutional doubts," *FCC v. Fox Television Stations, Inc.,* 556 U.S. 502, 516, 129 S.Ct. 1800, 173 L.Ed.2d 738 (2009).

II

"The appropriate starting point when interpreting any statute is its plain meaning." *United States v. Molina–Gazca,* 571 F.3d 470, 472 (5th Cir.2009). "In ascertaining the plain meaning of the statute, the court must look to the particular statutory language at issue, as well as the language and design of the statute as a whole." *Id.* (quoting *K Mart Corp. v. Cartier, Inc.,* 486 U.S. 281, 291, 108 S.Ct. 1811, 100 L.Ed.2d 313 (1988)). "It is 'a cardinal principle of statutory construction' that 'a statute ought, upon the whole, to be so construed that, if it can be prevented, no clause, sentence, or word shall be superfluous, void, or insignificant.' " *TRW Inc. v. Andrews,* 534 U.S. 19, 31, 122 S.Ct.

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

441, 151 L.Ed.2d 339 (2001) (quoting *Duncan v. Walker,* 533 U.S. 167, 174, 121 S.Ct. 2120, 150 L.Ed.2d 251 (2001)). "Interpretation of a word or phrase depends upon reading ***619** the whole statutory text, considering the purpose and context of the statute, and consulting any precedents or authorities that inform the analysis." *Dolan v. U.S. Postal Serv.,* 546 U.S. 481, 486, 126 S.Ct. 1252, 163 L.Ed.2d 1079 (2006).

First, the plain language of subsection 2703(d) states that an order " *may* be issued by any court that is a court of competent jurisdiction." 18 U.S.C. § 2703(d) (emphasis added); *see In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't,* 620 F.3d at 315–16 ("This is the language of permission, rather than mandate. If Congress wished that courts 'shall,' rather than 'may,' issue § 2703(d) orders whenever the intermediate standard is met, Congress could easily have said so." (citation omitted)).

The plain language of subsection 2703(d) also *prohibits* a court from issuing the statutory order if the government's application does not make out the statutory reasonable suspicion standard. The statute provides that an order "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." 18 U.S.C. § 2703(d) (emphasis added). The best plain reading of this language is simply that an order *may not issue unless* the standard is met.[FN2] In other words, a showing of reasonable suspicion clearly is a necessary condition for the issuance of a § 2703(d) order, but not a sufficient condition. Contrary to the assertions of the government and the majority, nowhere does the statute by its terms *require* a court to issue a § 2703(d) order *whenever* the government's application demonstrates reasonable suspicion.

FN2. *Cf. Barker v. Hercules Offshore,* 713 F.3d 208, 223 (5th Cir.2013) (discussing "Congress's recent clarification of 28 U.S.C. § 1441(b)" whereby instead of stating that " '[a]ny other such action *shall be removable only if none* of the ... defendants is a citizen of the State in which such action is brought,' the statute now explicitly specifies that a 'civil action otherwise removable solely on the basis of [diversity jurisdiction] *may not be removed if any* of the ... defendants is a citizen of the State in which such action is brought' " (emphasis omitted)); *Carver v. Lehman,* 558 F.3d 869, 876 n. 12 (9th Cir.2009) (" 'May ... only if' would be effectively identical to 'shall ... unless'; 'may ... if' is not.' " (elisions in original) (emphasis removed)).

The Supreme Court has specifically contrasted the meanings of "whenever" and "only if," explaining that the latter "states a *necessary,* but not a *sufficient,* condition." *California v. Hodari D.,* 499 U.S. 621, 627–28, 111 S.Ct. 1547, 113 L.Ed.2d 690 (1991). The Court reiterated this point in construing a statutory formulation similar to that here. In *Miller–El v. Cockrell,* 537 U.S. 322, 123 S.Ct. 1029, 154 L.Ed.2d 931 (2003), the Court analyzed the language of 28 U.S.C. § 2253(c)(2), which governs the standard for issuance of a certificate of appealability ("COA") to a habeas petitioner. The Court explained:

> Section 2253(c)(2) ... provides that "[a] certificate of appealability *may issue ... only if* the applicant has made a substantial showing of the denial of a constitutional right." (Emphasis added.) A "substantial showing" does not entitle an applicant to a COA; it is a necessary and not a sufficient condition. Nothing in the text of § 2253(c)(2) prohibits a circuit justice or judge from imposing additional requirements, and one such additional requirement has been approved by this Court.

Miller–El, 537 U.S. at 349, 123 S.Ct. 1029 (second and third alterations in original). Other courts have applied this same understanding of

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

"only if." *See Keweenaw Bay Indian Cmty. v. United States,* 136 ***620** F.3d 469, 475 (6th Cir.1998) (explaining that under 25 U.S.C. § 2710(d)(1), which "provid [es] that Class III gaming activities 'shall be lawful on Indian lands *only if* such activities are ... conducted in conformance with a valid Tribal–State compact,' " "[a] valid, approved compact is a necessary, but not a sufficient condition for Class III gaming"); *Williams v. Ward,* 556 F.2d 1143, 1158 n. 6 (2d Cir.1977) (characterizing the statutory formulations "release ... shall ... be granted ... *only if* ..." and "no prisoner shall be released on parole *unless* ..." as both "phrased ... as necessary rather than sufficient conditions" (emphasis added)). The Third Circuit's discussion of this point in its recent analysis of § 2703(d) is illustrative:

> [T]he "phrase 'only if' describe[s] a necessary condition, not a sufficient condition[.]' ... [W]hile a 'necessary condition describes a prerequisite [,] a 'sufficient condition is a guarantee[.]' ... [For] example[,] ... while "a team may win the World Series *only if* it makes the playoffs ... a team's meeting the necessary condition of making the playoffs does not guarantee that the team will win the World Series." In contrast, "winning the division is a sufficient condition for making the playoffs because a team that wins the division is ensured a spot in the playoffs ... [and thus] a team makes the playoffs *if* it wins its division."

In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d at 317 (some alterations in original) (citations omitted) (quoting *Township of Tinicum v. U.S. Dep't of Transp.,* 582 F.3d 482, 489–90 (3d Cir.2009)).

Following the government, the majority argues that this reading violates the superfluity canon by "ignor[ing]" the word "shall," Maj. Op. at 606–07, in § 2703(d)'s statement that an "order may be issued by any court that is a court of competent jurisdiction and *shall* issue only if" reasonable suspicion is shown, 18 U.S.C. § 2703(d) (emphasis added). However, the government's own interpretation renders superfluous the word "only" in the very same provision. That is, under the government's reading, the statute ought to simply say that an "order may be issued by any court that is a court of competent jurisdiction and shall issue ... if the" government's application meets the statutory standard. *See id.; see also United States v. Nordic Village, Inc.,* 503 U.S. 30, 32, 112 S.Ct. 1011, 117 L.Ed.2d 181 (1992) ("[It is a] settled rule that a statute must, if possible, be construed in such fashion that every word has some operative effect."); *Carver,* 558 F.3d at 876 n. 12 ("The distinction between 'if' and 'only if[ ]' ... is not a mere quibble over vocabulary—it goes right to the heart of whether [a condition is a] necessary or sufficient condition[ ]....").

The government's argument would have some force if Congress had *actually* omitted the word "only" from the phrase "shall issue only if," as the government apparently believes Congress intended. *See In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't,* 620 F.3d at 317 ("The difficulty with the Government's argument is that the statute does contain the word 'only' and neither we nor the Government is free to rewrite it."). Indeed, the warrant provision of the Federal Rules of Criminal Procedure—specifically adverted to in § 2703(c)(1)(A) and thus plainly part of the statutory context within which the text must be read [FN3] —would have served as ***621** a ready model. Rule 41 requires that "[a]fter receiving an affidavit or other information, a magistrate judge—or ... authorized ... judge of a state court of record— *must issue the warrant if there is probable cause* to search for and seize a person or property or to install and use a tracking device." Fed.R.Crim.P. 41(d)(1) (emphasis added). Similarly, in a related section of Title 18, Congress explicitly provided for mandatory issuance of surveillance orders. [FN4] Section 3123 governs "[i]ssuance of an order for a pen register or a trap and trace device" and mandates that "upon an application" by a government attorney for such a

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

device, "the court *shall* enter an ex parte order authorizing the installation and use of [the device], *if* the ... information likely to be obtained ... is relevant to an ongoing criminal investigation." 18 U.S.C. § 3123(a)(1) (emphasis added).[FN5] In rejecting the same interpretation of the statute advanced by the government here, the Third Circuit described "th[is] difference between 'shall ... if' (for a pen register) and 'shall ... only if' (for an order under § 2703(d))" as "a powerful argument to which the Government does not persuasively respond." *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't,* 620 F.3d at 315–16; *see also Carver,* 558 F.3d at 876 n. 12 (noting the critical semantic "distinction between 'if' and 'only if' ").

FN3. "It is a 'fundamental canon of statutory construction that the words of a statute must be read in their context and with a view to their place in the overall statutory scheme.' " *FDA v. Brown & Williamson Tobacco Corp.,* 529 U.S. 120, 133, 120 S.Ct. 1291, 146 L.Ed.2d 121 (2000). Although "[t]he Federal Rules ... are not enacted by Congress, ... 'Congress participates in the rulemaking process,' " and "the Rules do not go into effect until Congress has had at least seven months to look them over." *Bus. Guides, Inc. v. Chromatic Commc'ns Enters., Inc.,* 498 U.S. 533, 552, 111 S.Ct. 922, 112 L.Ed.2d 1140 (1991) (citation omitted) (citing 28 U.S.C. § 2074 (Rules Enabling Act)). Thus, courts "must assume that Congress [is] aware of th[e] [Federal] [R]ule[s] [of Criminal Procedure] when [legislation is] drafted." *United States v. Mitchell,* 723 F.2d 1040, 1046 (1st Cir.1983); *see also, e.g., United States v. Thompson,* 287 F.3d 1244, 1250 (10th Cir.2002) ("Federal Rule of Criminal Procedure 6(f) sheds further light on the meaning of 'found' in 18 U.S.C. § 3282.").

FN4. "We assume that Congress is aware of existing law when it passes legislation." *Miles v. Apex Marine Corp.,* 498 U.S. 19, 32, 111 S.Ct. 317, 112 L.Ed.2d 275 (1990). Additionally, "the meaning of one statute may be affected by other Acts." *Brown & Williamson Tobacco Corp.,* 529 U.S. at 133, 120 S.Ct. 1291; *see also Green v. Bock Laundry Machine Co.,* 490 U.S. 504, 528, 109 S.Ct. 1981, 104 L.Ed.2d 557 (1990) (Scalia, J., concurring) ("The meaning of terms on the statute books ought to be determined, [in part] ... on the basis of which meaning is ... most compatible with the surrounding body of law into which the provision must be integrated—a compatibility which, by a benign fiction, we assume Congress always has in mind."); *cf. Keene Corp. v. United States,* 508 U.S. 200, 208, 113 S.Ct. 2035, 124 L.Ed.2d 118 (1993) ("[W]here Congress includes particular language in one section of a statute but omits it in another ..., it is generally presumed that Congress acts intentionally in the disparate inclusion or exclusion." (alterations in original) (quoting *Russello v. United States,* 464 U.S. 16, 23, 104 S.Ct. 296, 78 L.Ed.2d 17 (1983))).

FN5. This distinct "if ... shall" formulation also appears in an analogous statute governing the issuance of orders for the production of records by judges of the Foreign Intelligence Surveillance Court. *See* 50 U.S.C. § 1861(c)(1) (providing that, upon government application for an order requiring the production of records for a counter-terrorism investigation, " *if* the judge finds that the application meets the [statutory] requirements"—including "a statement of facts showing that there are reasonable grounds to believe that the [records] sought are relevant to an authorized investigation"—the judge *shall* enter an ex parte order as requested" (emphasis added)).

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

Accordingly, it cannot be said that the only plausible construction of the statute is that a magistrate must issue a § 2703(d) order whenever the government demonstrates reasonable suspicion. Because the ***622** statute is at least ambiguous as to when warrant procedures are to be followed, if the government's interpretation "raise[s] serious constitutional problems, [we must] construe the statute to avoid such problems unless such construction is plainly contrary to the intent of Congress." *Edward J. DeBartolo Corp. v. Fla. Gulf Coast Bldg. & Constr. Trades Council,* 485 U.S. 568, 575, 108 S.Ct. 1392, 99 L.Ed.2d 645 (1988).

III

The government's interpretation raises the question of whether § 2703(c) offends the Fourth Amendment by authorizing law enforcement to obtain cell site location information without a warrant, which in turn depends on whether cellular customers have a reasonable expectation of privacy in that information. *See, e.g., Kyllo v. United States,* 533 U.S. 27, 33, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001) ("[A] Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable." (citing *Katz v. United States,* 389 U.S. 347, 361, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967) (Harlan, J., concurring))). This constitutes a "substantial constitutional question[ ]," *see St. Cyr,* 533 U.S. at 300, 121 S.Ct. 2271, requiring application of the avoidance canon.

As the Eleventh Circuit recently observed, the Supreme Court has "underscore[d] its disinclination to establish broad precedents as to privacy rights vis-a-vis electronic devices and emerging technologies" because of "the difficulty in determining what privacy expectations are reasonable." *Rehberg v. Paulk,* 611 F.3d 828, 845 (11th Cir.2010) (citing *City of Ontario v. Quon,* 560 U.S. 746, 130 S.Ct. 2619, 2630, 177 L.Ed.2d 216 (2010)). In *Quon,* the Supreme Court cautioned that "[t]he judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear." 130 S.Ct. at 2629. The Court avoided setting forth "[a] broad holding concerning employees' privacy expectations vis-à-vis employer-provided technological equipment." *Id.* at 2630. Instead, the Court held it "preferable to dispose of th[e] case on narrower grounds." *Id.* The Court achieved this narrower disposition by "assum[ing] several propositions *arguendo,* " including that a municipal police officer "ha[s] a reasonable expectation of privacy in the text messages sent on the pager provided to him by the City." *Id.* Particularly relevant here, the Court explained:

> In *Katz,* the Court relied on its own knowledge and experience to conclude that there is a reasonable expectation of privacy in a telephone booth. [*Katz,* 389 U.S. at 360–61, 88 S.Ct. 507 (Harlan, J., concurring).] It is not so clear that courts at present are on so sure a ground.... Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior.
>
> *Quon,* 130 S.Ct. at 2629.

Similarly, every member of the Court acknowledged last year that law enforcement's access to the location information generated by cell phones raises serious constitutional questions. *United States v. Jones,* ——U.S. ——, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012). In *Jones,* the Court unanimously held that attaching a global positioning system ("GPS") tracking device to a car and monitoring the car's movements without a valid warrant violated the Fourth Amendment, but divided in its reasoning. Notably, a majority eschewed engaging with the "particularly vexing problems" of applying a privacy analysis, *id.* at 953, and instead held that a search had occurred because of the trespass inherent in "physically occup[ying] private property ***623** for the purpose of obtaining information," *id.* at 949; *see also id.* at 950 ("The Government contends that ... Jones had no 'reasonable expectation of privacy' in ... the locations of the Jeep on the public roads, which were visible to all. But we need

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

not address the Government's contentions, because Jones's Fourth Amendment rights do not rise or fall with the *Katz* formulation."). The Court explained that even though "[i]t may be that [obtaining four weeks of location information] through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, ... [*Jones*] d[id] not require [the Court] to answer that question," which would "lead[ ] ... needlessly into additional thorny problems." *Id.* at 953–54. The Court noted that "[it] may have to grapple with these 'vexing problems' in some future case." *Id.* at 954.

Justice Sotomayor cast the critical fifth vote in support of the majority opinion. However, her concurrence expressed serious doubt about extending the third party records doctrine applied in *Smith v. Maryland,* 442 U.S. 735, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979) [FN6] —and relied upon by today's majority—to location information generated by modern devices such as "GPS-enabled smartphones." *Jones,* 132 S.Ct. at 955–57 (Sotomayor, J., concurring). Justice Sotomayor explained:

> FN6. *Smith* held that no Fourth Amendment "search" occurred, and thus "no warrant was required," when the government used a "pen register" to obtain the numbers that a telephone customer dialed because even if the customer "entertained [an] actual [i.e., subjective] expectation of privacy in the phone numbers he dialed, ... his expectation was not 'legitimate,' because the customer "voluntarily conveyed to [the phone company] information that it had facilities for recording and that it was free to record," such that the customer thereby "assumed the risk that the information would be divulged to police." 442 U.S. at 742–44, 99 S.Ct. 2577.

> [In future cases] considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements[,] ... it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.... I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.

Id. at 957 (citations omitted); *see also id.* at 956 n. * ("Owners of GPS-equipped ... smartphones do not contemplate that these devices will be used to enable covert surveillance of their movements."). Significantly, Justice Sotomayor explained that she "join[ed] the majority's opinion" "because the Government's physical intrusion on Jones' Jeep" made "[r]esolution of these *difficult questions* ... unnecessary." *Id.* at 957 (emphasis added). Justice Alito, writing for four justices, expressed similar concerns. *See id.* at 963 (Alito, J., concurring in the judgment) ("Recent years have seen the emergence of many new devices that permit the monitoring of a person's movements.... Perhaps most significant, cell phones and other wireless devices now permit wireless carriers to track and record the location of users.... The availability and use of these and other new devices will continue to shape the average person's ***624** expectations about the privacy of his or her daily movements.").

Quon and *Jones* thus suggest that warrantless compulsion of cell site location records raises serious Fourth Amendment questions. The cautious approach taken by the Supreme Court makes clear that lower courts venture onto uncertain terrain in applying a reasonable expectation of privacy analysis to this law enforcement practice. Justice Sotomayor's decisive concurrence in *Jones* warns us not

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

to "assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection." *See id.* at 957 (Sotomayor, J., concurring). "Although dicta, we do take such pronouncements from the Supreme Court seriously." *Croft v. Perry,* 624 F.3d 157, 164 (5th Cir.2010). The divergent conclusions reached by the Third Circuit and today's majority starkly illustrate this uncertainty.[FN7] In light of the difficulty of the constitutional question, "there is no reason for rushing forward to resolve [it] here." *See Jones,* 132 S.Ct. at 954. Rather, as in *Jones* and *Quon,* "[p]rudence counsels caution before ... establish[ing] far-reaching premises that define the existence, and extent, of privacy expectations." *See Quon,* 130 S.Ct. at 2629.

FN7. *See In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't,* 620 F.3d at 317–18 ("A cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way.... [I]t is unlikely that cell phone customers are aware that their cell phone providers *collect* and store historical location information. Therefore, '[w]hen a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed and there is no indication to the user that making that call will also locate the caller; when a cell phone user receives a call, he hasn't voluntarily exposed anything at all.' " (final alteration in original)).

IV

Because there is substantial doubt as to whether cell phone users have a reasonable expectation of privacy in cell site location information, it is not merely "preferable to dispose of this case on narrower grounds," *see id.,* but "incumbent upon us to read the statute to eliminate those doubts so long as such a reading is not plainly contrary to the intent of Congress," *United States v. X–Citement Video, Inc.,* 513 U.S. 64, 78, 115 S.Ct. 464, 130 L.Ed.2d 372 (1994). "This cardinal principle has its roots in Chief Justice Marshall's opinion for the Court in *Murray v. The Charming Betsy,* 6 U.S. 64, 2 Cranch 64, 118, 2 L.Ed. 208 (1804), and has for so long been applied by th [e] [Supreme] Court that it is beyond debate." *Edward J. DeBartolo Corp.,* 485 U.S. at 575, 108 S.Ct. 1392.

Rather than acknowledge this obligation, however the majority adopts the government's textually strained, constitutionally loaded construction after a cursory analysis; and boldly proceeds to pronounce upon the constitutional issue. The majority states that "we cannot avoid the [constitutional] question" because the district court below "held that all § 2703(d) orders for cell site information [are] unconstitutional." *See* Maj. Op. at 608. However, this unsupported assertion is contrary to the Supreme Court's instruction that whatever the basis for a decision below, "we *must* independently inquire whether there is another interpretation, not raising ... serious constitutional concerns, that may be fairly ascribed to [the statute]." *Edward J. DeBartolo Corp.,* 485 U.S. at 577, 108 S.Ct. 1392 (emphasis added); *accord, e.g., St. Cyr,* 533 U.S. at 299–300, 121 S.Ct. 2271 ("[I]f an otherwise acceptable construction of a statute would raise serious constitutional problems, and where an alternative interpretation of the statute is ***625** 'fairly possible,' *we are obligated* to construe the statute to avoid such problems." (emphasis added) (citations omitted)).[FN8]

FN8. Our obligation to " *independently* inquire" into plausible alternative interpretations, *see Edward J. DeBartolo Corp.,* 485 U.S. at 577, 108 S.Ct. 1392 (emphasis added), is particularly pronounced in this ex parte proceeding.

As required by these precedents, I have endeavored to "ascertain whether a construction of the statute is fairly possible by which the constitutional

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

question may be avoided." *See Sec. Indus. Bank,* 459 U.S. at 78, 103 S.Ct. 407. I conclude that such a construction is not only fairly possible, but better accords with the text, structure, and purpose of the statute than the government's interpretation.

V

A better interpretation is to read subsections 2703(c) and (d) together as implicitly directing that the warrant procedures incorporated into subsection 2703(c)(1)(A) are to be followed when law enforcement seeks records that may be protected by the Fourth Amendment. This alternative construction is both "plausible" and "fairly possible," *see Milavetz, Gallop & Milavetz, P.A. v. United States,* 559 U.S. 229, 130 S.Ct. 1324, 1334, 176 L.Ed.2d 79 (2010), and certainly is not "plainly contrary to the intent of Congress," *see X–Citement Video, Inc.,* 513 U.S. at 78, 115 S.Ct. 464; *Edward J. DeBartolo Corp.,* 485 U.S. at 575, 108 S.Ct. 1392. Rather, this construction effectuates the text, structure, and purpose of the statute.

For the reasons stated above, this alternative construction is not inconsistent with the ambiguous language of § 2703(d). Unlike the government's interpretation, this reading has the considerable virtue of "giv [ing] effect to all of th[e] [statute's] provisions." *See United States ex rel. Eisenstein v. City of New York,* 556 U.S. 928, 933, 129 S.Ct. 2230, 173 L.Ed.2d 1255 (2009). "[O]btain[ing] a warrant" is the first-listed procedure by which the government may seek to require the disclosure of non-content call records under § 2703(c). 18 U.S.C. § 2703(c)(1)(A). Subsection 2703(c)(1)(A) specifically adverts to the warrant "procedures described in the Federal Rules of Criminal Procedure" and "State warrant procedures." *Id.* § 2703(c)(1)(A); *see also, e.g.,* Fed.R.Crim.P. 41. The superfluity canon dictates that we should prefer a construction of § 2703(c) that gives meaning and significance to the warrant mechanism set forth in subsection 2703(c)(1)(A), rather than rendering this provision superfluous or insignificant. *See TRW Inc.,* 534 U.S. at 31, 122 S.Ct. 441. The construction I propose does precisely this, by construing subsection 2703(c)(1)(A) as applying when law enforcement seeks records that may be protected by the Fourth Amendment.

By contrast, the government's reading renders subsection 2703(c)(1)(A) largely insignificant if not entirely superfluous.[FN9] ***626** *See In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't,* 620 F.3d at 317 ("The Government's only retort to the argument that it would never need to get a warrant under § 2703(c)(1)(A) if it could always get [cell site location information] pursuant to an order under § 2703(d) is that the warrant reference in § 2703(c)(1)(A) is 'alive and well' because a prosecutor can 'at his or her option ... employ a single form of compulsory process (a warrant), rather than issuing a warrant for content and a separate subpoena or court order for the associated non-content records.' In other words, the Government asserts that obtaining a warrant to get [cell site location information] is a purely discretionary decision to be made by it, and one that it would make only if a warrant were, in the Government's view, constitutionally required. We believe it trivializes the statutory options to read the § 2703(c)(1)(A) option as included so that the Government may proceed on one paper rather than two." (elision in original) (citations to briefs omitted)).

FN9. I note that § 2703(d) provides that "[i]n the case of a State governmental authority, [a § 2703(d)] court order shall not issue if prohibited by the law of such State." 18 U.S.C. § 2703(d). Thus, even under the government's reading, the "State warrant procedures" adverted to in § 2703(c)(1)(A) would presumably be utilized by the law enforcement agencies of such a state. However, because this limitation on the issuance of § 2703(d) orders applies only to "State governmental authorit[ies]," the government's construction

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

> nonetheless renders superfluous § 2703(c)(1)(A)'s specific citation to the warrant "procedures set forth in the Federal Rules of Criminal Procedure." *See* 18 U.S.C. § 2703(c)(1)(A). Moreover, the language of subsection 2703(c)(1)(A) is identical to the description of warrant procedures under subsection 2703(a), in which a warrant is the only means by which the government may obtain the contents of an email stored for 180 days or less. *See* 18 U.S.C. § 2703(a).

This construction also accords with the larger structure of § 2703, which repeatedly categorizes records based on considerations of privacy and provides different and escalating mechanisms by which the government may access them. *See Brown & Williamson Tobacco Corp.,* 529 U.S. at 133, 120 S.Ct. 1291 ("A court must ... interpret [a] statute 'as a symmetrical and coherent regulatory scheme' and 'fit, if possible, all parts into an harmonious whole.' " (citations omitted)). First, subsection 2703(a) provides that the government "may require the disclosure by [an email service] of the contents of" a subscriber email stored for 180 days or less "only pursuant to a warrant." *See id.* § 2703(a). Under subsection 2703(b), the government may access the content of an email stored for longer than 180 days pursuant to either a subpoena or § 2703(d) order along with "prior notice ... to the subscriber." *Id.* § 2703(a)-(b). Subsection 2703(c) then provides four different mechanisms by which the government may access non-content call records without customer consent. *Id.* § 2703(c). To require disclosure of more extensive and revealing types of non-content information, the government must employ increasingly formal procedures. At the most permissive end of this hierarchy, a law enforcement agency conducting a telemarketing fraud investigation may obtain "the name, address and place of business of a subscriber who is engaged in telemarketing" using only "a formal written request" to the service provider. *Id.* § 2703(1)(D). To access somewhat more revealing customer information—such as a customer's "telephone connection records," "records of session times and durations," "length of service," "telephone or instrument number or other subscriber number or identity," and "means and source of payment"—the government must "use[ ] an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena." *Id.* § 2703(1)(E), (2). The government may seek information beyond such "essentially billing-related or business records," *In re Application of U.S. for an Order Pursuant to 18 U.S.C. Section 2703(d),* 707 F.3d at 297 (Wilson, J., concurring), " *only when* [it] ... obtains a warrant [or] ... a [§ 2703(d)] order," 18 U.S.C. § 2703(c)(1)(A)-(B) (emphasis added). It accords with this statutory structure to construe subsection 2703(c)(1)(A)'s warrant provision—the most formal and exacting of the procedures described—as applying to those records that may be subject to Fourth Amendment protection.

Like the statutory language and structure, the legislative history suggests that Congress drafted § 2703(c) to be flexible enough to avoid constitutional concerns ***627** that might endanger the statute's validity. The Stored Communications Act was intended "to protect privacy interests in personal and proprietary information, while protecting the Government's legitimate law enforcement needs." S.Rep. No. 99–541, at 3 (1986), 1986 U.S.C.C.A.N. 3555, 3557 (Committee Report).[FN10] The drafters were explicitly mindful of the need for privacy protections to evolve with "dramatic changes in new ... telecommunications technologies" such as "cellular ... telephones." *See id.* at *1–2. The Committee Report stated:

> FN10. "In surveying legislative history [the Supreme Court] ha [s]repeatedly stated that the authoritative source for finding the Legislature's intent lies in the Committee Reports on the bill, which 'represen[t] the considered and collective understanding of those Congressmen involved in drafting and studying proposed

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

legislation.' " *Garcia v. United States,* 469 U.S. 70, 76, 105 S.Ct. 479, 83 L.Ed.2d 472 (1984) (third alteration in original) (quoting *Zuber v. Allen,* 396 U.S. 168, 186, 90 S.Ct. 314, 24 L.Ed.2d 345 (1969)).

When the Framers of the Constitution acted to guard against the arbitrary use of Government power to maintain surveillance over citizens, there were limited methods of intrusion into the 'houses, papers, and effects' protected by the [F]ourth [A]mendment. During the intervening 200 years, development of new methods of communication and devices for surveillance has expanded dramatically the opportunity for such intrusions....

[T]he law must advance with the technology to ensure the continued vitality of the fourth amendment. Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances. Congress must act to protect the privacy of our citizens. If we do not, we will promote the gradual erosion of this precious right.

Id. at *1–2, 5 (1986). Congress was also mindful that "[i]n th[e] rapidly developing area of communications [such as] cellular non-wire telephone connections ..., distinctions such as [whether there does or does not exist a reasonable expectation of privacy] are not always clear or obvious." *Id.* at *4 (final alteration in original).[FN11]

FN11. *See also* H.R.Rep. No. 106–932, at 17 (2000) ("Currently, there are no clear legal standards governing when the government can collect location information from cell phone companies.").

As Congress is well aware, "the Constitution invests the Judiciary, not the Legislature, with the final power to construe the law." *Nationwide Mut. Ins. Co. v. Darden,* 503 U.S. 318, 325, 112 S.Ct. 1344, 117 L.Ed.2d 581 (1992). In drafting the Stored Communications Act, Congress certainly knew that a statute permitting law enforcement to access information about a suspect without a warrant or consent could be subject to constitutional challenge and potential invalidation. *See Marshall v. Barlow's, Inc.,* 436 U.S. 307, 98 S.Ct. 1816, 56 L.Ed.2d 305 (1978) (holding statute unconstitutional insofar as it purported to authorize search without warrant or warrant equivalent); *Berger v. New York,* 388 U.S. 41, 87 S.Ct. 1873, 18 L.Ed.2d 1040 (1967) (holding facially unconstitutional statute authorizing issuance of orders for electronic eavesdropping without probable cause). The drafters of the Stored Communications Act were consciously engaged in an ongoing conversation between Congress and the Court regarding privacy protections. *See, e.g.,* S.Rep. No. 99–541, at 2 (1986), 1986 U.S.C.C.A.N. 3555 (citing *Berger,* 388 U.S. 41, 87 S.Ct. 1873).[FN12]

FN12. *See also Bartnicki v. Vopper,* 532 U.S. 514, 522–23, 121 S.Ct. 1753, 149 L.Ed.2d 787 (2001) ("In *Berger,* we held that New York's broadly written statute authorizing the police to conduct wiretaps violated the Fourth Amendment. Largely in response to that decision, and to our holding in *Katz v. United States,* 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967), that the attachment of a listening and recording device to the outside of a telephone booth constituted a search, 'Congress undertook to draft comprehensive legislation both authorizing the use of evidence obtained by electronic surveillance on specified conditions, and prohibiting its use other- wise.['']").

***628** "It is presumable that Congress legislates with knowledge of our basic rules of statutory construction," *McNary v. Haitian Refugee Ctr.,* 498 U.S. 479, 496, 111 S.Ct. 888, 112 L.Ed.2d 1005 (1991), and the constitutional avoidance canon has long been recognized as "['']a cardinal principle' of statutory interpretation," *Zadvydas,* 533 U.S. at 689, 121 S.Ct. 2491. Indeed, that canon "rest[s] on

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

the reasonable presumption that Congress did not intend" its enactments to be construed so as to "raise[ ] serious constitutional doubts." *Clark,* 543 U.S. at 381, 125 S.Ct. 716. In § 2703(c), Congress appears to have created a framework capable of accommodating constitutional concerns that might arise by providing for the use of warrant procedures as a sort of safety valve by which such concerns could be avoided and thereby alleviated. Subsection 2703(c)(1)(A) strongly indicates that Congress intended warrant procedures to play a meaningful role in its legislative effort to balance "protect[ion] [of] privacy interests" with "legitimate law enforcement needs." *See* S.Rep. No. 99–541 at 3 (1986), 1986 U.S.C.C.A.N. 3555.[FN13]

FN13. *See also In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't,* 620 F.3d at 317 n. 8 ("In our experience, magistrate judges have not been overly demanding in providing warrants as long as the Government is not intruding beyond constitutional boundaries."); *cf. Johnson v. United States,* 333 U.S. 10, 13–14, 68 S.Ct. 367, 92 L.Ed. 436 (1948) ("When the right of privacy must reasonably yield to the right of search is, as a rule, to be decided by a judicial officer, not by a policeman or Government enforcement agent."); *Jones,* 132 S.Ct. at 964 (Alito, J., concurring in the judgment) ("[W]here uncertainty exists with respect to whether a certain period of GPS surveillance is long enough to constitute a Fourth Amendment search, the police may always seek a warrant.").

In observing that the government's interpretation raises serious constitutional doubts and construing § 2703 in light of that observation, I take no position on the constitutional question of whether or when the Fourth Amendment itself would require the government to obtain a warrant for cell site location records. As the Supreme Court has emphasized, "the canon of constitutional avoidance ... allows courts to *avoid* the decision of constitutional questions"; it "is not a method of adjudicating constitutional questions by other means." *Clark,* 543 U.S. at 381, 125 S.Ct. 716. In my view, we must accord Congress the respect inherent in "the reasonable presumption" upon which the avoidance canon rests, *see id.,* by reading the statute as adopted by a body mindful of the constitutional complexities of privacy legislation. Indeed, the legislative history reflects precisely such concerns. *See* S. Rep. 99–541 at 1–5 (1986), 1986 U.S.C.C.A.N. 3555; *cf. Jones,* 132 S.Ct. at 964 (Alito, J., concurring in the judgment) ("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."). Moreover, as the Supreme Court noted in *Clark,* "[i]t is not at all unusual to give a statute's ambiguous language a limiting construction called for by one of the statute's applications." *See Clark,* 543 U.S. at 380, 125 S.Ct. 716; *see also Zadvydas,* 533 U.S. at 689, 121 S.Ct. 2491 ("We have read significant limitations into [numerous] statutes in order to avoid their constitutional invalidation.").[FN14]

FN14. In *Zadvydas,* the Court "read an implicit limitation into" an immigration detention statute, 8 U.S.C. § 1231(a)(6) (1994). 533 U.S. at 689, 121 S.Ct. 2491. "[T]he Government[ ] argu[ed] that the statute ... set[ ] no 'limit on the length of time beyond the removal period that an alien who falls within one of the [statutory] categories may be detained.' " *Id.* Applying the avoidance canon in light of a potential due process problem, the Court construed the statute as implicitly "limit [ing] an alien's post-removal-period detention to a period reasonably necessary to bring about that alien's removal from the United States." *Id.* In *Clark,* the Court applied the same limiting construction to all the stat-

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

utory categories. 543 U.S. at 377–79, 125 S.Ct. 716.

Here, as with the statute construed in *Zadvydas* and *Clark,* it is not clear that Congress intended § 2703(c)'s statement that "[a] governmental entity *may* require a provider ... to disclose [non-content customer] records" without the customer's consent " *only when* the governmental entity ... obtains a warrant" or "a [§ 2703(d)] order," *see* 18 U.S.C. § 2703(c)(1) (emphasis added), to mean that the government has sole discretion as to when to follow warrant procedures. *See Zadvydas,* 533 U.S. at 697, 121 S.Ct. 2491 ("We cannot find ... any clear indication of congressional intent to grant the Attorney General the power to hold indefinitely in confinement an alien ordered removed.... The Government points to the statute's word 'may.' But while 'may' suggests discretion, it does not necessarily suggest unlimited discretion. In that respect the word 'may' is ambiguous.").

***629 VI**

Having concluded that the statute is best construed as directing that warrant procedures be followed when the government seeks non-content records that may be protected by the Fourth Amendment, I would further hold that historical cell site location records constitute one example of this potentially protected information. Thus, I would hold that the government must obtain a warrant pursuant to § 2703(A)(1)(B) when it seeks to compel disclosure of historical cell site location data, because that individual data may be constitutionally protected.

The precise nature of the cell site location records sought in the present case is a matter of some dispute. In general, however, historical cell site location information appears to consist of, at minimum, a cellular service provider's records of which "cell sites"—i.e., "cell towers" or "base stations" mounted with antennae—a particular customer's cell phone has accessed over a particular period. The briefs submitted by the government and various amici provide different accounts of the precision of the information that such records contain. The magistrate judge below premised his Fourth Amendment analysis upon a series of "findings ... based on expert testimony ... given at a [June 2010] House Judiciary Subcommittee hearing ... [intended] to educate Congress on the current state of location technology in the telecommunications industry." *In re Application of U.S. for Historical Cell Site Data,* 747 F.Supp.2d 827, 830 (S.D.Tex.2010) (Smith, M.J.). In particular, the magistrate judge looked to the testimony of Matt Blaze, "Associate Professor of Computer and Information Science, University of Pennsylvania." *Id.* at 830 n. 13; *see also id.* at 831–33 nn. 7–28. A subsequent committee report summarized Professor Blaze's testimony at the June 2010 hearing as follows:

Professor Blaze educat[ed] the Subcommittee on location technologies—specifically how different technologies interface with cell phones and locate their positions with varying degrees of specificity and precision in various types of environments, both indoors and out. Professor Blaze explained how, even if a network only records cell tower data (as opposed to GPS), the precision of that data will vary widely for any given customer over the course of a day and, for a typical user over time, some of that data will likely have locational precision similar to that of GPS. Indeed, in urban areas where providers are using microcell technology, the level of precision for cell tower location data can include individual floors and rooms within buildings.

H.R.Rep. No. 111–712, at 90 (2011).

The government disputes several of these assertions. As the majority acknowledges,***630** however, it is undisputed that "the reason that the Government seeks such information is to locate or

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

track a suspect in a criminal investigation" and that "[t]he data must be precise enough to be useful to the Government, which would suggest that, at least in some cases, it can narrow someone's location to a fairly small area." Maj. Op. at 609. Moreover, there seems to be no serious question that the precision of these records is constantly increasing as cellular service providers construct ever denser networks of base stations and substations to keep pace with consumer demand and to comply with federal regulations requiring them to provide emergency dispatchers with increasingly precise coordinates for 911 calls placed by cell phone. *See* 47 C.F.R. § 20.18(h)(1). However, I will not attempt to wade into the empirical debate as to whether or when network-based cell site location records will provide law enforcement with information regarding a suspect's location and movements that are equivalent to phone-based GPS location records.[FN15] Even were it possible to ascertain the nature of the records generated and stored by the various cellular service providers, such a determination is unnecessary here.

FN15. *Cf. Quon,* 130 S.Ct. at 2629 ("In *Katz,* the Court relied on its own knowledge and experience to conclude that there is a reasonable expectation of privacy in a telephone booth. It is not so clear that courts at present are on so sure a ground." (citation omitted)).

Although government access to cell site location information was not specifically envisioned or considered by Congress when it enacted the Stored Communications Act, presently these records appear to be the most personally revealing information that may be said to fall within § 2703(c)'s framework for the disclosure of "information pertaining to a subscriber or customer ... not including the contents of communications." *See* 18 U.S.C. § 2703(c)(1). The general character of cell site location information and the purposes for which the government seeks it make it largely analogous to GPS location information, which the Supreme Court has indicated may implicate Fourth Amendment privacy interests. *See Jones,* 132 S.Ct. at 953–54; *id.* at 955–57 (Sotomayor, J., concurring); *id.* at 963–64 (Alito, J., concurring in the judg- ment).

Accordingly, I would hold that subsection 2703(c)(1)(A) applies to historical cell site location records, such that the statute requires the government to "obtain[ ] a warrant" to compel their disclosure. *See* 18 U.S.C. § 2703(c)(1)(A).

VII

The Third Circuit recently analyzed § 2703(c) without reference to avoidance principles. In contrast to today's majority, I agree with the Third Circuit that § 2703(c) is best read as not requiring a court to issue a § 2703(d) order whenever the government's application satisfies the statutory reasonable suspicion standard. *See In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't,* 620 F.3d at 314–17. However, the Third Circuit would give effect to subsection 2703(c)(1)(A) by instructing magistrates to determine whether to insist upon warrant procedures by engaging in a *Katz*-like inquiry that "balances the Government's need ... for [cell site location] information with the privacy interests of cell phone users." *See id.* at 319.[FN16] Respectfully, it ***631** seems to me that this would require magistrates routinely to conduct a constitutional privacy analysis of the kind the Supreme Court has instructed courts to avoid whenever fairly possible.[FN17] In this respect, I believe that the Third Circuit failed to heed the Supreme Court's repeated admonitions regarding the difficulty and uncertainty of conducting this sort of privacy analysis at a time when communications technologies and our corresponding privacy expectations are both in flux.[FN18]

FN16. The Third Circuit committed the same error as today's majority by unnecessarily pronouncing upon the ultimate constitutional question of whether cellular customers have a reasonable expectation of

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

privacy in cell site location information. *See In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't,* 620 F.3d at 317–18.

FN17. Similarly, the proposal set forth in Judge Tashima's Third Circuit concurrence is at odds with avoidance principles insofar as it suggests that magistrates should attempt to determine whether issuing a § 2703(d) order "would violate the Fourth Amendment absent a showing of probable cause." *See id.* at 320 (Tashima, J., concurring).

FN18. *See Quon,* 130 S.Ct. at 2629; *see also Jones,* 132 S.Ct. at 962 (Alito, J., concurring in the judgment) ("The *Katz* expectation-of-privacy test ... involves a degree of circularity and judges are apt to confuse their own expectations of privacy with those of the hypothetical reasonable person to which the *Katz* test looks. In addition, the *Katz* test rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations. But technology can change those expectations. Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes." (citations omitted)); *cf. Rehberg,* 611 F.3d at 846 ("[T]he questions of whether Fourth Amendment principles governing a search of [a suspect]'s home also should apply to subpoenas sent to a third-party [internet service provider (ISP)] for electronic data stored on the third-party's server, and whether [the suspect] had a reasonable privacy expectation in the contents of his personal emails sent voluntarily through that third-party ISP, are complex, difficult, and 'far-reaching' legal issues that we should be cautious about resolving too broadly." (quoting *Quon,* 130 S.Ct. at 2629)).

Moreover, ex parte application proceedings conducted in the absence of concrete investigative facts provide a poor vehicle for the development of Fourth Amendment doctrine. The *Quon* Court cautioned against using "the facts in [a single] case ... to establish far-reaching" privacy principles. 130 S.Ct. at 2629. It seems to me even less prudent to set forth such principles in the context of an ex parte § 2703(d) application, in which there is literally *no factual record whatsoever.*[FN19] The speculative***632** nature of this abstract constitutional analysis confirms that § 2703(c) is best construed to provide for warrant procedures when the government seeks information pertaining to individuals that may be constitutionally protected, such as historical cell site location records.

FN19. *See Sibron v. New York,* 392 U.S. 40, 59, 88 S.Ct. 1889, 20 L.Ed.2d 917 (1968) ("The constitutional validity of a warrantless search is pre-eminently the sort of question which can only be decided in the concrete factual context of the individual case."); *Warshak v. United States,* 532 F.3d 521, 528 (6th Cir.2008) (en banc) ("In determining the ... the legitimacy of citizens' expectations of privacy, courts typically ... reach[ ] case-by-case determinations that turn on the concrete, not the general, and offer[ ] incremental, not sweeping, pronouncements of law [,] ... in two discrete, post-enforcement settings: (1) a motion to suppress in a criminal case or (2) a damages claim ... against the officers who conducted the search. In both settings, the reviewing court looks at the claim in the context of an actual, not a hypothetical, search and in the context of a developed factual record of the reasons for and the nature of the search." (citations omitted)); Orin S. Kerr, Ex Ante Regulation of Computer Search and Seizure, 96 Va. L.Rev.

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

1241, 1281 (2010) ("[E]x ante predictions of reasonableness will be more error prone than ex post assessments [because] ex ante restrictions require courts to 'slosh [their] way through the factbound morass of reasonableness' without actual facts." (third alteration in original) (footnotes omitted) (quoting *Scott v. Harris,* 550 U.S. 372, 383, 127 S.Ct. 1769, 167 L.Ed.2d 686 (2007))); *cf. Massachusetts v. EPA,* 549 U.S. 497, 517, 127 S.Ct. 1438, 167 L.Ed.2d 248 (2007) (explaining that Article III standing doctrine works to "assure that concrete adverseness which sharpens the presentation of issues upon which the court so largely depends for illumination" and "preserves the vitality of the adversarial process by assuring ... that the legal questions presented ... will be resolved, not in the rarified atmosphere of a debating society, but in a concrete factual context conducive to a realistic appreciation of the consequences of judicial action" (second elision in original)).

VIII

In sum, I conclude that the text of the Stored Communications Act is ambiguous as to when the government is to follow warrant procedures to compel disclosure of non-content customer call records. To resolve this ambiguity, I would apply the Supreme Court's constitutional avoidance jurisprudence. I would recognize that non-consensual, warrantless compulsion of customer cell site location records raises serious and debatable constitutional questions. In order to avoid these difficult questions, as we must if fairly possible, I would construe the statutory framework as implicitly directing that § 2703(c)(1)(A) warrant procedures be followed when the government seeks non-content records that may be constitutionally protected, including historical cell site location records. Thus, I would instruct magistrates to require the government to obtain a warrant pursuant to § 2703(c)(1)(A) when it seeks cell site location data. Accordingly, I would affirm the denial of the government's application to compel disclosure of such records here without consent or a warrant supported by probable cause, albeit on different grounds than those relied upon by the district court and magistrate judge. Therefore, and for the reasons set forth above, I respectfully dissent.

C.A.5 (Tex.),2013.
In re U.S. for Historical Cell Site Data
724 F.3d 600, 58 Communications Reg. (P&F) 1292

END OF DOCUMENT

© 2015 Thomson Reuters. No Claim to Orig. US Gov. Works.

SELECTED DECISIONS ADDRESSING CELL SITE LOCATION INFORMATION

APPELLATE COURTS

United States v. Davis, 785 F.3d 498 (11th Cir. May 5, 2015) (en banc)

United States v. Guerrero, 768 F.3d 351 (5th Cir. 2014)

In re Application, 724 F.3d 600, 615 (5th Cir. 2013);

United States v. Skinner, 690 F.3d 772 (6th Cir. 2012)

In re Application of United States, 620 F.3d 304, 313, 317 (3d Cir. 2010)

DISTRICT COURTS

In re Application for Telephone Information, 15-CR-90304 (N.D. Cal. Apr. 2015) (warrant required)

United States v. Cooper, 2015 WL 881578 (N.D. Cal. Mar. 2, 2015) (warrant required)

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

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

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

United States v. Giddins, ___ F. Supp. 3d ___, 2014 WL 4955472 (D. Md. 2014)

United States v. Lang, ___ F.3d ___, 2015 WL 327338 (N.D. Ill. Jan. 23, 2015)

United States v. Rogers, ___ F.3d ___, 2014 WL 5152543 (N.D. Ill. Oct. 9, 2014)

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

United States v. Caraballo, 963 F. Supp. 2d 341 (D. Vt. 2013)

In re Application, 42 F. Supp. 3d 511 (S.D.N.Y. 2014) (MJ Francis tower dump decision)

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

United States v. Salas, 2013 WL 4459858 (**E.D. Cal**. 2013)

United States v. Booker, 2013 WL 2903563 (N.D. Ga. 2013)

United States v. Rigmaiden, 2013 WL 1932800 (**D. Ariz**. 2013)

United States v. Ruby, 2013 WL 544888 (S.D. Cal. Feb. 12, 2013)

United States v. Banks, ___ F.Supp. 3d ___, 2014 WL 4594197 (D. Kans. Dept. 15, 2014)

United States v. Wilson, 2013 WL 1129199, at *6-*7 (N.D. Ga. Feb. 20, 2013) (denying suppression);

United States v. Madison, 2012 WL 3095357, at *9 (S.D. Fla. July 30, 2012) (same);

United States v. Dye, 2011 WL 1595255, at *9 (N.D. Ohio April 27, 2011)(same);

United States v. Velasquez, 2010 WL 4286276, at *5 (N.D. Cal. Oct. 22, 2010) (same)

United States v. Benford, 2010 WL 1266507, at *3 (N.D. Ind. Mar. 26, 2010) (same);

United States v. Suarez-Blanca, 2008 WL 4200156, at *8-*11 (N.D. Ga. Mar. 26, 2008) (same).

In re Application of United States, 809 F. Supp. 2d 113 (E.D.N.Y. 2011) (later, Ashburn and Herron decided on good faith)

In re Application, Misc. No.11-449 (D.D. C. Oct. 3, 2011) (C.J. Lamberth overruling MJ Facciola)

ENGROSSED SUBSTITUTE HOUSE BILL 1440

State of Washington **64th Legislature** **2015 Regular Session**

By House Public Safety (originally sponsored by Representatives Taylor, Goodman, Pollet, Scott, Condotta, Shea, G. Hunt, Young, Moscoso, Smith, Ryu, Jinkins, Magendanz, Farrell, and McCaslin)

READ FIRST TIME 02/17/15.

AN ACT Relating to prohibiting the use of a cell site simulator device without a warrant; amending RCW 9.73.260; adding a new section to chapter 9.73 RCW; and declaring an emergency.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

NEW SECTION. **Sec. 1.** A new section is added to chapter 9.73 RCW to read as follows:

The state and its political subdivisions shall not, by means of a cell site simulator device, collect or use a person's electronic data or metadata without (1) that person's informed consent, (2) a warrant, based upon probable cause, that describes with particularity the person, place, or thing to be searched or seized, or (3) acting in accordance with a legally recognized exception to the warrant requirements.

Sec. 2. RCW 9.73.260 and 1998 c 217 s 1 are each amended to read as follows:

(1) As used in this section:

(a) "Wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception, including the

use of such connection in a switching station, furnished or operated by any person engaged in providing or operating such facilities for the transmission of intrastate, interstate, or foreign communications, and such term includes any electronic storage of such communication.

(b) "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo-optical system, but does not include:

(i) Any wire or oral communication;

(ii) Any communication made through a tone-only paging device; or

(iii) Any communication from a tracking device<u>, but solely to the extent the tracking device is owned by the applicable law enforcement agency</u>.

(c) "Electronic communication service" means any service that provides to users thereof the ability to send or receive wire or electronic communications.

(d) "Pen register" means a device that records or decodes electronic or other impulses that identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached, but such term does not include any device used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business.

(e) "Trap and trace device" means a device that captures the incoming electronic or other impulses that identify the originating number of an instrument or device from which a wire or electronic communication was transmitted.

<u>(f) "Cell site simulator device" means a device that transmits or receives radio waves for the purpose of conducting one or more of the following operations: (i) Identifying, locating, or tracking the movements of a communications device; (ii) intercepting, obtaining, accessing, or forwarding the communications, stored data, or metadata of a communications device; (iii) affecting the hardware or software operations or functions of a communications device; (iv) forcing transmissions from or connections to a communications device; (v) denying a communications device access to other communications</u>

devices, communications protocols, or services; or (vi) spoofing or simulating a communications device, cell tower, cell site, or service, including, but not limited to, an international mobile subscriber identity catcher or other invasive cell phone or telephone surveillance or eavesdropping device that mimics a cell phone tower and sends out signals to cause cell phones in the area to transmit their locations, identifying information, and communications content, or a passive interception device or digital analyzer that does not send signals to a communications device under surveillance.

(2) No person may install or use a pen register ((~~or~~)), trap and trace device, or cell site simulator device without a prior court order issued under this section except as provided under subsection (6) of this section or RCW 9.73.070.

(3) A law enforcement officer may apply for and the superior court may issue orders and extensions of orders authorizing the installation and use of pen registers ((~~and~~)), trap and trace devices, and cell site simulator devices as provided in this section. The application shall be under oath and shall include the identity of the officer making the application and the identity of the law enforcement agency conducting the investigation. The applicant must certify that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

(4) If the court finds that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation and finds that there is probable cause to believe that the pen register ((~~or~~)), trap and trace device, or cell site simulator device will lead to obtaining evidence of a crime, contraband, fruits of crime, things criminally possessed, weapons, or other things by means of which a crime has been committed or reasonably appears about to be committed, or will lead to learning the location of a person who is unlawfully restrained or reasonably believed to be a witness in a criminal investigation or for whose arrest there is probable cause, the court shall enter an ex parte order authorizing the installation and use of a pen register ((~~or a~~)), trap and trace device, or cell site simulator device. The order shall specify:

(a)(i) In the case of a pen register or trap and trace device, the identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register or trap and trace device is to be attached; or

(ii) In the case of a cell site simulator device, the identity, if known, of (A) the person to whom is subscribed or in whose name is subscribed the electronic communications service utilized by the device to which the cell site simulator device is to be used and (B) the person who possesses the device to which the cell site simulator device is to be used;

(b) The identity, if known, of the person who is the subject of the criminal investigation;

(c)(i) In the case of a pen register or trap and trace device, the number and, if known, physical location of the telephone line to which the pen register or trap and trace device is to be attached and, in the case of a trap and trace device, the geographic limits of the trap and trace order; or

(ii) In the case of a cell site simulator device: (A) The telephone number or other unique subscriber account number identifying the wire or electronic communications service account used by the device to which the cell site simulator device is to be attached or used; (B) if known, the physical location of the device to which the cell site simulator device is to be attached or used; (C) the type of device, and the communications protocols being used by the device, to which the cell site simulator device is to be attached or used; (D) the geographic area that will be covered by the cell site simulator device; (E) all categories of metadata, data, or information to be collected by the cell site simulator device from the targeted device including, but not limited to, call records and geolocation information; (F) whether or not the cell site simulator device will incidentally collect metadata, data, or information from any parties or devices not specified in the court order, and if so, what categories of information or metadata will be collected; and (G) any disruptions to access or use of a communications or internet access network that may be created by use of the device; and

(d) A statement of the offense to which the information likely to be obtained by the pen register ((~~or~~)), trap and trace device, or cell site simulator device relates.

The order shall direct, if the applicant has requested, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register ((~~or~~)), trap and trace device, or cell site simulator device. An order issued under this section shall authorize the installation and use of a: (i) Pen register or a trap and trace device for a period not to exceed

sixty days; and (ii) a cell site simulator device for sixty days. An extension of the original order may only be granted upon: A new application for an order under subsection (3) of this section; and a showing that there is a probability that the information or items sought under this subsection are more likely to be obtained under the extension than under the original order. No extension beyond the first extension shall be granted unless: There is a showing that there is a high probability that the information or items sought under this subsection are much more likely to be obtained under the second or subsequent extension than under the original order; and there are extraordinary circumstances such as a direct and immediate danger of death or serious bodily injury to a law enforcement officer. The period of extension shall be for a period not to exceed sixty days.

An order authorizing or approving the installation and use of a pen register ((~~or a~~)), trap and trace device, or cell site simulator device shall direct that the order be sealed until otherwise ordered by the court and that the person owning or leasing the line to which the pen register ((~~or~~)), trap and trace device, and cell site simulator devices is attached or used, or who has been ordered by the court to provide assistance to the applicant, not disclose the existence of the pen register ((~~or~~)), trap and trace device, or cell site simulator device or the existence of the investigation to the listed subscriber or to any other person, unless or until otherwise ordered by the court.

(5) Upon the presentation of an order, entered under subsection (4) of this section, by an officer of a law enforcement agency authorized to install and use a pen register under this chapter, a provider of wire or electronic communication service, landlord, custodian, or other person shall furnish such law enforcement officer forthwith all information, facilities, and technical assistance necessary to accomplish the installation of the pen register unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such assistance is directed by a court order as provided in subsection (4) of this section.

Upon the request of an officer of a law enforcement agency authorized to receive the results of a trap and trace device under this chapter, a provider of a wire or electronic communication

service, landlord, custodian, or other person shall install such device forthwith on the appropriate line and shall furnish such law enforcement officer all additional information, facilities, and technical assistance including installation and operation of the device unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such installation and assistance is directed by a court order as provided in subsection (4) of this section. Unless otherwise ordered by the court, the results of the trap and trace device shall be furnished to the officer of a law enforcement agency, designated in the court order, at reasonable intervals during regular business hours for the duration of the order.

A provider of a wire or electronic communication service, landlord, custodian, or other person who furnishes facilities or technical assistance pursuant to this subsection shall be reasonably compensated by the law enforcement agency that requests the facilities or assistance for such reasonable expenses incurred in providing such facilities and assistance.

No cause of action shall lie in any court against any provider of a wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order under this section. A good faith reliance on a court order under this section, a request pursuant to this section, a legislative authorization, or a statutory authorization is a complete defense against any civil or criminal action brought under this chapter or any other law.

(6)(a) Notwithstanding any other provision of this chapter, a law enforcement officer and a prosecuting attorney or deputy prosecuting attorney who jointly and reasonably determine that there is probable cause to believe that an emergency situation exists that involves immediate danger of death or serious bodily injury to any person that requires the installation and use of a pen register ((~~or a~~)), trap and trace device, or cell site simulator device before an order authorizing such installation and use can, with due diligence, be obtained, and there are grounds upon which an order could be entered under this chapter to authorize such installation and use, may have installed and use a pen register ((~~or~~)), trap and trace device, or cell site simulator device if, within forty-eight hours after the

installation has occurred, or begins to occur, an order approving the installation or use is issued in accordance with subsection (4) of this section. In the absence of an authorizing order, such use shall immediately terminate when the information sought is obtained, when the application for the order is denied or when forty-eight hours have lapsed since the installation of the pen register ((~~or~~)), trap and trace device, or cell site simulator device, whichever is earlier. If an order approving the installation or use is not obtained within forty-eight hours, any information obtained is not admissible as evidence in any legal proceeding. The knowing installation or use by any law enforcement officer of a pen register ((~~or~~)), trap and trace device, or cell site simulator device pursuant to this subsection without application for the authorizing order within forty-eight hours of the installation shall constitute a violation of this chapter and be punishable as a gross misdemeanor. A provider of a wire or electronic service, landlord, custodian, or other person who furnished facilities or technical assistance pursuant to this subsection shall be reasonably compensated by the law enforcement agency that requests the facilities or assistance for such reasonable expenses incurred in providing such facilities and assistance.

(b) A law enforcement agency that authorizes the installation of a pen register ((~~or~~)), trap and trace device, or cell site simulator device under this subsection (6) shall file a monthly report with the administrator for the courts. The report shall indicate the number of authorizations made, the date and time of each authorization, whether a court authorization was sought within forty-eight hours, and whether a subsequent court authorization was granted.

(c) A law enforcement agency authorized to use a cell site simulator device in accordance with this section must: (i) Take all steps necessary to limit the collection of any information or metadata to the target specified in the applicable court order; (ii) take all steps necessary to permanently delete any information or metadata collected from any party not specified in the applicable court order immediately following such collection and must not transmit, use, or retain such information or metadata for any purpose whatsoever; and (iii) must delete any information or metadata collected from the target specified in the court order within thirty days if there is no longer probable cause to support the belief that such information or metadata is evidence of a crime.

1 NEW SECTION. **Sec. 3.** If any provision of this act or its
2 application to any person or circumstance is held invalid, the
3 remainder of the act or the application of the provision to other
4 persons or circumstances is not affected.

5 NEW SECTION. **Sec. 4.** This act is necessary for the immediate
6 preservation of the public peace, health, or safety, or support of
7 the state government and its existing public institutions, and takes
8 effect immediately.

--- END ---

66 Hastings L.J. 183

Hastings Law Journal
December, 2014

Articles

TRIGGERFISH, STINGRAYS, AND FOURTH AMENDMENT FISHING EXPEDITIONS

Brian L. **Owsley** [a1]

Copyright (c) 2014 UC Hastings College of the Law; Brian L. Owsley

Cell site simulators are an electronic surveillance device that mimics a cell tower causing all nearby cell phones to register their data and information with the cell site simulator. Law enforcement increasingly relies on these devices during the course of routine criminal investigations.

The use of cell site simulators raises several concerns. First, the federal government seeks judicial authorization to use such devices via a pen register application. This approach is problematic because a cell site simulator is different than a pen register. Moreover, the standard for issuance of a pen register is very low. Instead, this Article proposes that the applicable standard for granting a request to use a cell site simulator should be based on the Fourth Amendment probable cause standard.

Second, cell site simulators sweep up the data and information of innocent third-parties. The government fails to account for this problem. This Article proposes that the granting of an application for a cell site simulator should require a protocol for dealing with the third-party information that is captured.

***184 TABLE OF CONTENTS**

INTRODUCTION 185
I. CELL SITE SIMULATORS UTILIZE BASIC EXISTING CELLULAR TELEPHONE TECHNOLOGY 187
II. CELL SITE SIMULATORS CAPITALIZE ON EXISTING CELLULAR TECHNOLOGY TO RETRIEVE A CELL PHONE USER'S INFORMATION 191
A. BASIC OPERATIONS OF CELL SITE SIMULATORS 191
B. THE MANNER IN WHICH LAW ENFORCEMENT OFFICIALS USE CELL SITE SIMULATORS 192
III. THE DEVELOPMENT OF THE PEN REGISTER STATUTE 194
IV. FEW AVAILABLE EXAMPLES OF EITHER MOTIONS OR COURT ORDERS ADDRESS CELL SITE SIMULATORS & SIMILAR DEVICES 200
A. COURT ORDERS ADDRESSING APPLICATIONS FOR DIGITAL ANALYZERS AND CELL SITE SIMULATORS 201
1. The Central District of California 201
2. The Southern District of Texas 203
a. The Use of a Cell Site Simulator in a Prison Setting 203
b. The Use of a Cell Site Simulator to Target a Drug Dealer 204
3. The Northern District of Texas 205
4. The District of Maryland 206
5. The District of New Jersey 207
6. The District of Arizona 208

7. Other Magistrate Judges Have Acknowledged Handling Cell Site Simulator Applications 210
B. FORM APPLICATIONS AND ORDERS DRAFTED BY LAW ENFORCEMENT AGENCIES 211
1. The United States Attorneys' Bulletin 211
2. The Department of Justice Electronic SurveillanceManual 212
3. The District of Arizona Form 213
4. The Los Angeles Police Department Form 215
V. THE DEVELOPMENT OF FOURTH AMENDMENT JURISPRUDENCE 218
A. HISTORICALLY, THE FOURTH AMENDMENT WAS PROPERTY-CENTRIC 218
B. IN *KATZ*, the Supreme Court Established the Reasonable Expectation of Privacy Analysis 220
C. PEOPLE HAVE A REASONABLE EXPECTATION OF PRIVACY IN THEIR CELL PHONES, INCLUDING THE NUMBERS THEY DIAL 227
CONCLUSION 230

*185 INTRODUCTION

In recent years, traditional and online media have raised concerns about a means of electronic surveillance employed by the government that has various colorful and ominous names: TriggerFish, StingRay, AmberJack, KingFish, LoggerHead, Gossamer, Harpoon, Hailstorm, International Mobile Subscriber Identifier ("IMSI") [1] catcher, Electronic Serial Number ("ESN") [2] reader, cell site simulator, or digital analyzer. [3] The first eight names are essentially brand names of similar devices manufactured and sold by the Harris Corporation. [4] In the course of various criminal investigations, the government seeks to utilize an electronic device known as a StingRay that acts as a cell site simulator. [5] In other words, the device deceives nearby cell phones into believing that the device is a cell tower so that the cell phone's information is then downloaded into the cell site simulator. [6]

Imagine if you will, a federal agent sitting inside an unmarked van in a parking lot monitoring the activities of some subject of a criminal investigation. Inside the van the agent has an electronic surveillance device about the size of a bankers box connected to a laptop computer. With this device, the agent is targeting the subject's cell phone in a manner that the cell phone's number and other data, including, potentially, voice communications, can be downloaded. This is a great device for apprehending the bad guys. Unfortunately, this device is ***186** capturing similar information from all the cell phones in the surrounding area. So the person who lives nearby, the couple who are sitting in the coffee shop on the corner, and you as you drive by in your car--all of you are also having your cell phone information captured and downloaded into the agent's computer. Let us assume that the agent obtained some kind of judicial authorization for this electronic surveillance. Would you want your information captured and saved in a government computer forever based only on the most minimal of standards? That is what the federal government is doing through its current use of cell site simulators.

Whatever these devices are called, they have proliferated in recent years, being used by state and federal law enforcement officials as well as by American and foreign intelligence agencies. [7] Not only are large law enforcement agencies like the Los Angeles Police Department using them, [8] but small cities like Gilbert, Arizona have also acquired them. [9] This technology, which has been patented since at least 2002, [10] has often been purchased with funds from the Department of Homeland Security to assist in regional terrorism investigations. [11] However, these devices have also come to be used for routine criminal investigations, including such offenses as burglary and murder. [12]

This Article addresses the use of cell site simulators and makes three principal points. First, the government's current approach of relying on the pen register statute to justify its requests for court orders fails because cell site simulators are not pen registers and thus are not covered by the pen register statute. Second, the use of cell site simulators constitutes a Fourth Amendment search, which requires probable cause. ***187** Consequently, the proper approach is for the government to establish probable

cause in order to obtain a search warrant consistent with the Fourth Amendment. Third, the use of the cell site simulators raises privacy concerns for third parties.

This Article raises the issue of cell site simulators in two ways that have not been addressed in current scholarship. First, I provide examples of court orders that address the use of these devices that have not been probed in previous legal scholarship. Second, I analyze the statutory and constitutional framework in which the government seeks to use cell site simulators. This Article provides a brief description of cellular telephone and cell site technology that concerns devices such as cell site simulators in Part I. Next, Part II provides a detailed description of how these types of devices operate. In Part III, the discussion documents the historical development of pen registers, including their statutory history. Part IV provides the various few examples of the government's applications for cell site simulators, as well as orders addressing such applications. Part V analyzes the development of Fourth Amendment jurisprudence and discusses the use of cell site simulators in light of people's reasonable expectations of privacy. In assessing these expectations, courts have, to a certain extent, relied on decisions that shape the third party doctrine --*Smith v. Maryland* [13] and *United States v. Miller* [14] --that no longer adequately address the realities of today's cell phone technology or people's expectations of privacy. Finally, in Part VI, I conclude by making some proposals as to how to address the privacy concerns.

I. CELL SITE SIMULATORS UTILIZE BASIC EXISTING CELLULAR TELEPHONE TECHNOLOGY

To fully appreciate the significance of a cell site simulator, it is important to understand the basics of how cellular telephones work. In enacting the Electronic Communications Privacy Act ("ECPA"), Congress addressed cellular telephones, which at that time were based on radio transmission. [15] In building a network, telecommunications providers created "large service areas [[that] are divided into honeycomb-shaped segments or 'cells'--each of which is equipped with a low-power ***188** transmitter or base station which can receive and radiate messages within its parameters" from cellular phones within the providers' networks. [16] Each "cell," in turn, collects "a number of pieces of data 'regarding the strength, angle, and timing of the caller's signal measured at two or more cell sites, as well as other system information such as a listing of all cell towers in the market area, switching technology, protocols, and network architecture."' [17] Consequently, each cell site "detects the radio signal from the handset, and connects it to the local telephone network, the Internet, or another wireless network." [18] Typically, cell sites are physically located atop towers, but the equipment can also be placed on trees, roofs, flagpoles, and buildings. [19]

Within this framework of cell tower networks, the origination of a cellular telephone call initiates a series of relays along the cell site network:

> When a caller dials a number on a cellular telephone, a transceiver sends signals over the air on a radio frequency to a cell site. From there the signal travels over phone lines or a microwave to a computerized mobile telephone switching office ("MTSO") or station. The MTSO automatically and inaudibly switches the conversation from one base station and one frequency to another as the portable telephone . . . moves from cell to cell. [20]

Whenever any cellular phone is turned on, it sends out a signal seeking the closest cell site, which in turn will register that telephone with that cell site. [21] "This process, called 'registration,' occurs approximately every ***189** seven seconds," [22] enabling "cellular providers to obtain a plethora of information about the telephones contacting their cell-sites." [23]

The Department of Justice ("DOJ") has explained that "to provide service to cellular telephones, providers have the technical capability to collect information such as the cell tower nearest to a particular cell phone, the portion of that tower facing the

phone, and often the signal strength of the phone." [24] For example, in 1997, the Federal Communications Commission ("FCC") issued rules "requir[ing] cellular service providers to upgrade their systems to identify more precisely the longitude and latitude of mobile units making emergency 911 calls." [25] Telecommunications providers "generally keep detailed historical records of this information for billing and other business purposes." [26]

This network of cell towers was designed to further communication among a subscriber's cell phone with other cell phones or landline telephones. It is necessary for efficient operation of the network. It is unlikely to change in any significant manner because the complete overhaul of the technology would be expensive. It is this system of cell tower networks that government officials seek to utilize when employing cell site simulators.

***190** Most cellular telephones around the world operate through the Global System for Mobile Communications ("GSM"). [27] Within this system, a cell phone initiating a call connects through its unique International Module Equipment Identity ("IMEI") [28] to a base station, which is essentially the hardware of a cell tower. [29] A base station potentially can operate with signal strength as low as fifty watts. [30] Of course, the number of base stations in an area hinges on the volume of demand for cellular service in that area:

> The size of the cell depends basically on the geographic features of the area and consequently on the range of the stations. But also the number of possible calls, that have to be handled simultaneously, has to be considered, since it is limited by the number of available channels. Hence, in densely populated areas, the cells often have a diameter of only a few hundred meters, whereas in sparsely populated areas several kilometers are usual. [31]

A base station is "not only responsible for the connectivity [of the cell phone call, but is] also needed for encryption and decryption of communication data." [32] From the base station, a cell phone call is routed to a base station controller, which in turn will move the call to another base station to prevent the call from being terminated. [33] If this handoff has to be done beyond a base station controller's range, then the transfer is handled by a mobile switching center. [34] This transfer represents the final stage of the call as the mobile switching center "is responsible for the authentication, routing, handoffs over different Base Station Controllers, connection to the landline, etc." [35]

*191 II. CELL SITE SIMULATORS CAPITALIZE ON EXISTING CELLULAR TECHNOLOGY TO RETRIEVE A CELL PHONE USER'S INFORMATION

Understanding how cell phone technology works, it is next important to appreciate how cell site simulators exploit cell phone technology in order to gather electronic information.

A. BASIC OPERATIONS OF CELL SITE SIMULATORS

Cell site simulators are being used more and more by intelligence agencies around the world, not just in the United States. [36] Although the Harris Corporation is one of the major producers of these devices, these days, a reasonably bright computer whiz with $1,500 can buy the raw components to make one. [37] The names TriggerFish and StingRay are trade names manufactured by the Harris Corporation, which sells those devices to American law enforcement and intelligence agencies. [38] Essentially, a TriggerFish is an older piece of technology that is a digital analyzer for passive interception of analog cell phone service. [39]

In other words, while it can intercept a cell phone call's verbal content, a digital analyzer (because it is a passive surveillance technique) can intercept only cell phones that are actually transmitting.

On the other hand, a StingRay is an IMSI catcher that captures digital cell phone information through an active interception process.[40] In 1996, Rohde & Schwarz, a German electronics company specializing in wireless communications, first invented an IMSI catcher that was able "to identify a subscriber by forcing it to transmit the IMSI."[41] One year later, the next model created by Rohde & Schwarz enabled the user "not ***192** only to identify, but also to tap outgoing calls."[42] Thus, as early as 1997, an IMSI catcher could be used to capture audio content.

Within the GSM, there is a vulnerability in the authentication process that enables cell site simulators, like an IMSI catcher, to breach the system.[43] Specifically, "it is not necessary to authenticate a Base Station to a Mobile Station."[44] In other words, the cell site simulator tricks the nearby cell phone into transmitting information to it as it would the nearest cell tower. "An IMSI catcher exploits this weakness and masquerades to a Mobile Station as a Base Station."[45] Through this masquerade, the cell site simulator "causes every mobile phone of the simulated network operator within a defined radius to log in" or register with it as it would a cell tower.[46]

Cell phones are designed to optimize reception by seeking the strongest signal among nearby base stations.[47] A base station can operate effectively with signal strength as low as twenty-five watts.[48] Thus, for a cell site simulator to be effective, it need only be marginally stronger than the signal of the nearest cell towers.

B. THE MANNER IN WHICH LAW ENFORCEMENT OFFICIALS USE CELL SITE SIMULATORS

Law enforcement officials will often use a cell site simulator inside a vehicle in conjunction with a computer that has mapping software.[49] Normally when a cellular phone is turned on, it seeks a connection to its telecommunications network system by using the nearest cell tower within its network.[50] This registration process enables the cell phone to communicate with its network, transmitting information and data, including audio content. Capitalizing on this registration, after the cell ***193** site simulator mimics a cell tower, nearby cellular phones will connect to it. This connection enables the device to download telephone numbers and other information related to the cellular phones, such as signal strength, because it typically emits the strongest signal in the nearby area.[51] For example, this technology would enable the user of a cell site simulator to detect the electronic serial number of the phone, the number for the cellular telephone, as well as any telephone numbers called from the cell phone.[52] The surveillance vehicle can then move to several different locations, collecting the phone's signal strength, thus enabling the officers to triangulate and map the phone's location.[53]

In addition to downloading information from all the cellular phones located within the area, a cell site simulator can be used to locate a specific cellular phone when the number is already known, but the location is unknown.[54] Law enforcement officials "can drive around until they get a signal from the target phone while pinging it."[55] After the target phone is located, the signal strength is measured in order to triangulate and map the location again.[56] In a hearing addressing electronic surveillance issues, an FBI agent "testified that he was able to determine the approximate distance from the originating cell tower where the cell phone and Stingray switched from the originating cell tower to another cell tower."[57] He further explained "that this method allows him to determine, with a reasonable degree of certainty, a fairly narrow geographical location where an individual is located while a cell call is being placed."[58]

Similarly, in a warrantless search by the Tallahassee Police Department, officers used a handheld device, as well as one mounted on ***194** a police vehicle.[59] Testimony from an unsealed hearing transcript revealed how the cell site simulators were employed:

Police drove through the area using the vehicle-based device until they found the apartment complex in which the target phone was located, and then they walked around with the handheld device and stood 'at every door and every window in that complex' until they figured out which apartment the phone was located in. In other words, police were lurking outside people's windows and sending powerful electronic signals into their private homes in order to collect information from within.[60]

Consistent with the testimony in *United States v. Allums*, it is apparent that some law enforcement officials are personally using this technology, as opposed to relying on any third-party telecommunications providers.

Any signals sent by law enforcement officials using a cell site simulator are signals that would not otherwise have been sent during the normal operations of a telecommunication provider's operation of its cell towers.[61] Moreover, the use of this device causes a brief disruption in the telecommunication provider's service to the cell phone.[62]

Some law enforcement officials are utilizing cell site simulators without court authorization.[63] Moreover, the federal officials who do seek a court order routinely file such applications pursuant to the pen register statute.[64] This approach is highly advantageous for the government, as the standard for a pen register application is much lower than the standard for a warrant because it does not require probable cause.[65]

III. THE DEVELOPMENT OF THE PEN REGISTER STATUTE

In order to analyze the inapplicability of the pen register statute to cell site simulators, one must know the function of a pen register. When the government seeks to ascertain the telephone numbers of incoming and outgoing calls, it files an application seeking a court order ***195** authorizing a pen register and a trap and trace device, respectively.[66] Historically, the Supreme Court defined a pen register as a device recording the outgoing numbers dialed from a specific telephone.[67] In *United States v. New York Telephone Company*,[68] the Court similarly defined a pen register: "A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed."[69] In other words, the Court reiterated the position from *United States v. Giordano*, that a pen register concerns the telephone numbers of outgoing calls from a specific telephone.

In *New York Telephone*, the Supreme Court held that Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Wiretap Act") did not apply to pen registers.[70] Instead, the Court held that the statute concerned only "orders 'authorizing or approving the *interception* of a wire or oral communication.'"[71] Because pen registers do not intercept any communications, the Wiretap Act did not authorize pen registers. Nonetheless, the Court concluded that district courts have the authority to authorize the installation of a pen register.[72] The basis for this authority was Rule 41 of the Federal Rules of Criminal Procedure, which requires a showing of probable cause.[73] Specifically, the Court reasoned "that Rule 41 is sufficiently broad to include seizures of intangible items such as dial impulses recorded by pen registers."[74]

In 1986, Congress enacted the ECPA, which amended the Wiretap Act to explicitly address pen registers. [75] The ECPA defined a pen ***196** register as a "device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted . . . on the telephone line to which such device is attached." [76] This definition essentially follows the definition enunciated in *New York Telephone*.

In the Communications Assistance for Law Enforcement Act of 1994, Congress mandated that both telecommunications and Internet service providers permit authorized law enforcement officers access to their networks in order for them to engage in electronic surveillance. [77] Regarding pen registers, however, the statute required that use of such technology "shall not include any information that may disclose the physical location of the subscriber." [78] Through this revision, Congress sought to capture transmitted e-mail data as well as the outgoing number dialed on cell phones, but not the location of the cell phone itself. In testifying before Congress in support of the statute, then-FBI Director Louis Freeh attempted to assuage legislators' concerns the statute would be used to authorize the tracking of individuals. [79]

In 2001, Congress amended the definition of the term "pen register" in the USA Patriot Act. [80] The Patriot Act defines a "pen register" as "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any ***197** communication." [81] An order authorizing a pen register pursuant to the Patriot Act must specify:
(A) the identity, *if known*, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied;

(B) the identity, *if known*, of the person who is the subject of the criminal investigation;

(C) the attributes of the communications to which the order applies, including the number or other identifier and, *if known*, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied. [82]

Analysis of §3123(b)(1) reveals that, in each subsection, Congress inserted the language "if known" to specify that the order need only contain the aforementioned information if known at the time authorization is requested. For example, in subsection (A), the order need not contain the name of the person to whom the cell phone is leased unless that person's name is known. Similarly, in subsection (B), the court order does not have to provide the name of the target of the investigation unless that person's name is known. However, in subsection (C), Congress did not modify the language "the attributes of the communications to which the order applies, including the number or other identifier" to add "if known." Indeed, the word "and" in that subsection makes clear that "the location of the telephone line or other facility" must be included in the order only "if known." Consequently, the rest of "the attributes of communications," including "the number or other identifier," must be specified within any order authorizing any pen register application.

Moreover, the inclusion of the word "facility" within the text of § 3123(b)(1), in addition to "telephone line," as covered by the pen register statute, does not permit law enforcement to obtain subscriber information without providing the cell phone number. The DOJ acknowledged that "facility" would include "a cellular telephone number" or "a specific cellular telephone identified by its electronic ***198** serial number." [83] Pursuant to § 3123(b)(1), pen register applicants can make requests when they know the cell phone number or the electronic serial number. [84] Indeed, the DOJ's *Field Guidance on New Authorities that Relate to Computer Crime and Electronic Evidence*s suggests that a pen register is not appropriate when the targeted cell phone

number or electronic serial number is unknown. Much of the significance of the amending language is attributable to the fact that Congress sought to ensure that the use of pen registers extended to new technologies, such as cell phones and computers.[85]

Accordingly, this revision in the USA Patriot Act broadened the definition of a pen register. Some judges have interpreted the Patriot Act to expand the definition to include electronic communications in addition to dialing information, but not to the capture of cell site information.[86] Others have rejected this approach, concluding that the Patriot Act applies to all communications to and from the targeted cell phone.[87] Regardless of the debate over the scope of a pen register following the Patriot Act, courts have routinely determined that law enforcement submit an application to use a pen register when seeking information about a particular telephone.[88] Indeed, the purpose of a pen register is to track telephone numbers, not people.

***199** In *New York Telephone*, the Supreme Court's conclusion that the Wiretap Act did not apply to pen registers did not also mean that the government could obtain pen registers without any judicial intervention.[89] To the contrary, the Court determined that the government could only obtain a pen register by establishing probable cause, consistent with the seizure standard enunciated in Rule 41 of the Federal Rules of Criminal Procedure, which is based on the Fourth Amendment.[90] Even if cell site simulators are not covered by the current iteration of the pen register statute, that does not grant the government carte blanche to use these devices without any judicial authorization. Instead, the appropriate approach is for the government to seek authorization for the use of a cell site simulator consistent with the requirements of Rule 41 and the Fourth Amendment.

Congress has limited judicial review of pen register applications to the "ministerial" task of confirming that the government has properly identified the attorney and agency seeking the order as well as providing a certification that the information sought through the device is relevant to an ongoing investigation.[91] When reviewing these applications, courts inquire neither into the veracity of the facts asserted by the government, nor into the reasonableness of its judgment concerning likelihood or relevance.[92] One scholar notes that "the ECPA's vague definition of a pen register, in combination with innovations in communications technologies and judicial permissiveness, allows law enforcement to acquire much communication attribute information by satisfying, at most, the minimal pen register procedures."[93] Consequently, the government is typically able to provide the proper identifications and certification to satisfy this low bar.[94] That low standard may be ***200** appropriate in applications in which law enforcement officials are truly seeking a traditional pen register to ascertain the numbers called from a specific cell phone. However, as the few known examples of requests for authorization to employ a cell site simulator demonstrate, the use of the pen register statute to support seeking materials with a cell site simulator is more troubling.

IV. FEW AVAILABLE EXAMPLES OF EITHER MOTIONS OR COURT ORDERS ADDRESS CELL SITE SIMULATORS & SIMILAR DEVICES

Very few judicial decisions address the use of these tools of electronic surveillance. One possible reason for the lack of decisions is that the government has attempted to keep its use of cell site simulator technology a secret.[95] For example, law enforcement officials often file their applications as requests for pen registers without much, if any, reference to the fact that the device to be used is a different type of electronic surveillance than the traditional pen register.[96] Moreover, when courts ask the government to provide legal authority for such electronic surveillance, pursuant to the pen register statute, the government is less than candid.[97] Finally, various government agencies, both federal and state alike, have taken measures to keep their use of cell site simulators secret. The FBI has gone so far as to require its employees to sign nondisclosure agreements to prevent them from disclosing any information about the government's use of cell site simulators.[98] There ***201** are also allegations that the Sarasota Police Department distorted its response to the court regarding its use of a StingRay.[99]

Indeed, in one case that I heard as a federal magistrate judge, the Assistant United States Attorney ("AUSA") who appeared before me repeatedly indicated that a legal memorandum would be forthcoming, but instead filed a motion to withdraw after a month. In another case the federal prosecutor indicated that he would provide legal authority the next day, but ultimately did not provide any such support. [100] The magistrate judge hearing the case informed the AUSA that there were some problems with the application. [101] Despite providing feedback and guidance, the magistrate judge never heard from the applicant. [102]

Existing decisions reveal that the government filed such applications pursuant to the pen register statute. With the exception of one published decision, they all address the standard after the amendments in the USA Patriot Act. Additionally, few, if any, form motions and orders created by law enforcement officials exist.

A. COURT ORDERS ADDRESSING APPLICATIONS FOR DIGITAL ANALYZERS AND CELL SITE SIMULATORS

1. The Central District of California

One of the first known decisions discussing law enforcement's use of this technology involves an application by the government for authorization to use a digital analyzer. [103] This is the only published decision addressing such electronic surveillance devices prior to the USA Patriot Act.

In this application, the government could not identify the cell phones of any of the five subjects of its narcotics investigation, but instead sought to analyze the signals from these subjects' cell phones. [104] Specifically, the applicant indicated that the investigators would "conduct surveillance of the subjects of the investigation, and when they ***202** observe[d] a subject using a cellular telephone, they [would] turn on the digital analyzer." [105] At that time they would obtain the information related to the specific cellular telephone that the subject was using.

Although the application sought a court order for the digital analyzer pursuant to 18 U.S.C. §3123, the government maintained that a court order was not necessary. [106] The trial court agreed, reasoning that the Fourth Amendment did not afford the subjects of a criminal investigation a reasonable expectation of privacy regarding their telephone numbers. [107] The court further explained that the pen register statute did not apply to the government's application because the statute contemplated investigation of a specific phone, whereas in this instance, law enforcement was targeting the individuals using the phones. [108]

Although the pen register statute did not apply per se, the court found that the spirit of the statute covered the intended activity. Applying the requirements of the statute, the court found the proposed order deficient. First, because the telephone numbers of the subjects of the investigation were unknown, it would be impossible to comply with the statute. [109] The court concluded that in passing the pen register statute, Congress had two principal concerns: "(1) the abusive interception of communications and (2) the accountability of law enforcement officers using advanced technology that might threaten privacy rights." [110] The trial court specifically expressed concern about the digital analyzer intercepting the "telephone numbers and calls made by others than the subjects of the investigation." [111] Additionally, because the proposed court order did not list the specific telephone numbers to be targeted by the digital analyzer, the order should have included "a requirement that the investigative agency maintain a time log identifying each target cellular telephone analyzed (by ESN and telephone number), together with all intercepted telephone numbers dialed or pulsed from each such ***203** telephone." [112] Because the application did not include the numbers or this requirement, the court denied the application without prejudice. [113]

2. The Southern District of Texas

a. The Use of a Cell Site Simulator in a Prison Setting

Since the enactment of the USA Patriot Act in 2001, there have been a few examples of applications for cell site simulators in federal court. In April of 2011, for example, the government filed an application for a pen register in the Southern District of Texas. [114] Specifically, the AUSA indicated that the government suspected that federal prison inmates were using cellular phones to perpetrate various federal offenses. [115] The government knew the names of the suspects, their location, and the location where they typically used their cell phones; [116] however, it did not know the phone numbers or in whose names the phones were purchased or leased. [117] To advance its investigation, federal law enforcement agents sought an order authorizing the installation of a pen register and a trap and trace device. [118] In the application, the government requested authority to use a device that could ascertain the number of any cell phones operating within a particular area, including the prison facilities. [119] According to the AUSA's statements during *ex parte* discussions, the device functioned by impersonating a cell tower, thereby receiving all of the signals sent from any nearby cellular phones. [120]

The government acknowledged that the device would capture the phone numbers of other phones that happened to be in the vicinity, but was confident in its ability to quickly winnow those numbers out and target the phones being used by the suspects. [121] The AUSA did not indicate how this winnowing process would be done. When asked about legal authority supporting the government's application, the Court was advised that a brief with legal support would be filed.

Instead of filing this legal brief, about a month after the application was filed, the government filed a motion to withdraw the application ***204** because prison officials had discovered and confiscated the cellular telephones that the government was trying to locate. [122] Because the application was moot, the motion to withdraw was granted. [123]

b. The Use of a Cell Site Simulator to Target a Drug Dealer

In another application before the Southern District of Texas, the government sought a pen register and a trap and trace regarding a Drug Enforcement Administration ("DEA") investigation. [124] The underlying investigation focused on an individual who was allegedly engaged in narcotics trafficking, based on an investigation of a number of years. [125] In its application, the government acknowledged that it did not know the telephone number of the cell phone used by the subject of the investigation. [126] During an *ex parte* hearing, the federal agent in charge of the investigation acknowledged that the application sought to use a StingRay device "to detect radio signals emitted from wireless cellular telephones in the vicinity of the [Subject] that identify the telephones." [127] Specifically, he explained that if the application were granted, the device would be employed from a vehicle that would be driven near the home of the subject of the investigation; that same vehicle would also follow the subject when he went other places during the period of surveillance. [128] In this manner, the agents hoped that a common cell phone number would materialize from the numbers obtained at the various surveillance-gathering locations.

The AUSA indicated "that the application was based on a standard application model and proposed order approved by the United States Department of Justice" for use by federal prosecutors. [129] During the hearing, the AUSA was unfamiliar with some case law raised during the discussion, but represented to the court that he would file a legal ***205** memorandum in support of his application the next day. [130] However, that legal support was never provided to the court. [131]

In its analysis of the application, the court first discussed the historical view of pen registers. [132] Next, it discussed the revised definition of a pen register based on the USA Patriot Act. [133] Notwithstanding the broader definition of a pen register in the Patriot Act, the court found that the statute and case law required that the pen register applicant be targeting a known telephone number. [134] According to the judge, "the plain language of the statute mandates that this Court have a telephone number or some similar identifier before issuing an order authorizing a pen register." [135] In other words, given the absence of a known cell phone number target, neither case law nor statutory language supported the applicability of the pen register statute to an application for a cell site simulator.

3. The Northern District of Texas

In an application filed in the Northern District of Texas in 2012, the government sought an order authorizing a pen register regarding the cellular phones used by the subject of an ongoing narcotics trafficking investigation. The alleged violations were possession with intent to distribute cocaine, marijuana, and methamphetamine in violation of 21 U.S.C. §841 and for conspiracy to possess with intent to distribute cocaine, marijuana, and methamphetamine in violation of 21 U.S.C. §846. [136] The ASUA represented that the subject of the investigation was using one or more unidentified cellular phones. [137] The government knew that this subject lived at one specific location and frequented another where he worked. [138] However, the government did not know the cell phone subscriber information of the persons leasing the cell phones that the subject was using. [139]

***206** In its application, the government explained that it sought to use the pen register to simply identify the subject's telephone number, as opposed to tracking the cell phone or attempting to determine its location. [140] Consequently, the use of surveillance equipment was to be limited: "Once the identifying registration data and the number of the *Subject Telephone* is identified, utilization of the pen register . . . shall cease." [141]

The court granted the government's application; however, the judge did impose some limits on the government's use of these devices. [142] The judge mandated that the order applied only to the cell phone used by the subject, and that the cell site simulator was to be used only in the subject's vicinity to ascertain his cell phone number. [143] Additionally, the judge specifically barred the use of the cell site simulator "when the *Subject* [was] in a location in which he would have a reasonable expectation of privacy; including but not limited to: a private residence, a vehicle, or a private office." [144] Once the subject's cell phone number was determined, the government was ordered to cease using the cell site simulator. [145] The government was apparently displeased with the court's conditions and ultimately did not use a cell site simulator. [146] Indeed, the AUSA informed the magistrate judge that the restrictions were too onerous. [147]

4. The District of Maryland

In an application filed in the District of Maryland in 2012, the government sought an order relating to the cellular phones used by the subject of an ongoing narcotics trafficking investigation for alleged violations of conspiracy to distribute controlled substances. [148] Specifically, the government sought to use a device to obtain "certain unknown mobile telephone(s) presently with unknown call number(s); unknown subscriber(s); and unknown service provider(s)" used by the subject of the ongoing investigation. [149] The AUSA elaborated that "[t]he ***207** purpose of this requested order is to identify this unknown information by deploying the device to the Target Telephone(s)." [150]

The AUSA indicated that the cell site simulator would "detect radio signals emitted from wireless cellular telephones in the vicinity of the target, including the Target Telephone(s)." [151] The AUSA further explained that "[b]y determining the identifying registration data at various locations in which the subject telephone is reasonably believed to be operating, the telephone number(s) and/or subscriber identities corresponding to the Target Telephone(s) can be identified." [152] The government acknowledged that, by using the device, it would invariably capture the telephone numbers of innocent third parties. [153]

The application requested the court to order that, when the federal agents obtained information from the search, they were "to log the identity of each cellphone analyzed, together with the intercepted subscriber identities for each device." [154] Moreover, it sought an order requiring that the government "avoid the collection of data from individuals other than that of the target." [155]

Interestingly, the government asserted that the 1995 Central District of California opinion provided support for its application. [156] Although the application acknowledged that the 1995 decision was not favorable to the government, the decision provided guidance as to what any subsequent applications should contain. [157] Finally, the AUSA maintained that the application and the attached proposed order pending before the Maryland district court adhered to the dictates from the 1995 decision. [158]

5. The District of New Jersey

In an application filed in the District of New Jersey in 2012, the government sought an order authorizing a pen register and trap and trace device as well as subscriber information, pursuant to 18 U.S.C. §2703. [159] The government knew the targeted cell phone number and that it was issued by Simple Mobile through its relationship with T-Mobile. [160] ***208** Because the location of the targeted cell phone was unknown, the application also sought authorization for "the FBI to deploy mobile pen register and trap and trace equipment to determine the general location of the cellular telephone facility assigned [to the specific] telephone number." [161] The court authorized the use of this "mobile pen register equipment" "in order to determine the general location" of the cell phone. [162] However, the court limited the FBI from "us[ing] the mobile equipment, absent other authority, to locate the Target Facility once it leads them to believe that they have identified a single residence or private space within which the Target Facility may be located." [163]

6. The District of Arizona

In a criminal prosecution in the District of Arizona, the government sought the defendant, a fugitive indicted on 74 counts of mail and wire fraud, aggravated identity theft, and conspiracy. [164] "The government located and arrested Defendant, in part, by tracking the location of an aircard connected to a laptop computer that allegedly was used to perpetuate the fraudulent scheme." [165]

After the defendant's arrest, he filed a motion for disclosure of evidence, as well as additional discovery. Specifically, he sought extremely detailed information regarding the aircard, as well as the identities and training of the FBI agents capable of using this technology. [166] In support of the defendant's motion, the American Civil Liberties Union ("ACLU") filed an *amicus* brief arguing that because the AUSA seeking the original order authorizing the use of the StingRay failed "to apprise the magistrate that it intended to use a stingray, what the device is, and how it works, it prevented the judge from exercising his constitutional function of ensuring that warrants are not overly intrusive and all aspects of the search are supported by probable cause." [167]

The government stipulated to a number of facts related to the motion for discovery, as well as the motion to suppress. It agreed that "[t]he mobile tracking device used by the FBI to locate the aircard function[ed] as a cell-site simulator. The mobile tracking device ***209** mimicked a Verizon Wireless cell tower and sent signals to, and received signals from, the aircard." [168] Additionally, the government acknowledged that "[t]he FBI used the mobile tracking device in multiple locations," taking readings and then moving to another location to take more readings. [169]

In locating the defendant with the use of the cell site simulator device, the government indicated that "[t]he FBI never used more than a single piece of equipment at any given time." [170] Moreover, the agents using the device were on foot near the defendant's apartment. [171] During that surveillance, these agents made telephone calls to the aircard. [172] The government indicated that "[t]he mobile tracking device used to simulate a Verizon cell tower [was] physically separate from the pen register trap and trace device used to collect information from Verizon." [173] Finally, for purposes of the defendant's pending motion, the government stipulated that "[t] he tracking operation was a Fourth Amendment search and seizure." [174]

In July 2008, the government obtained a warrant pursuant to Rule41 of the Federal Rules of Criminal Procedure from a magistrate judge in the Northern District of California authorizing the use of the StingRay device to locate the aircard. [175] In finding probable cause, the magistrate judge identified the aircard by both its specific assigned telephone number as well as its ESN. [176] In the motion to suppress, the defendant argued that the government's use of the device to track the aircard violated his Fourth Amendment rights. [177] Specifically, he argued "that the warrant is not supported by probable cause, that it lacks particularity, that the government's searches and seizures exceeded the warrant's scope, and that agents executed the warrant unreasonably because they failed to comply with inventory and return requirements." [178]

The district court judge found that the agent's affidavit in support of the warrant clearly linked locating the aircard with a high likelihood that it would lead to evidence of criminal activity. [179] Furthermore, the court noted that the agent's affidavit specifically indicated that the authorized device was used to locate the aircard. [180] Next, the court concluded that ***210** the warrant was sufficiently particular based on the use of the specific telephone number and the ESN identifying the aircard. [181] Regarding any argument for privacy by the defendant, the judge concluded that the defendant did not have a legitimate expectation of privacy in light of the fact that he obtained his residence and the computers through identity theft and other fraudulent means. [182]

Regarding the scope of the warrant, defendant argued that Verizon, rather than the FBI, was authorized to search for the aircard. [183] Again, the court rejected this argument, noting that while the warrant was "not a model of clarity," it satisfied the standard mandated by Rule 41. [184] Ultimately, the court denied the motion to suppress the evidence related to the aircard in part because the defendant did not have a legitimate expectation of privacy in his aircard. [185]

7. Other Magistrate Judges Have Acknowledged Handling Cell Site Simulator Applications

Of course, the above discussion is not exhaustive, as other magistrate judges may have received applications using the pen register application and not realized that they were authorizing or denying use of a cell site simulator. [186] One magistrate judge in the Western District of Washington explained that he received a request for a TriggerFish in 2011, which he denied. [187] Similarly, a magistrate judge in the Eastern District of Texas was faced with a pen register application for a cell site

simulator. [188] He indicated some concerns that he had with the request and sought some revisions, or in the alternative, some authority in support of the requested application. [189] Ultimately, the AUSA withdrew the application. [190]

Another magistrate judge indicated that he and his colleagues in the Southern District of California routinely grant requests for cell site simulators because people do not have any expectation of privacy in their telephone numbers. [191] He did note that an authorization covered ***211** only the recording of the ESN and MIN numbers transmitted to the telecommunication providers by cell phone. [192]

B. FORM APPLICATIONS AND ORDERS DRAFTED BY LAW ENFORCEMENT AGENCIES

In addition to these judicial examples addressing government applications to use cell site simulators, law enforcement officials have provided other examples in their training manuals.

1. The United States Attorneys' Bulletin

In a September 1997 *United States Attorneys' Bulletin*, the Electronic Surveillance Unit of the Officer of Enforcement Operations within the Criminal Division of the DOJ issued guidance regarding certain electronic surveillance techniques, including digital analyzers and cell site simulators. [193] This Bulletin explained that "[i]t is now possible for agents to capture electronically the unknown [ESN] or telephone number of a cellular telephone through the use of a device known as a *digital analyzer*." [194] It further explained that a digital analyzer "can be programmed to identify the telephone number assigned to the subject cellular telephone and telephone numbers dialed from this phone, as well as its ESN; i.e. a number assigned by the cellular telephone manufacturer and programmed into the telephone." [195] The Bulletin explicitly acknowledged that, because a digital analyzer is capable of intercepting communications as well as telephone numbers, the device "is programmed so it will not intercept cellular conversations or dialed numbers when it is used for the limited purpose of seizing ESNs and/or the cellular telephone's number." [196]

The Bulletin also discussed cell site simulators, explaining that they "can provide agents with a cellular telephone's ESN and mobile identification number ('MIN,' which contains the cellular telephone number and other information related to the operation of the phone)." [197] Next, it elaborated that cell site simulators:

[S]imulate[] some of the activities of a cellular service provider's cell site transmitter, albeit in a much smaller area, and allow[] agents to query cellular phones for their ESNs and MINs through "autonomous ***212** registration," an activity a cell site transmitter normally conducts to identify cellular phones operating within its cell or area. [198]

Finally, the Bulletin discussed that as with "a real cell site transmitter, the [cell site simulator] can determine ESNs and MINs of cellular phones that are 'powered up' or turned on. (The phone need *not* be in a 'use' mode; the information can be obtained unbeknownst to the cellular phone user.)" [199]

The Bulletin discussed that both digital analyzers and cell site simulators:

[C]an capture the cell site codes identifying the cell location and geographical sub-sector from which the cellular telephone is transmitting; the call's incoming or outgoing status; the telephone numbers dialed (pen register order required); and the date, time, and duration of the call. This cell site data is transmitted continuously from a cellular telephone (not by the user) as a necessary part of call direction and processing. [200]

Each telecommunications provider "uses this information to connect with the account in order to direct calls, and constantly reports to the customer's telephone a readout regarding the signal power, status, and mode of the telephone." [201]

2. The Department of Justice Electronic Surveillance Manual

In 2005, the DOJ published an *Electronic Surveillance Manual* to provide guidance to its attorneys throughout the country. Specifically, the *Electronic Surveillance Manual* "sets forth the procedures established by the Criminal Division of the Department of Justice to obtain authorization to conduct electronic surveillance." [202] The manual, last revised in 2005, discusses digital analyzers in a section concerning pen registers and trap and trace devices. [203] It explicitly cautions the need for a court order prior to using a cell site simulator:

> Because section 3127 of Title 18 defines pen registers and trap and trace devices in terms of recording, decoding or capturing dialing, routing, addressing, or signaling information, a pen register/trap and trace order must be obtained by the government before it can use its own device to capture the ESN or MIN of a cellular telephone, even though there will be no involvement by the service provider. [204]

***213** This determination by the DOJ, that a device used only to obtain a MIN requires a court order, indicates that a device used to ascertain the telephone number would also require a court order.

In the *Electronic Surveillance Manual*, the DOJ explained that "[l]aw enforcement possesses electronic devices that allow agents to determine the location of certain cellular phones by the electronic signals that they broadcast." [205] Specifically, a cell site simulator's "equipment includes an antenna, an electronic device that processes the signals transmitted on cell phone frequencies, and a laptop computer that analyzes the signals and allows the agent to configure the collection of information." [206]

The DOJ does not describe a device used to ascertain a phone number as a pen register. However, it demonstrates a belief that the same legal standards apply to such devices. The point is made explicit in the model form application and proposed order for a TriggerFish, a digital analyzer. [207] The caption for the application reads "In the Matter of the United States of America for an Order Authorizing the Installation and Use of a Pen Register." [208] Moreover, the caption on the proposed order reads similarly. [209]

3. The District of Arizona Form

In 2012, the Acting United States Attorney for the District of Arizona created a form application to guide attorneys in that office in requesting ESN identification numbers. [210] In the form application, the AUSA sought a court order "pursuant to 18 U.S.C. §§3122 and 3123, authorizing law enforcement to use an electronic serial number identifier to collect non-content wireless signaling information." [211] The caption on the application reads, "In the Matter of the Application of the United States of America for an Order Authorizing the Use of a Mobile Number Recorder to Collect Non-Content Signaling Information from Cellular Telephones." [212] Although the form anticipates that the requesting ***214** officials have the name of a subject of the investigation, it does not anticipate them having the cellular telephone numbers used by the subject or his drug trafficking organization, assuming the case pertains to drug trafficking. [213] The application explains that a "Mobile Number Recorder . . .

is an instrument that will decode and/or record non-content signaling information transmitted by a cellular telephone within a limited radius to determine the unique numeric identifiers of the telephone or telephones." [214] The form indicates that agents seek to use the Mobile Number Recorder in conjunction with traditional physical surveillance on the subject, such as by tracking the subject in an unmarked van, to obtain telephone numbers. [215]

In support of the application, the government must certify the relevance of the telephone numbers sought. [216] The form acknowledges that the mobile number recorder will gather telephone numbers unrelated to the subject, but asserts that these unrelated numbers will not be used by the investigating agents. [217] Additionally, it acknowledges that the device might also gather dialed digit information and posits that such information will be usable by the government pursuant to the pen register statute. [218] Next, the application contains blanks in which the government is to provide the specific criminal offenses that the subject allegedly committed, as well as specific facts in support of the application. [219] The government notes that it does not need to provide "specific and articulable facts" in support of its application because it will simply be using the pen register statute to obtain the subject's cell phone numbers with the mobile number recorder. [220]

The government also included, in this package to attorneys, a memorandum in support of its position. In the memorandum, the government argues that the mobile number recorder falls within the pen register statute as it is a recording of signaling information. [221] The memorandum also discusses the difference in the pen register definition in the ECPA with the amendment in the USA Patriot Act. [222] The government also argues that the Fourth Amendment does not apply to the use of a mobile number recorder. [223]

***215** The memorandum also provides an argument against the pen register statute's applicability to the mobile number recorder. [224] Specifically, it notes that any court order must "include[] the number or other identifier." [225] The government acknowledges that, since the 2001 amendment, "no court has held that a device like the one in this case falls within the statutory definition of a pen register." [226] Instead, it addresses the fact that at least one court viewing the 2001 amendments simply focused on applying the pen register statute to e-mails. [227] Consequently, that court determined that a "pen register must still be tied to an actual number or attempted phone call." [228]

The government also provided a proposed order to grant its application. [229] The proposed order follows the rationale provided by the application. [230]

4. The Los Angeles Police Department Form

At least one city has also developed form materials for use by its law enforcement officers. On September 29, 2012, Donal Brown, an editor at the First Amendment Coalition, filed a California Public Records Act Request with the Los Angeles Police Department ("LAPD") for information regarding the use of devices to track and identify a cellular phone's IMSI. [231] Among the various requests, Brown sought "[a] copy of any LAPD internal policies, guidelines or standards for police use of an IMSI device" or in lieu of such records "all other records sufficient to show the policies, guidelines or standards in effect for LAPD use of an IMSI device." [232] Next, he requested "[r]ecords sufficient to show whether judicial authorization is obtained for LAPD deployment and use of an IMSI device and the type of judicial authorization obtained." [233] He also asked for "[r]ecords sufficient to show, for the time period June 1 [to] Sept. 30, 2012, the frequency of LAPD's deployment and use of an IMSI device," as well as, for the same time period, "[r]ecords sufficient to show . . . all LAPD uses of an IMSI device in which LAPD

personnel ***216** eavesdropped on conversation." [234] Finally, he requested "[r]ecords sufficient to identify all prosecutions or other judicial proceedings initiated by the LAPD or LA District Attorney during 2011 in which information was filed in, or furnished to, the Superior Court (LA County) derived from LAPD's use of an IMSI device." [235] Brown asked that a response be provided within ten days. [236]

On December 14, 2012, Officer Martin Bland, the Officer-in-Charge of the Discovery Section within the Legal Affairs Division of the LAPD, responded to Brown's records request. [237] With respect to the first three requests, Bland indicated that he would make documents available after Brown paid the duplicating fee. [238] Bland then acknowledged that, "[d]uring the time period in your request, 21 cell phone numbers were subjected to the deployment of an IMSI," but "there were no uses of an IMSI device that involved the eavesdropping of conversations." [239] Finally, Bland declined to provide any information in response to the request regarding prosecutions involving an IMSI device because "there is no centralized repository for records (or information) responsive to [the] request," which made the request "significantly and unduly burdensome." [240]

On December 28, 2012, Bland provided Brown with thirty-one pages of records responsive to his request. [241] Notably, there was an October 16, 2012 memorandum to all Commanding Officers explaining that "[t]he law regarding the use of cellular and GPS tracking is evolving. Protocols governing cellphone tracking requests are necessary to ensure Department personnel are abiding by the most current case law." [242] Consequently, the memorandum mandated that "[a]ll requests for cellular tracking, made concurrent with an investigation (whether by use ***217** of a court order or under an exigent circumstances process), shall be directed through [the Real-Time Analysis and Critical Division]." [243]

In the December28, 2012 letter from Bland to Brown, Bland provided an explanation of the statutory basis and procedures for requesting applications and court orders that use a "cell phone tracking system for identifying" a cell phone's IMSI, as well as forms for applications and orders. [244] Notably, in response to Brown's request, Bland turned over an LAPD form application addressing requests for authorization of an IMSI device in the Superior Court for the County of Los Angeles. [245] The caption reads, "In the Matter of the Application of the People of the State of California for an Order Authorizing the Use of a Pen Register and a Trap-and-Trace Device on Telephone Line Currently Designated by Telephone Number," with a blank space to fill in the specific telephone number. [246] The application sought to distinguish between a telephone number and a telephone line because it maintained that the pen register statute was "defined with respect to telephone lines" as opposed to telephone numbers. [247] The application contained a section to be filled in by the police officer indicating the probable cause that supported the request. [248]

With this form application, the LAPD also provided a proposed order. [249] In support of its recommendation, the LAPD proposed citing 18 U.S.C. § 2703(d) [250] as the statutory authority for the order, notwithstanding the fact that the form application is characterized as a pen register request. [251]

*218 V. THE DEVELOPMENT OF FOURTH AMENDMENT JURISPRUDENCE

In order to understand the applicability of the Fourth Amendment to the government's applications seeking authorization of cell site simulators, one must understand the history of the Fourth Amendment. Fourth Amendment jurisprudence developed from a fairly narrow property-centric interpretation to a more flexible standard based on reasonable expectations. This more flexible standard should be reassessed in order to ensure that cell phone users have privacy from governmental intrusions into their cell phones.

A. HISTORICALLY, THE FOURTH AMENDMENT WAS PROPERTY-CENTRIC

To better understand the current state of Fourth Amendment jurisprudence, it is important to understand a little about where we started. In light of disputes with the British authorities, the founding fathers sought to ensure that people in the newly formed country would be secure from discretionary governmental intrusions in their lives. [252] The Fourth Amendment provides that it is "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." [253] It further mandates that "no Warrants shall issue, but upon probable cause." [254] Consequently, the threshold matter in Fourth Amendment jurisprudence "is whether a specific action or intrusion by the government constitutes a 'search' within the meaning of the Amendment." [255]

Historically, the Fourth Amendment was viewed to safeguard citizens against search of their homes, persons, and papers based on a right of property. Many scholars have posited that Fourth Amendment jurisprudence was based on a theory of trespass. [256] One scholar further explained that this trespass theory is rooted in the landmark pre-constitution decision of *Entick v. Carrington*. [257] However, Orin Kerr ***219** recently asserted that he and others had it wrong in viewing Fourth Amendment theory as having its historical foundation in trespass. [258]

In one of the first Supreme Court decisions to address the Fourth Amendment, the defendant challenged the use of his records, seized without a warrant, to convict him for failure to pay customs duties. [259] In *Boyd*, the Court addressed the question of "compulsory production of a man's private papers, to be used against him in a proceeding to forfeit his property for alleged fraud against the revenue laws . . . [and whether that constituted] an '*unreasonable* search and seizure' within the meaning of the Fourth Amendment." [260] In concluding that the trial court erred in requiring the production of the defendant's papers, the Court looked to early colonial history as well as English history, including the decision in *Entick*, finding that the entering and searching of the home constituted a trespass. [261]

In *Olmstead v. United States*, [262] the Supreme Court considered a challenge to information that federal agents obtained from wiretapping the telephones within the homes of targets of a criminal investigation. Chief Justice Howard Taft made clear that the wiretapping was "made without *trespass* upon any property of the defendants" because the line that was tapped was "made in the basement of the large office building." [263] Nonetheless, he stressed that "[t]he well-known historical purpose of the Fourth Amendment, directed against general warrants and writs of assistance, was to prevent the use of governmental force to search a man's house, his person, his papers, and his effects, and to prevent their seizure against his will." [264] In many regards, the applied approach was a plain language interpretation of the amendment. Indeed, Chief Justice Taft distinguished *Hester v. United States*, [265] in which he acknowledged that there was a trespass on defendant's property, but ***220** ultimately "no search of person, house, papers, or effects." [266] In dissent, however, Justice Louis Brandeis famously cautioned that the Fourth Amendment protected citizens against "invasion of 'the sanctities of a man's home and the privacies of life.'" [267]

In *Goldman v. United States*, [268] the Supreme Court considered federal agents' use of a detectaphone against a wall to listen and assist in the recording of defendants' conversation within one defendant's office on the other side of the wall. The Court specifically held "what was heard by the use of the detectaphone was not made illegal by trespass or unlawful entry." [269] Instead, the only trespass occurred when agents actually entered the defendant's office to install another device that ultimately did not function properly and provided no information. [270] As in *Olmstead*, the dissents argued for individual privacy interests. For example, Chief Justice Harlan Fiske Stone and Justice Felix Frankfurter wrote simply:

> Had a majority of the Court been willing to overrule the *Olmstead* case, we should have been happy to join them. But as they have declined to do so, and as we think this case is indistinguishable from *Olmstead*'s, we have no occasion to repeat here the dissenting views in that case with which we agree. [271]

Similarly, Justice Frank Murphy dissented, noting an individual's "right of personal privacy guaranteed by the Fourth Amendment." [272]

B. IN *KATZ*, THE SUPREME COURT ESTABLISHED THE REASONABLE EXPECTATION OF PRIVACY ANALYSIS

Regardless of whether one views the development of Fourth Amendment jurisprudence through the prism of property rights, a trespass theory, or a literalist construction, after *Katz v. United States*, [273] the paradigm shifted. In *Katz*, the Supreme Court held that a listening device that recorded the defendant's conversation while he talked in a public telephone booth violated the Fourth Amendment. Justice Stewart Potter explained that Katz, by entering the telephone booth and closing the door before engaging in his telephone call, evidenced an attempt and a belief that his conversation would be private. [274] Justice Potter then ***221** elaborated that "[t]o read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication." [275] Finally, he determined that "[t]he Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment." [276] Interestingly, the phrase "reasonable expectation of privacy," which has been the lasting impact of *Katz*, is not from Justice Stewart's majority opinion, but instead from a concurring opinion by Justice Harlan. [277]

This "reasonable expectation of privacy" standard was reiterated and adopted by a majority of the Supreme Court in *Terry v. Ohio*. [278] In elaborating on this standard, the Court explained, in *United States v. Jacobsen*, [279] that "[a] 'search' occurs when an expectation of privacy that society is prepared to consider reasonable is infringed." [280] In the post-*Katz* world we are left to ponder what reasonable expectation of privacy, if any, cell phone users have as it relates to the government's use of cell site simulators.

Orin Kerr has posited that while "the phrase 'reasonable expectation of privacy' is notoriously murky, much of the Supreme Court's case law on the reasonable expectation of privacy test can be understood as distinguishing between inside and outside surveillance." [281] In an earlier article he echoed this theme: "Although the phrase 'reasonable expectation of privacy' sounds mystical, in most (though not all) cases, an expectation of privacy becomes 'reasonable' only when it is backed by a right to exclude borrowed from real property law." [282] He distinguished between inside and outside by elaborating that governmental conduct breaches a reasonable expectation of privacy ***222** when the surveillance exposes private, enclosed spaces, such as homes, cars, or packages. [283] On the other hand, Patricia Bellia has maintained:

> The main constitutional question is whether one retains a reasonable expectation of privacy in communications stored with a third party, such that acquisition of these communications constitutes a 'search' within the meaning of the Fourth Amendment. I call into question the prevailing assumption that an expectation of privacy is lacking when a service provider holds communications on a user's behalf. [284]

In *Smith v. Maryland*, the Supreme Court considered whether there were any privacy rights in the information that a pen register captures from a landline telephone. [285] The Court held that the use of a pen register to obtain the telephone numbers dialed was not a Fourth Amendment search because the telephone user had "no actual expectation of privacy in the phone numbers he dialed." [286] However, the Court's decision is a very narrow one and addresses pen register technology from the 1960s. Most importantly, the pen register at issue simply recorded a list of telephone numbers that were dialed from a *landline* telephone. [287] Indeed, the decision was issued a decade before the cell phone became ubiquitous. The *Smith* Court did not address the vast amount of information that the government routinely seeks these days in pen register applications for cellular telephones, including the time, date, and duration of any cell phone call as well as the physical location from which the call was made. [288] In other words, the analysis of *Smith v. Maryland*, predicated on the information obtained on a landline telephone, does not apply to the information that is obtainable through a pen register for a cell phone today. [289] The typical consumer does not expect that all of this data is widely available to the government any time that it simply asks for it. [290] The uproar and outrage over the breaches by the National Security Agency ("NSA") further demonstrate that there is no reasonable expectation that this information is anything but private. [291]

***223** In *Georgia v. Randolph*, [292] the Supreme Court addressed a Fourth Amendment challenge in which the defendant sought to suppress cocaine obtained during a search of his home that resulted in this conviction for possession of cocaine. Specifically, when police officers responded to a call about a domestic dispute at the residence, the defendant's estranged wife indicated to them that her husband had narcotics in their home. [293] Although the defendant expressly refused to consent to the search of his home when officers asked, they then obtained consent from his wife. [294] In the majority opinion written by Justice David Souter, the Court held that the warrantless search was unreasonable in light of the defendant's express refusal to consent to the search. [295]

In a dissenting opinion joined by Justice Antonin Scalia, Chief Justice John Roberts took issue with the notion that defendant had a reasonable expectation of privacy in his home once he shared that home with another person, in this case his wife. [296] Chief Justice Roberts continued by explaining that there are a large number of situations that might lead to various and different social expectations. [297] Ultimately, he asserted that custom and "widely shared social expectation" were not a basis for evaluating a search pursuant to the Fourth Amendment. [298]

Chief Justice Roberts' visceral reaction to social expectation in *Georgia v. Randolph* is interesting when compared to his response to the Government's oral argument in *United States v. Jones*. In *Jones*, the Court dealt with whether the government could place a GPS tracking device on the vehicle of a subject of a criminal investigation without a warrant. During oral argument, Chief Justice Roberts had this exchange with the Deputy Solicitor General:

***224** CHIEF JUSTICE ROBERTS: You think there would also not be a search if you put a GPS device on all of our cars, monitored our movements for a month? You think you're entitled to do that under your theory?

MR. DREEBEN: The Justices of this Court?

CHIEF JUSTICE ROBERTS: Yes.

(Laughter.)

MR. DREEBEN: Under our theory and under this Court's cases, the Justices of this Court when driving on public roadways have no greater expectation of --

CHIEF JUSTICE ROBERTS: So, your answer is yes, you could tomorrow decide that you put a GPS device on every one of our cars, follow us for a month; no problem under the Constitution?

MR. DREEBEN: Well, equally, Mr. Chief Justice, if the FBI wanted to, it could put a team of surveillance agents around the clock on any individual and follow that individual's movements as they went around on the public streets. [299]

Put simply, Chief Justice Roberts appeared to address the reasonable expectations of privacy as it personally relates to him and the other members of the Court. Roberts was seemingly concerned about the real possibility that someone could legally engage in this type of surveillance of his vehicle without judicial authorization. [300] While the majority decision, which he joined, focused on a Fourth Amendment violation based on a trespass theory, he implied that the Supreme Court Justices (and others) had an expectation of some privacy. [301] The reason for this expectation could arguably be based on the personal nature of one's vehicle and daily travels. Still, he argued there was no expectation of privacy if law enforcement officials arrived at his residence and sought to search his home over his objections if his wife gave them express authority. [302] Possibly, he was more certain that he and his wife are of one mind regarding such a potential intrusion than the possibility that a tracking device could be placed on his vehicle.

In *Jones*, Justice Sonia Sotomayor discussed both *Smith* and *Miller* in arguing that the third-party doctrine needs to be reconsidered: "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." [303] She continued by asserting that the approach established ***225** in *Miller* and *Smith* "is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks" including revealing information based on their cell phone usage. [304] In criticizing Justice's Scalia's opinion in *Jones*, Justice Samuel Alito noted that the issue was not the physical trespass, but the lengthy and intrusive nature of the electronic surveillance. [305] He continued by positing that the old method of Fourth Amendment analysis may be inapplicable to the new issues raised by electronic surveillance. [306] Similarly, the Court in *Kyllo v. United States* [307] cautioned that "[w]hile the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development." [308]

Since the Supreme Court decided *Jones*, one federal appellate court has addressed the issue of whether the use of warrantless cell site location information violates the Fourth Amendment. The Eleventh Circuit concluded that "it cannot be denied that the Fourth Amendment protection against unreasonable searches and seizures shields the people from the warrantless interception of electronic data or sound waves carrying communications." [309] The court continued with an analysis of the three decisions in *Jones* and noted that the *Katz* privacy test is still applicable. [310] Ultimately, the Eleventh Circuit held "that cell site location information is within the subscriber's reasonable expectation of privacy" and that "obtaining of that data without a warrant is a Fourth Amendment violation." [311]

Most recently, in *Riley v. California*, the Supreme Court addressed whether evidence obtained by police from a defendant's cell phone during a warrantless search subsequent arrest violated the Fourth Amendment. [312] In the first of the consolidated cases, David Riley was stopped by police officers for a routine traffic stop and then subsequently arrested after his car was impounded and a search revealed firearms. [313] During his arrest, the officers seized his smart phone from his pants pocket and searched it, thereafter concluding that he was a member of a ***226** street gang. [314] The prosecution charged him with a number

of offenses, some of which carried sentencing enhancements based on his gang affiliation.[315] Riley challenged the denial of his motion to suppress this information.[316]

In the second case, Brima Wurie was arrested for selling drugs. While under arrest, police officers noticed that his flip phone was receiving several calls from a number labeled "my house."[317] After searching this cell phone's call log, the officers traced the number to his apartment.[318] The police then went to Wurie's residence and confirmed that it was in fact his home, in part because the woman pictured in his flip phone was found at the apartment.[319] A subsequent search of the apartment revealed drugs and firearms, resulting in multiple federal charges against him.[320] The district court denied his motion to suppress, but the Court of Appeals for the First Circuit reversed and vacated Wurie's three convictions.[321]

In analyzing these two cases, the Court first discussed the history of Fourth Amendment in the context of searches incident to arrest, and ultimately held "that officers must generally secure a warrant before conducting such a search" of a cell phone.[322] The Court continued its analysis by noting that "[d]igital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape. Once an officer has secured a phone and eliminated any potential physical threats, however, data on the phone can endanger no one."[323]

The Court focused next on privacy concerns raised by cell phones, explaining that these devices were essentially small computers that stored immense amounts of data and information.[324] The opinion focused on several reasons that cell phones implicate significant privacy concerns:

> First, a cell phone collects in one place many types of information--an address, a note, a prescription, a bank statement, a video--that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a ***227** photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all of his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.[325]

Finally, the Court emphasized the pervasiveness of cell phones and the fact that people carry them, with all their sensitive information, with them all of the time.[326] Thus, all nine justices held that police must get a search warrant prior to searching a seized cell phone.[327]

C. PEOPLE HAVE A REASONABLE EXPECTATION OF PRIVACY IN THEIR CELL PHONES, INCLUDING THE NUMBERS THEY DIAL

While *Katz* established the principle of an individual's reasonable expectation of privacy, *Smith v. Maryland* and *United States v. Miller*[328] are the Supreme Court decisions that are relied upon for the third-party doctrine, which in some ways undercuts *Katz*. In *Miller*, federal agents served grand jury subpoenas issued by the United States Attorney on the defendant's banks seeking records to support a criminal investigation.[329] In a motion to suppress, the defendant challenged the subpoenas because they were not issued by a court.[330] Because the defendant had provided his information to the bank in the regular course of his various banking transactions, the Supreme Court determined that he no longer had a reasonable expectation of privacy.[331]

Consequently, the Court held "that there was no intrusion into any area in which respondent had a protected Fourth Amendment interest and that the District Court therefore correctly denied respondent's motion to suppress." [332] Of course, in this day and age of online banking, people may have a different expectation of privacy than they used to.

Generally, there is not much in the way of empirical research regarding people's reasonable expectations of privacy. [333] Moreover, there does not appear to be any research questioning people's reasonable expectations of privacy regarding the telephone numbers that they dial with their cell phones. The limited data reflects that individuals, when ***228** surveyed, "overwhelmingly expressed agreement with precedent limiting invasions of communications privacy." [334] In one survey, 63.1% of participants agreed with the decision in *Katz* requiring a warrant to record a phone conversation. [335] That rate went up to 91.7% if the phone in question was the participant's cell phone. [336]

Some scholars have asserted that the Supreme Court's determinations of what constitutes "reasonable expectations of privacy" "are often not in tune with commonly held values." [337] The limited existing quantitative research supports this claim. For example, 85.5% of respondents in one survey disagreed with *United States v. Knott*, [338] in which the Supreme Court upheld the warrantless installation of a tracking device on a vehicle. [339] Similarly, in a poll of Californians, 73 percent "favor a law that required the police to convince a judge that a crime has been committed before obtaining location information from the cell phone company." [340] Moreover, in a question based on *United States v. Miller*, 85.4% of those surveyed disagreed with the Court's ruling that there is no reasonable expectation of privacy in one's bank records. [341] These results demonstrate a significant disconnect between the Supreme Court's interpretation of what constitutes a reasonable expectation of privacy in various contexts and individual's actual expectations.

Specifically, several state courts have rejected the applicability of *Miller* pursuant to state constitutions. [342] Similarly, various state courts have rejected the reasoning and ruling in *Smith v. Maryland*. [343] In light of numerous state court decisions addressing pen registers, the ***229** government's use of a pen register to obtain authorization for cell site simulators is troubling from the perspective of a reasonable expectation of privacy standard. A number of state courts have concluded, based on state constitutions and statutes, that their citizens have such a privacy expectation and that probable cause and a warrant are necessary for a pen register. [344] Interestingly, these various state court decisions regarding privacy rights, pen registers, and one's reasonable expectations of privacy were all decided in the 1980s, before the cell phone became ubiquitous in American life. These expectations have not disappeared as pen registers have grown more sophisticated and most people rely exclusively on their cell phones to communicate with others. For example, in *State v. Branigh*, [345] the Court of Appeals of Idaho concluded that the defendant "had a reasonable expectation of privacy in the telephone log records that the State obtained from Sprint and that the State's acquisition of those logs was subject to the restraints of [the Idaho Constitution]." [346] Moreover, this protection extends to the records documenting the dates, times, and recipients of text messages. [347]

These state court decisions just start to scratch the surface of various jurisdictions' notions of reasonable expectations of privacy regarding these matters. It stands to reason that if various people around the country have a reasonable expectation of privacy in preventing law enforcement officials from obtaining their telephone call records based on standard pen register requests, then these same people would have similar privacy expectations in any pen register request for a cell site simulator.

***230** That so many state courts and legislatures conclude that there is a reasonable expectation of privacy regarding pen registers further supports the position that a cell site simulator would have a similar, if not stronger, expectation of privacy. Coupled with the fact that the pen register at issue in *Smith v. Maryland* was a significantly less technologically advanced version of the pen registers typically sought today, there is a good argument that the day for reassessment of the continued

viability of the decision is coming. One need look no further than the recent issues involving massive electronic searches of American citizens by the NSA to know that many people believe this day has arrived. Indeed, while a pen register in the *Smith v. Maryland* era obtained the only outgoing telephone numbers called, a pen register for a cell phone provides much more information today, including the telephone numbers dialed for text messages and phone calls; the date, time, duration of such phone calls and text messages; and the location of the cell phone. [348]

CONCLUSION

The purpose of this Article is not to reject the use of cell site simulators. Indeed, it is clear that these devices can be effective tools in law enforcement arsenals. For example, the use of a cell site simulator near a prison facility can assist in locating a cell phone used by inmates in furtherance of criminal activity.

Nonetheless, there are significant concerns for the privacy rights and interests of third parties. Regarding the applications for the use of cell site simulators, law enforcement officials should minimize the impact that cell site simulators have on such third parties, including by developing a protocol that explains attempts to minimize the invasion of privacy. [349]

It is clear that an application for a cell site simulator seeks authorization for a device unanticipated by Congress in the pen register statute. "If courts find that the new methods do not fit into the statutory definition, they may follow the lead of those courts who have regarded the new practices as completely unregulated." [350] For law enforcement officials to obtain judicial approval for the use of cell site simulators, they should have to seek authorization pursuant to a search warrant consistent with Rule 41 of the Federal Rules of Criminal Procedure. Alternatively, they can persuade Congress to amend the pen register statute to authorize cell site simulators.

Scholars have long called for Congress to amend the ECPA in order to update it to address the myriad of technological developments in ***231** surveillance since 1986. [351] As Susan Freiwald has asserted, "[t]he ECPA, because it permits a substantial amount of surveillance to proceed without the requirement of a warrant, let alone the heightened procedural safeguards that apply to wiretapping, should have been quite vulnerable to constitutional challenges." [352] Congressional reticence to amend may require that the courts handle the matter of safeguarding the public: "the Supreme Court has taken a hands-off approach to technological development, refusing to recognize Fourth Amendment privacy barriers to its use. However, the Court has sometimes been willing to intervene even at the risk of dramatically changing Fourth Amendment law." [353] Because the ECPA does not provide a suppression remedy, individuals cannot assert claims for violations of the statute themselves, and the courts become all the more important. [354] Such courts are those presided over by magistrate judges who handle the vast majority of these types of requests at their initial stages. Only if these judges safeguard the Constitution and bring a voice to the countless citizens across the country can the reasonable expectations of so many be protected.

Footnotes

a1 Brian L. Owsley, Assistant Professor of Law, Indiana Tech Law School; B.A., 1988, University of Notre Dame; J.D., 1993, Columbia University School of Law; M.I.A., 1994, Columbia University School of International and Public Affairs. From 2005 until 2013, the Author served as a United States Magistrate Judge for the U.S. District Court for the Southern District of Texas. I am very grateful for valuable comments and critiques provided by Steven Friedland, Jonah Horwitz, Stephen Wm. Smith, and Christopher Soghoian.

1 *See In re* Application of the U.S. for an Order Pursuant to 18 U.S.C. §2703(d), 964 F. Supp. 2d 674, 675 (S.D. Tex. 2013).

2 *See id.*

3 *See generally* Marc Rotenberg & David Brody, *Protecting Privacy: The Role of the Courts and Congress*, 39 HUM. RTS. 7 (2013); Jon Campbell, *LAPD Spied on 21 Using StingRay Anti-Terrorism Tool*, L.A. WEEKLY (Jan. 24, 2013), http://www.laweekly.com/2013-01-24/news/stingray-LAPD-spying-21-terrorism-tool-against-citizens; Ryan Gallagher, *FBI Files Unlock History Behind Clandestine Cellphone Tracking Tool*, SLATE (Feb. 15, 2013, 2:34 PM), www.slate.com/blogs/future_tense/2013/02/15/stingray_imsi_catcher_fbi_files_ unlock_history&uscore;behind_cellphone_tracking.html; John Kelly, *It's Not Just the NSA: An Increasing Number of Police Agencies Across the USA Are Snatching Your Cellphone Data, Whether You're a Suspect or Not*, USA TODAY, Dec. 9, 2013, at A1; Leslie Meredith, *Law Enforcement Tracks Phones With Phony Cell Towers*, TECH NEWS DAILY (July 12, 2012), https:// web.archive.org/web/20140531131028/http://www.technewsdaily.com/4537-embargoed-law-enforcement-tracks-real-phones-phony-cell-towers.html; Ellen Nakashima, *Little-Known Surveillance Tool Raises Questions Over Privacy*, WASH. POST, Mar. 28, 2013, at A3; Jennifer Valentino-Devries, *'Stingray' Phone Tracker Fuels Constitutional Clash*, WALL ST. J. (Sept. 22, 2011), http:// online.wsj.com/article/SB10001424053111904194604576583112723197574 *see also* DAEHYUN STROBEL, IMSI CATCHER 1 (2007), *available at* http:// www.emsec.rub.de/media/crypto/attachments/files/2011/04/imsi_catcher.pdf ("The IMSI Catcher is an expensive device to identify, track and tap a mobile phone user in such a way, that even the network operator cannot notice anything.").

4 HARRIS WIRELESS PRODS. GRP., HARRIS GCSD PRICE LIST, *available at* https://info.publicintelligence.net/Harris-SurveillancePriceList.pdf; Ryan Gallagher, *Meet the Machines That Steal Your Phone's Data*, ARS TECHNICA (Sept. 25, 2013, 10:00 AM), http://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/.

5 *See* Nakashima, *supra* note 3; Campbell, *supra* note 3; Valentino-Devries, *supra* note 3.

6 *See* STROBEL, *supra* note 3, at 13-15.

7 Kelly, *supra* note 3.

8 Campbell, *supra* note 3; *see* Cyrus Farivar, *Local Cops in 15 U.S. States Confirmed to Use Cell Tracking Devices*, ARS TECHNICA (June 12, 2014, 12:32 PM), http://arstechnica.com/tech-policy/2014/06/local-cops-in-15-us-states-confirmed-to-use-cell-tracking-devices.

9 In response to a request for information on electronic surveillance, Gilbert police officials informed the ACLU about their cell site simulator purchase: "The Gilbert Police Department obtained a $150,000 grant from the State Homeland Security Program. These funds, along with $94,195 of R.I.C.O. monies, were used to purchase cell phone tracking equipment in June 2008 (total acquisition cost of [$] 244,195)." Letter from Kate Weiby, Gilbert Police Legal Advisor, & Tim Dorn, Gilbert Chief of Police, to Dan Pochoda, ACLU (Sept. 6, 2011), *available at* http://www.aclu.org/files/assets/town_of_gilberts_response_to_prr_re_cell_phone_location_records.pdf; *accord* Bob Sullivan, *Pricey 'Stingray' Gadget Lets Cops Track Cellphones Without Telco Help*, NBC NEWS (Apr. 3, 2012, 2:47 AM), http://www.nbcnews.com/business/consumer/pricey-stingray-gadget-lets-cops-track-cellphones-without-telco-help-f635294. Based on the 2010 U.S. Census, Gilbert had an estimated population of 221,140 in 2012. *Gilbert Quick Facts*, U.S. CENSUS BUREAU, http:// quickfacts.census.gov/qfd/states/04/0427400.html (last visited Dec. 14, 2014).

10 Allie Bohm, *You're Getting Warmer ...*, ACLU BLOG OF RTS. (Sept. 26, 2011, 2:12 PM), http://www.aclu.org/blog/technology-and-liberty/youre-getting-warmer; *see* MMI Research Ltd. v. Cellxion Ltd., [2012] EWCA (Civ) 7 (Eng.).

11 Campbell, *supra* note 3; Joel Kurth & Lauren Abdel-Razzaq, *Oakland Deputies Use Cellphone Tracker*--Military Device Sweeps All Calls Made in Wide Area, DETROIT NEWS, Apr. 4, 2014, at A6.

12 Kurth & Abdel-Razzaq, *supra* note 11.

13 442 U.S. 735 (1979).

14 425 U.S. 435 (1976).

15 *See* Timothy B. Lee, *Documents Show Cops Making Up the Rules on Mobile Surveillance*, ARS TECHNICA (Apr. 3, 2012, 7:40 AM) http:// arstechnica.com/tech-policy/2012/04/documents-show-cops-making-up-the-rules-on-mobile-surveillance; *see also In re* Application of the U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 831 (S.D. Tex. 2010) ("[C]ellular telephones use radio waves to communicate between the user's handset and the telephone network."); *In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 750 (S.D. Tex. 2005) ("A cell phone is a sophisticated two-way radio with a low-power transmitter that operates in a network of cell sites."); Brian Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in its Electronic Surveillance*, 16 U. PA. J. CONST. L. 1, 3 (2013).

16 S. REP. NO. 99-541, at 9 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3563; *see* In re *Application for Pen Register & Trap/ Trace Device*, 396 F. Supp. 2d 750 ("'Cell' refers to geographic regions often illustrated as hexagons, resembling a bee's honeycomb; a 'cell site' is where the radio transceiver and base station controller are located (at the point three hexagons meet)."); Aaron Blank, *The Limitations and Admissibility of Using Historical Cellular Site Data to Track the Location of a Cellular Phone*, 18 RICH. J.L. & TECH. 3, 4 (2011) (discussing the honeycomb pattern creating cells); Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact*, 27 BERKELEY TECH. L.J. 117, 126 (2012) ("Service providers maintain large numbers of radio base stations (also called 'cell sites') spread through their geographic coverage areas. These cell sites are generally located on 'cell towers' serving geographic areas of varying sizes, depending upon topography and population concentration.").

17 Ian Herbert, *Where We Are with Location Tracking: A Look at the Current Technology and the Implications on Fourth Amendment Jurisprudence*, 16 BERKELEY J. CRIM. L. 442, 478 (2012) (quoting *In re Application for Pen Register & Trap/Trace Device*, 396 F. Supp. 2d at 749); *see* Owsley, *supra* note 15, at 3-4.

18 *In re Application of the U.S. for Historical Cell Site Data*, 747 F. Supp. 2d at 831 (citations omitted).

19 *Id.*; *see* Owsley, *supra* note 15, at 4.

20 S. REP. NO. 99-541, at 9; *see* Pell & Soghoian, *supra* note 16, at 127 ("mobile telephones (as their name suggests) are portable, and so when a phone moves away from the cell site with which it started a call and nearer to a different cell site, the call is 'handed over' from one cell site to another without interruption"); Owsley, *supra* note 15, at 4.

21 *ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the Comm. on the Judiciary*, 111th Cong. 13-14 (2010) (statement of Matt Blaze, Associate Professor, University of Pennsylvania); Stephanie K. Pell & Christopher Soghoian, *A Lot More than a Pen Register, and Less than a Wiretap*, 16 YALE J. L. & TECH. 134, 144 (2014); Blank, *supra* note 16, at 5; *see* Owsley, *supra* note 15, at 5.

22 *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 534 F. Supp. 2d 585, 590 (W.D. Pa. 2008) (citation omitted), *rev'd on other grounds*, 620 F.3d 304, 313 (3d Cir. 2010); *accord* Owsley, *supra* note 15, at 5; Kevin McLaughlin, Note, *The Fourth Amendment and Cell Phone Location Tracking: Where Are We?*, 29 HASTINGS COMM. & ENT. L.J. 421, 426 (2007).

23 Owsley, *supra* note 15, at 5.

24 U.S. DEP'T OF JUSTICE, ELECTRONIC SURVEILLANCE MANUAL 41 (rev. 2005) [hereinafter ELECTRONIC SURVEILLANCE MANUAL], *available at* www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf; *see In re* Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 115 (E.D.N.Y. 2011) ("Cell phones work by communicating with cell-sites operated by cell-phone service providers. Each cell-site operates at a certain location and covers a certain range of distance.").

25 *In re* Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 532 (D. Md. 2011); *see* Laurie Thomas Lee, *Can Police Track Your Wireless? Call Location Information and Privacy Law*, 21 CARDOZO ARTS. & ENT. L.J. 381, 384-86 (2003) (discussing the FCC's enhanced 9-1-1 regulations); 47 C.F.R. § 20.18(h) (2013) (setting accuracy standards for cell phone calls within targeted distances).

26 ELECTRONIC SURVEILLANCE MANUAL, *supra* note 24, at 41; *In re* Application of the U.S. for & Order: (1) Authorizing the Use of a Pen Register & Trap & Trace Device; (2) Authorizing Release of Subscriber & Other Info.; & (3) Authorizing the Disclosure of Location-Based Servs., 727 F. Supp. 2d 571, 573 (W.D. Tex. 2010) (cell site location information "is information that resides on computer servers of telecommunications providers"); *see In re* Application of the U.S. for an Order Authorizing the Use of a Cellular Tel. Digital Analyzer, 885 F. Supp. 197, 199 (C.D. Cal. 1995) ("The telephone company uses this information both to bill the subscriber of the cellular telephone based on its usage and also to connect the cellular telephone to the telephone number called."); Pell & Soghoian, *supra* note 16, at 128 ("Wireless service providers retain detailed logs for diagnostic, billing, and other purposes.").

27 STROBEL, *supra* note 3, at 3 ("GSM is the most common standard for communication. It is used in more than 200 countries and territories all over the world."); Karsten Nohl & Chris Paget, *GSM*--SRSLY?, CHAOS COMMC'N CONG. 2 (Dec. 27, 2009), http:// events.ccc.de/congress/2009/Fahrplan/attachments/1519_ 26C3.Karsten.Nohl.GSM.pdf (noting that GSM is used by eighty percent of the cell phone market, with over four billion users).

28 *In re* Application of the U.S. for an Order Pursuant to 18 U.S.C. §2703(d), 964 F. Supp. 2d 674, 675 (S.D. Tex. 2013); *see Analysis of IMEI Numbers*, INT'L NUMBERING PLANS, https://www.numberingplans.com/? page=analysis&sub=imeinr (last visited Dec. 14, 2014) ("All mobile phones are assigned a unique 15 digit IMEI code upon production.").

29 *See* STROBEL, *supra* note 3, at 4; *see also GSM*--The Base Station Subsystem (BSS), TUTORIALSPOINT, http:// www.tutorialspoint.com/gsm/gsm_base_ station_subsystem.htm (last visited Dec. 14, 2014).

30 STROBEL, *supra* note 3, at 13; David Talbot, *A 50-Watt Cellular Network*, MIT TECH. REV. (Feb. 10, 2010), http:// www.technologyreview.com/news/417442/a-50-watt-cellular-network.

31 STROBEL, *supra* note 3, at 4.

32 *Id.*

33 *Id.* at 4-5; *see* Blank, *supra* note 16, at 5-6 (discussing the handoff process).

34 STROBEL, *supra* note 3, at 5.

35 *Id.*

36 *See* Ryan Gallagher, *Criminals May Be Using Covert Mobile Phone Surveillance Tech for Extortion*, SLATE (Aug. 22, 2012, 9:00 AM), http:// www.slate.com/blogs/future_tense/2012/08/22/imsi_catchers_criminals_law_ enforcement_using_high_tech_portable_devices_to_intercept_communications_.html.

37 Chris Soghoian, Cellular Phones and Mobile Privacy: Direct Government Surveillance (Stingrays), Location Tracking and Biometrics Conference at Yale Law School (Mar. 3, 2013), *available at* http:// www.youtube.com/watch?v=OwutGSjNQ0k.

38 Declan McCullagh, *FBI Prepares to Defend 'Stingray' Cell Phone Tracking*, CNET (Mar. 27, 2013, 4:57 PM), http:// news.cnet.com/8301-13578_3-57576690-38/fbi-prepares-to-defend-stingray-cell-phone-tracking; Valentino-Devries, *supra* note 3. Interestingly, while the Harris Corporation notes a number of the products and services it provides to customers on its websites, it does not address this electronic surveillance technology. HARRIS, http:// www.harris.com (last visited Dec. 14, 2014).

39 Location Tracking and Biometrics Conference, *supra* note 37; *see* Gallagher, *supra* note 4; *see also In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 755 (S.D. Tex. 2005) (defining a TriggerFish as a device that "enables law enforcement to gather cell site data directly, without the assistance of the service provider").

40 Location Tracking and Biometrics Conference, *supra* note 37; Nohl & Paget, *supra* note 27.

41 STROBEL, *supra* note 3, at 13; *see* MMI Research Ltd. v. Cellxion Ltd., [2012] EWCA (Civ) 7, [4] (Eng.) ("These are devices used by the police and security services to discover the mobile phone numbers of suspected criminals or terrorists. Every mobile phone has an 'IMSI' associated with its SIM card, which is its permanent identity number.").

42 STROBEL, *supra* note 3, at 13; *see Integrated Ratio Communication Network*--Rohde & Schwarz, TIARA COMMC'NS, https://web.archive.org/web/20090209050710/http://tiaracom.com.my/rohde&schwarz.htm (last visited Dec. 14, 2014) (informational sheet from Rohde & Schwarz regarding its IMSI catcher's capacities).

43 STROBEL, *supra* note 3, at 7.

44 *Id.* at 13.

45 *Id.*; Pell & Soghoian, *supra* note 21, at 145-46; *see MMI Research*, [2012] EWCA (Civ) 7, [5] (Noting the IMSI catcher created by Rohde & Schwarz "involves the creation of a false base station. Mobile phones in a particular area will transmit information to a base station which operates as a transmitter and a receiver to and from the phones. The IMSI catcher uses a false base station which is constructed in a manner which leads the phone to believe it is genuine, and thereby to communicate with it.").

46 STROBEL, *supra* note 3, at 13; Kelly, *supra* note 3; Pell & Soghoian, *supra* note 21, at 147-48.

47 STROBEL, *supra* note 3, at 13; Blank, *supra* note 16, at 5 ("When a user places a call, the cell phone connects to the cell site with the strongest signal.").

48 STROBEL, *supra* note 3, at 13.

49 Kelly, *supra* note 3; Jennifer Valentino-Devries, *How 'Stingray' Devices Work*, WALL ST. J. (Sept. 21, 2011, 10:33 PM), http://blogs.wsj.com/digits/2011/09/21/how-stingray-devices-work.

50 Kelly, *supra* note 3; Jon Campbell, *LAPD Spy Device Taps Your Cell Phone*, L.A. WEEKLY (Sept. 13, 2012), http://www.laweekly.com/2012-09-13/news/LAPD-stingray-spying-cellphone.

51 Valentino-Devries, *supra* note 49; Campbell, *supra* note 50.

52 *In re* Application of the U.S. for an Order Authorizing the Use of a Cellular Tel. Digital Analyzer, 885 F. Supp. 197, 199 (C.D. Cal. 1995).

53 Valentino-Devries, *supra* note 49; *see* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 712-13 (2011) (discussing triangulation).

54 Valentino-Devries, *supra* note 49.

55 *Id.* Pinging is the system by which a cell phone sends out data to register with the nearest cell phone towers. *Id. See* United States v. Allums, No. 2:08-CR-30 TS, 2009 WL 806748, at *3 (D. Utah Mar. 24, 2009) (discussing an agent driving around with the device); United States v. Rigmaiden (*Rigmaiden I*), 844 F. Supp. 2d 982, 995 (D. Ariz. 2012) ("The FBI used the device in multiple locations. The FBI analyzed signals exchanged between the mobile tracking device and the aircard. The FBI would take a reading, move to another location, take another reading, move to another location, etc."); United States v. Rigmaiden (*Rigmaiden II*), No. CR 08-814-PHX-DGC, 2013 WL 1932800, at *15 (D. Ariz. May 8, 2013) (same).

56 Valentino-Devries, *supra* note 49.

57 *Allums*, 2009 WL 806748, at *1; *see* Blank, *supra* note 16, at 30-31 (discussing the admissibility of expert testimony by the FBI agent).

58 *Allums*, 2009 WL 806748, at *1.

59 *See* Thomas v. State, 127 So. 3d 658, 660 (Fla. Dist. Ct. App. 2013); Nathan Freed Wessler, *Victory: Judge Releases Information About Police Use of Stingray Cell Phone Trackers*, ACLU (June 3, 2014, 3:12 PM), https:// www.aclu.org/blog/national-security-technology-and-liberty/victory-judge-releases-information-about-police-use.

60 *See* Wessler, *supra* note 59.

61 *Rigmaiden I*, 844 F. Supp. 2d 982, 995 (D. Ariz. 2012); *Rigmaiden II*, No. CR 08-814-PHX-DGC, 2013 WL 1932800, at *15 (D. Ariz. May 8, 2013).

62 *Rigmaiden I*, 844 F. Supp. 2d at 995; *Rigmaiden II*, 2013 WL 1932800, at *15.

63 *See* Wessler, *supra* note 59 (noting that Tallahassee police were using a StingRay without a warrant).

64 18 U.S.C. §3123 (2012).

65 *Compare ID.* §3123(a)(1) (a pen register order is issued "if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation"), *with* FED. R. CRIM. P.41(d)(1) ("After receiving an affidavit or other information, a magistrate judge--or if authorized by Rule 41(b), a judge of a state court of record-- must issue the warrant if there is probable cause to search for and seize a person or property or to install and use a tracking device.").

66 *See generally* ELECTRONIC SURVEILLANCE MANUAL, *supra* note 24, at 38-400.

67 *See* United States v. Giordano, 416 U.S. 505, 511 n.2 (1974) (noting that a pen register is "a device that records telephone numbers dialed from a *particular phone*") (emphasis added); *see also id.* at 549 n.1 (Powell, J., concurring in part and dissenting in part) ("A pen register is a mechanical device attached to a given telephone line and usually installed at a central telephone facility. It records on a paper tape all numbers dialed from that line. It does not identify the telephone numbers from which incoming calls originated, nor does it reveal whether any call, either incoming or outgoing, was completed. Its use does not involve any monitoring of telephone conversations.").

68 434 U.S. 159 (1977).

69 *Id.* at 161 n.1; *see* 18 U.S.C. §3127(3) (2012).

70 434 U.S. at 166; *see* David McPhie, *Almost Private: Pen Registers, Packet Sniffers, and Privacy at the Margin*, 2005 STAN. TECH. L. REV. 1, 8 ("Almost ten years after Title III had been signed into law, the Supreme Court in *United States v. New York Telephone Company* relied on th[e] legislative history and the statutory language in holding that pen registers did not intercept the 'contents' of communications, and so did not fall within the scope of Title III.").

71 *N.Y. Tel.*, 434 U.S. at 166 (quoting 18 U.S.C. § 2518(1) (1976)) (emphasis in original).

72 *Id.* at 168.

73 *Id.* at 168-69; *see* FED. R. CRIM. P. 41(d) ("After receiving an affidavit or other information, a magistrate judge ... must issue the warrant if there is probable cause to search for and seize a person or property or to install and use a tracking device.").

74 *N.Y. Tel.*, 434 U.S. at 170.

75 S. REP. NO. 99-541, at 9 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3557 ("Title III of the bill addresses pen registers.").

76 Electronics Communications Privacy Act of 1986, Pub. L. No. 99-5088, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.); *In re* Application of the U.S. for an Order Authorizing the Use of a Cellular Tel. Digital Analyzer, 885 F. Supp. 197, 200 (C.D. Cal. 1995) (addressing the statutory definition); *accord* United States v. Forrester, 512 F.3d 500, 512 (9th Cir. 2008) (citing 18 U.S.C. §3127(3) and explaining this pen register definition applied when the surveillance occurred, between May and July 2001); Donahue v. Gavin, 280 F.3d 371, 373 n.3 (3d Cir. 2002); Brown v. Waddell, 50 F.3d 285, 290 (4th Cir. 1995) (citing 18 U.S.C. §3127(3)); *see* U.S. Telecom Ass'n v. FCC, 227 F.3d 450, 454 (D.C. Cir. 2000) ("Pen registers record telephone numbers of outgoing calls.").

77 *See generally* Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended in scattered sections of 47 U.S.C.); *see also* Timothy Casey, *Electronic Surveillance and the Right to Be Secure*, 41 U.C. DAVIS L. REV. 977, 1003 (2008).

78 47 U.S.C. §1002(a)(2)(B) (2011).

79 *See Police Access to Advanced Communication Systems: Hearing Before the Subcomm. on Tech. & the Law of the Comm. on the Judiciary, U.S. S., and the Subcomm. on Civil & Constitutional Rights of the Comm. on the Judiciary, H.R.*, 103d Cong. (1994) (statement of Louis J. Freeh, Director, FBI), *available at* 1994 WL 223962; *see also In re* Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register, 415 F. Supp. 2d 211, 216-17 (W.D.N.Y. 2006) (discussing Director Freeh's testimony); *In re* Application of the U.S. for an Order Authorizing the Disclosure of Prospective Cell Site Info., 412 F. Supp. 2d 947, 955 (E.D. Wis. 2006) (same).

80 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered sections of 8, 12, 15, 18, 20, 31, 42, 47, 49, 50 and 51 U.S.C.); *see In re* Application of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d 448, 455 (S.D.N.Y. 2006) (discussing legislative history).

81 18 U.S.C. §3127(3) (2012); *see* United States v. Jadlowe, 628 F.3d 1, 6 n.4 (1st Cir. 2010) ("A 'pen register' is a device used, inter alia, to record the dialing and other information transmitted by a targeted phone."). The Patriot Act distinguished a pen register from a trap and trace device, which is defined as "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication." 18 U.S.C. §3127(4).

82 18 U.S.C. §3123(b)(1) (2012) (emphasis added); *see* Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1431-32 (2004) ("[T]he statute required the court order to specify the number of the 'telephone line' to which the pen register or trap and trace would be attached.").

83 U.S. DEP'T OF JUSTICE, COMPUTER CRIME AND INTELLECTUAL PROP. SECTION, FIELD GUIDANCE ON NEW AUTHORITIES THAT RELATE TO COMPUTER CRIME AND ELECTRONIC EVIDENCE ENACTED IN THE USA PATRIOT ACT OF 2001 4 (2001), *available at* https://www.student.cs.uwaterloo.ca/~cs492/papers/ccips.pdf [hereinafter FIELD GUIDANCE ON NEW AUTHORITIES]; *see* Patricia Mell, *Big Brother at the Door: Balancing National Security with Privacy Under the USA Patriot Act*, 80 DENV. U. L. REV. 375, 402 n.226 (2002).

84 FIELD GUIDANCE ON NEW AUTHORITIES, *supra* note 83, at 4.

85 *See id.* at 5.

86 *In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 753 n.8 (S.D. Tex. 2005); *accord In re* Application of the U.S. for an Order (1) Authorizing the Use of Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Information and/or Cell Site Information, 396 F. Supp. 2d 294, 318 (E.D.N.Y. 2005) (adopting the reasoning of *In re Application for Pen Register & Trap/Trace Device*, 396 F. Supp. 2d 747).

87 *In re* Application of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d 448, 456 (S.D.N.Y. 2006)); *see In re* Application of the U.S. for an Order Authorizing the Use of a Pen Register & Trap on [xxx]Internet Service Account/User Name [[xxxxxxxxxxx@xxx.com], 396 F. Supp. 2d 45, 49-50 (D. Mass. 2005) ("There can be no doubt that the expanded definition of a pen register, especially the use of the term 'device or *process*,' encompasses e-mail communications and communications over the internet.") (emphasis in original).

88 United States v. Jadlowe, 628 F.3d 1, 6 n.4 (1st Cir. 2010); *In re* Applications of the U.S. for Orders (1) Authorizing the Use of Pen Registers & Trap & Trace Devices & (2) Authorizing Release of Subscriber Info., 515 F. Supp. 2d 325, 328 (E.D.N.Y. 2007) ("In layman's terms, a pen register is a device capable of recording all digits dialed from a particular telephone."); United States

v. Bermudez, No. IP 05-43-CR-B/F, 2006 WL 3197181, at *8 (S.D. Ind. June 30, 2006) (unpublished) ("A 'pen register' records telephone numbers dialed for outgoing calls made from the target phone."); *In re Application of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel.*, 460 F. Supp. 2d at 455 (pen registers apply to particular cell phones); *In re* Application of the U.S. for an Order for Disclosure of Telecomm. Records & Authorizing the Use of a Pen Register & Trap & Trace, 405 F. Supp. 2d 435, 438 (S.D.N.Y. 2005) ("Pen Register Statute is the statute used to obtain information on an ongoing or prospective basis regarding outgoing calls from a particular telephone."); *In re* Application of U.S. for an Order Authorizing Installation & Use of a Pen Register & a Caller Identification Sys. on Tel. Nos. [Sealed] & [Sealed] & the Production of Real Time Cell Site Info., 402 F. Supp. 2d 597, 602 (D. Md. 2005) ("A pen register records telephone numbers dialed for outgoing calls from the target phone..."); *In re Application for Pen Register & Trap/Trace Device*, 396 F. Supp. 2d at 752 ("A 'pen register' is a device that records the numbers dialed for outgoing calls made from the target phone.").

89 *See* United States v. N.Y. Tel. Co., 434 U.S. 159, 170 (1977).

90 *See id.*

91 18 U.S.C. §3122 (2012); *see* United States v. Fregoso, 60 F.3d 1314, 1320 (8th Cir. 1995) ("[U]pon a proper application being made under 18 U.S.C. §3122, 'the court *shall* enter an ex parte order authorizing the installation' of such a device." (emphasis in original)).

92 *In re* Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, 846 F. Supp. 1555, 1559 (M.D. Fla. 1994); *see* Mell, *supra* note 83, at 403.

93 Susan Freiwald, *Uncertain Privacy: Communication Attributes After The Digital Telephony Act*, 69 S. CALIF. L. REV. 949, 988-89 (1996).

94 *See* Bellia, *supra* note 82, at 1431 ("[T]he statute does not appear to require the judge to independently assess the factual predicate for the government's certification."); Lee, *supra* note 25, at 397 ("Pen register and trap and trace authority is also problematic in that orders are generally rubberstamped without question."). *But see In re* Application of the U.S. for an Order Authorizing the Installation & Use of a Device [Pen Register], No. 87-0831RC, 1987 WL 8946 (D. Mass. Apr. 3, 1987) (denying a pen register without prejudice due to deficiencies in the application).

95 *See* Elec. Privacy Info. Ctr. v. FBI, 933 F. Supp. 2d 42 (D.D.C. 2013) (denying the FBI's motion for a stay of deadline to provide responses to Freedom of Information Act requests regarding StingRay); Paul Ohm, *Electronic Surveillance Law and the Intra-Agency Separation of Powers*, 47 U.S.F. L. REV. 269, 275 (2012) (discussing rumors of various types of electronic surveillance, including StingRays, that have ultimately been confirmed); Kurth & Abdel-Razzaq, *supra* note 11; Nathan Freed Wessler, *U.S. Marshals Seize Local Cops' Cell Phone Tracking Files in Extraordinary Attempt to Keep Information From Public*, ACLU (June 3, 2014, 12:13 PM), https:// www.aclu.org/blog/national-security-technology-and-liberty/us-marshals-seize-local-cops-cell-phone-tracking-files (discussing the federal government's efforts to prevent disclosure of information related to the Sarasota Police Department's use of a cell site simulator).

96 *In re* Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, 890 F. Supp. 2d 747, 747 (S.D. Tex. 2012).

97 Owsley, *supra* note 15, at 40; Pell & Soghoian, *supra* note 16, at 158.

98 Ryan Gallagher, *Judge Oks FBI Tracking Tool That Tricks Cellphones with Clandestine Signal*, SLATE (May 9, 2013, 4:35 PM), http:// www.slate.com/blogs/future_tense/2013/05/09/ stingray_imsi_catcher_judge_oks_ fbi_use_of_controversial_tool_in_daniel.html. Obviously, these nondisclosure agreements do not apply to FBI agents seeking judicial authorization. *See* Wessler, *supra* note 59 (discussing the FBI's attempt to keep sealed testimony about the Tallahassee Police Department's use of a StingRay); Kurth & Abdel-Razzaq, *supra* note 11.

99 Cyrus Farivar, *Legal Experts: Cops Lying About Cell Tracking "Is a Stupid Thing to Do,"* ARS TECHNICA (June 20, 2014, 9:38 PM), http:// arstechnica.com/tech-policy/2014/06/legal-experts-cops-lying-about-cell-tracking-is-a-stupid-thing-to-do.

100 *In re Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device*, 890 F. Supp. 2d at 749.

101 E-mail from Magistrate Judge, U.S. District Court for the Eastern District of Texas, to Brian Owsley (Mar. 5, 2013, 10:58 AM) (on file with author).

102 *Id.*

103 *See generally In re* Application of the U.S. for an Order Authorizing the Use of a Cellular Tel. Digital Analyzer, 885 F. Supp. 197 (C.D. Cal. 1995); *see also Fourth Amendment and the Internet: Hearing Before the Subcomm. on the Constitution of the Comm. on the Judiciary H.R.*, 106th Cong. 165-66 (2000), *available at* http://commdocs.house.gov/committees/judiciary/hju 66503.000/hju66503_0.htm (prepared statement of Robert Corn-Revere, Att'y, Hogan & Hartson L.L.P.) (discussing the decision from the Central District of California).

104 In re *Application for Use of a Cellular Tel. Digital Analyzer*, 885 F. Supp. at 199.

105 *Id.* at 200.

106 *Id.* at 199.

107 *Id. (*discussing Smith v. Maryland, 442 U.S. 735, 742-45 (1979)); *see* Pell & Soghoian, *supra* note 16, at 157-58.

108 In re *Application for Use of a Cellular Tel. Digital Analyzer*, 885 F. Supp. at 199-200; *see* Freiwald, *supra* note 93, at 988-89 ("The court, having refused to consider the device a pen register since it did not attach to a telephone line, found that no court order of any kind was required to use the device."); *Fourth Amendment and the Internet: Hearing Before the Subcomm. on the Constitution of the Comm. on the Judiciary H.R.*, 106th Cong. 165 (2000) (prepared statement of Robert Corn-Revere, Att'y, Hogan & Hartson L.L.P.) (noting, regarding this decision, that "[c]onsistent with the statutory language and legislative history, reviewing courts have interpreted these provisions literally, and narrowly").

109 In re *Application for Use of a Cellular Tel. Digital Analyzer*, 885 F. Supp. at 201 (discussing §3123(b)(1)(C)).

110 *Id.* at 201.

111 *Id.*

112 *Id.* at 202.

113 *Id.*

114 *In re* Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, No. 2:11-mj-00468 (S.D. Tex Apr. 6, 2011).

115 *Id.* at 1.

116 *Id.* at 2.

117 *Id.*

118 *Id.* at 1.

119 *Id.* at 2.

120 Hearing Minutes, *In re* Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, No. 2:11-mj-00468 (S.D. Tex. May 6, 2011).

121 *Id.* at 2-3.

122 *See generally id.*

123 Order Granting Mot. to Withdraw, *In re* Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, No. 2:11-mj-00468 (S.D. Tex. May 6, 2011).

124 *See generally In re* Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, 890 F. Supp. 2d 747 (S.D. Tex. 2012); *see also* Pell & Soghoian, *supra* note 16, at 160-62.

125 *In re Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device*, 890 F. Supp. 2d at 748.

126 *Id.*

127 *Id.*; *accord* Pell & Soghoian, *supra* note 16, at 161.

128 *See In re Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device*, 890 F. Supp. 2d at 748.

129 *Id.* at 749; *see* ELECTRONIC SURVEILLANCE MANUAL, *supra* note 24, at 38-40.

130 *In re Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device*, 890 F. Supp. 2d at 749.

131 *Id.* at 749 n.1.

132 *Id.* at 749 (discussing United States v. Giordano, 416 U.S. 505, 512 n.2 (1974) and United States v. N.Y. Tel. Co., 434 U.S. 159, 161 n.1(1977)).

133 *Id.* at 749.

134 *Id.* at 750-51; *see* Gus Hosein & Caroline Wilson Palow, *Modern Safeguards for Modern Surveillance: An Analysis of Innovations in Communications Surveillance Techniques*, 74 OHIO ST. L.J. 1071, 1102 (2013).

135 *In re* Application of the U.S. for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, 890 F. Supp. 2d at 751 (discussing 18 U.S.C. § 3123(b)(1)(C)); Pell & Soghoian, *supra* note 16, at 161.

136 *In re* Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device (N.D. Tex. Apr. 5, 2012) (on file with author).

137 *Id.*

138 *Id.*

139 *Id.* at 1-2.

140 *Id.* at 2-3.

141 *Id.* at 3 (emphasis in original).

142 Order Granting, *In re* Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device (N.D. Tex. Apr. 5, 2012).

143 *Id.* at 2.

144 *Id.* (emphasis in original).

145 *Id.*

146 E-mail from Magistrate Judge, U.S. District Court for the Northern District of Texas, to Brian Owsley (June 4, 2012, 11:49 AM) (on file with author).

147 *Id.*

148 *In re* Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register/Trap & Trace Device, No. [Redacted] (D. Md. Mar. [Redacted], 2012).

149 *Id.*

150 *Id.* at 2.

151 *Id.*at 3 n.4.

152 *Id.*

153 *Id.* at 3-4, 4 n.5.

154 *Id.* at 4.

155 *Id.* at 5.

156 *Id.* at 3 n.3 (citing *In re* Application of the U.S. for an Order Authorizing the Use of a Cellular Tel. Digital Analyzer, 885 F. Supp. 197 (C.D. Cal. 1995)).

157 *Id.*

158 *Id.*

159 *In re* Application of the U.S. for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device for the Cellular Telephone Facility Currently Assigned Telephone Number [Redacted], Mag. No. 12-3016 (D.N.J. Feb. 21, 2012).

160 *Id.* at 1.

161 *Id.*

162 *Id.* at 4.

163 *Id.*

164 *See Rigmaiden I*, 844 F. Supp. 2d 982, 987-88 (D. Ariz. 2012).

165 *Id.* "Air cards are devices that plug into a computer and use the wireless cellular networks of phone providers to connect the computer to the internet. The devices are not phones and therefore don't have the ability to receive incoming calls..." Kim Zetter, *Secrets of FBI Smartphone Surveillance Tool Revealed in Court Fight*, WIRED (Apr. 9, 2013, 6:30 AM), http:// www.wired.com/ threatlevel/2013/04/verizon-rigmaiden-aircard/all.

166 *Rigmaiden I*, 844 F. Supp. 2d at 993.

167 [Proposed] Brief Amici Curiae in Support of Daniel Rigmaiden's Motion to Suppress at 14, *Rigmaiden II*, No. CR 08-814-PHX-DGC, 2013 WL 1932800 (D. Ariz. May 8, 2013).

168 *Rigmaiden I*, 844 F. Supp. 2d at 995.

169 *Id.*

170 *Id.*

171 *Id.*

172 *Id.*

173 *Id.*

174 *Id.* at 995-96.

175 *Rigmaiden II*, No. CR 08-814-PHX-DGC, 2013 WL 1932800, at *14 (D. Ariz. May 8, 2013).

176 *Id.*

177 *Id.*

178 *Id.*

179 *Id.* at *16.

180 *Id.*

181 *Id.* at *17.

182 *Id.* at *8-9.

183 *Id.* at *18.

184 *Id.* at *19.

185 *Id.* at *33-34.

186 Soghoian, *supra* note 37.

187 E-mail from Magistrate Judge, U.S. District Court for the Western District of Washington, to Brian Owsley (May 31, 2012, 11:40 AM) (on file with author).

188 E-mail from Magistrate Judge, U.S. District Court for the Eastern District of Texas, to Brian Owsley (Mar. 5, 2013, 10:58 AM) (on file with author).

189 *Id.*

190 *Id.*

191 E-mail from Magistrate Judge, U.S. District Court for the Southern District of California, to Brian Owsley (May 31, 2012, 1:01 PM) (on file with author).

192 *Id.*; *see* United States v. Espudo, 954 F. Supp. 2d 1029, 1045 (S.D. Cal. 2013) (denying as moot a motion to suppress evidence obtained by a cell site simulator where the federal agent testified that the information gathered was not "utilized to further the investigation").

193 *The Office of Enforcement Operations*--Its Role in the Area of Electronic Surveillance, 45 U.S. ATT'Y BULL., no. 5, Sept. 1997, at 8, 11, *available at* http://www.justice.gov/usao/eousa/foia_reading_room/usab4505.pdf.

194 *Id.* at 13 (emphasis in original).

195 *Id.* at 13-14.

196 *Id.* at 14.

197 *Id.*

198 *Id.*

199 *Id.* (emphasis in original).

200 *Id.*

201 *Id.*

202 ELECTRONIC SURVEILLANCE MANUAL, *supra* note 24, at ii.

203 *Id.* at 38-41.

204 ELECTRONIC SURVEILLANCE MANUAL, *supra* note 24, at 41. The MIN used to be the same as the assigned cell phone number. United States v. O'Shield, No. 97-2493, 1998 WL 104625, at *1 n.1 (7th Cir. Mar. 6, 1998) (per curiam) (unpublished table decision); United States v. Bailey, 41 F.3d 413, 415 (9th Cir. 1994). Pursuant to Federal Communications Commission policy, these numbers are now separate. Cellular Telecomms. Indus. Ass'n's Petition for Forbearance from Commercial Mobile Radio Servs. No. Portability Obligations & Tel. No. Portability, 14 FCC Rcd. 3092, 3105 (1999); see Pinney v. Nokia, Inc., 402 F.3d 430, 439-40 (4th Cir. 2005).

205 *Id.* at 44.

206 *Id.*; *compare with* Valentino-Devries, *supra* note 49.

207 ELECTRONIC SURVEILLANCE MANUAL, *supra* note 24, at 171-74.

208 *Id.* at 171.

209 *Id.* at 173.

210 U.S. ATTORNEY'S OFFICE, DISTRICT OF ARIZ., APPLICATION FOR USE OF AN ELECTRONIC SERIAL NUMBER IDENTIFIER [hereinafter ARIZONA FORM APPLICATION] (2012) (on file with author). Acting United States Attorney Ann Birmingham Scheel served until July 3, 2012, when the new United States Attorney was sworn in. *See Meet the U.S. Attorney*, U.S. DEP'T OF JUSTICE, http:// www.justice.gov/usao/az/meettheattorney.html (last visited Dec. 14, 2014).

211 ARIZONA FORM APPLICATION, *supra* note 210, at 1.

212 *Id.*

213 *Id.*

214 *Id.*

215 *Id.* at 1-2.

216 *Id.* at 2.

217 *Id.* at 4.

218 *Id.* at 4-5.

219 *Id.* at 5.

220 *Id.* at 6.

221 *Id.* at 9.

222 *Id.* at 10.

223 *Id.* at 13-14 (discussing Smith v. Maryland, 442 U.S. 735 (1979) and United States v. Forrester, 495 F.3d 1041, 1049-50 (9th Cir. 2007)).

224 *Id.* at 11.

225 *Id.* (quoting 18 U.S.C. §3123(b)(1)(C)).

226 *Id.*

227 *Id.* at 11-12 (discussing *In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Authorization, 396 F. Supp. 2d 747, 761-62 (S.D. Tex. 2005)).

228 *Id.* at 12 (discussing In re *Application for Pen Register & Trap/Trace Device*, 396 F. Supp. 2d at 762).

229 *Id.* at 13-15.

230 *Id.*

231 Letter from Donal Brown, Editor, First Amendment Coal., to Martin Bland, Officer-in-Charge, Discovery Section, L.A. Police Dep't (Sept. 29, 2012) (citing CAL. GOV. CODE §6250, *et seq.*), *available at* firstamendmentcoalition.org/wp-content/uploads/2013/03/LAPD-CPRA.pdf.

232 *Id.*

233 *Id.*

234 *Id.*

235 *Id.*

236 *Id.*

237 Letter from Martin Bland, Officer-in-Charge, Discovery Section, L.A. Police Dep't, to Donal Brown, Editor, First Amendment Coal. (Dec. 14, 2012), *available at* firstamendmentcoalition.org/wp-content/uploads/2013/03/LAPD-CPRA.pdf.

238 *Id.*

239 *Id.*

240 *Id.* (citing CAL. GOV. CODE §6255).

241 Letter from Martin Bland, Officer-in-Charge, Discovery Section, L.A. Police Dep't, to Donal Brown, First Amendment Coal. (Dec. 28, 2012), *available at* firstamendmentcoalition.org/wp-content/uploads/2013/03/LAPD-CPRA.pdf.

242 Memorandum from Kirk J. Albanese, Chief of Detectives, L.A. Police Dep't & Stephen R. Jacobs, Chief of Staff, L.A. Police Dep't to All Commanding Officers (Oct. 16, 2012), *available at* firstamendmentcoalition.org/wp-content/uploads/2013/03/LAPD-CPRA.pdf. Indeed, earlier that year, the Supreme Court had concluded that the attachment of a GPS tracking device to the defendant's car, whereby the government monitored its movement on public streets, constituted a Fourth Amendment search and affirmed the suppression of the resulting evidence. *See* United States v. Jones, 132 S. Ct. 945, 964 (2012).

243 Memorandum from Kirk J. Albanese & Stephen R. Jacobs to All Commanding Officers, *supra* note 242.

244 Letter from Martin Bland to Donal Brown, *supra* note 241.

245 *Id.*

246 *Id.*

247 *Id.*

248 *Id.*

249 *Id.* at 11-13.

250 18 U.S.C. §2703(c)(2) (In the Stored Communications Act, Congress authorized law enforcement officials to obtain telecommunications customer records, including "name; address; local and long distance telephone connection records, or records of session times and durations; length of service (including start date) and types of service utilized; telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and means and source of payment for such service (including any credit card or bank account number)."); *accord In re* §2703(d) Order, 787 F. Supp. 2d 430, 436 (E.D. Va. 2011); *see In re* Application of the U.S. for an Order Pursuant to 18 U.S.C. §2703(d), 157 F. Supp. 2d 286, 288 (S.D.N.Y. 2001) (a §2703 order authorized law enforcement officials to obtain "the subscriber's name, home address, telephone number, e-mail address and any other identifying information [the provider] may have, such as date of birth, social security number, driver's license number and billing information"). For a court to issue an order pursuant to §2703(d), the government must demonstrate "*specific and articulable facts* showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are *relevant and material to an ongoing criminal investigation*." 18 U.S.C. § 2703(d) (2013) (emphasis added).

251 Letter from Martin Bland to Donal Brown, *supra* note 241, at 11-13.

252 Casey, *supra* note 77, at 983.

253 U.S. CONST. amend IV.

254 *Id.*; *see* FED. R. CRIM. P. 41 (addressing the issuance of warrants, including for the seizure of electronically stored information).

255 Casey, *supra* note 77, at 983.

256 *See, e.g.*, Susan W. Brenner, *The Privacy Privilege: Law Enforcement, Technology, and the Constitution*, 7 J. TECH. L. & POL'Y 123, 150 (2002) ("When the Fourth Amendment was adopted, the protection against invasions of privacy lay in trespass law ...."); Jace C. Gatewood, *Warrantless GPS Surveillance: Search and Seizure*--Using the Right to Exclude to Address the Constitutionality of GPS Tracking Systems Under the Fourth Amendment, 42 U. MEM. L. REV. 303, 333-34 (2011); Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-first Century*, 65 IND. L.J. 549, 556 n.36 (1990) ("Linking the fourth amendment to its historical context, the Supreme Court during the pre-*Katz* era allowed the law of trespass to control the outcome whenever it was claimed that government had conducted a 'search.'"); David E. Steinberg, *The Uses and Misuses of Fourth Amendment History*, 10 U. PA. J. CONST. L. 581, 583 (2008) ("Historical sources indicate that the Framers were focused on a single, narrow problem: physical trespasses into houses by government agents.").

257 (1765) 95 Eng. Rep. 807 (K.B.); Katz, *supra* note 256, at 556 n.36.

258 Orin S. Kerr, *The Curious History of Fourth Amendment Searches*, 2012 SUP. CT. REV. 67, 69 (2012); *see* Fabio Arcila, Jr., *GPS Tracking Out of Fourth Amendment Dead Ends:* United States v. Jones *and the* Katz *Conundrum*, 91 N.C. L. REV. 1, 21-22 (2012) ("*Katz* famously moved search jurisprudence to a privacy model. It did so by rejecting the property-centric Fourth Amendment model that had previously controlled, and which the Court had applied in *Olmstead v. United States*.").

259 Boyd v. United States, 116 U.S. 616, 618 (1886).

260 *Id.* at 622 (emphasis in original).

261 *Id.* at 625-28.

262 277 U.S. 438, 455 (1928).

263 *Id.* at 457 (emphasis added); *see* Henry F. Fradella, et al., *Quantifying* Katz: *Empirically Measuring "Reasonable Expectations of Privacy" in the Fourth Amendment Context*, 38 AM. J. CRIM. L. 289, 325 (2011) ("The majority rested its decision on the premise that since the wiretapping involved no physical trespass onto the defendants' property, there had been no Fourth Amendment violation.").

264 *Olmstead*, 277 U.S. at 463.

265 265 U.S. 57, 59 (1924) (holding that defendant's illicit whiskey discovered by revenue officers in an open field on the property of the defendant's father's did not violate the Fourth Amendment); *see* United States v. Karo, 468 U.S. 705, 712-13 (1984) ("technical trespass" in applying the beeper was insufficient to establish a Fourth Amendment violation).

266 *Olmstead*, 277 U.S. at 465.

267 *Id.* at 473 (Brandeis, J., dissenting) (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

268 316 U.S. 129 (1942).

269 *Id.* at 134.

270 *Id.* at 134-35.

271 *Id.* at 136 (Stone, C.J. & Frankfurter, J., dissenting).

272 *Id.* (Murphy, J., dissenting).

273 389 U.S. 347 (1967).

274 *Id.* at 352; *see* Owsley, *supra* note 15, at 10 (discussing *Katz*). *But see* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 821 (2004) (the question of "[e]xactly *why* the user of the phone booth was constitutionally entitled to his privacy was left to the reader's imagination") (emphasis in original).

275 *Katz*, 389 U.S. at 352.

276 *Id.* at 353.

277 *Id.* at 360 (Harlan, J., concurring) ("I join the opinion of the Court, which I read to hold only...that an enclosed telephone booth is an area where, like a home, and unlike a field, a person has a constitutionally protected reasonable expectation of privacy ....") (citations omitted); *see* Casey, *supra* note 77, at 988 (discussing Justice Harlan's concurrence).

278 392 U.S. 1, 9 (1968) ("We have recently held that 'the Fourth Amendment protects people, not places'...and wherever an individual may harbor a reasonable 'expectation of privacy.'") (quoting *Katz*, 389 U.S. at 351; 389 U.S. at 361 (Harlan, J., concurring)).

279 466 U.S. 109 (1984).

280 *Id.* at 113 (citations omitted); *see* Rakas v. Illinois, 439 U.S. 128, 144 n.12 (1978) ("Legitimation of expectations of privacy by law must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society.").

281 Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 316 (2012).

282 Kerr, *supra* note 274, at 809-10.

283 Kerr, *supra* note 281, at 316-17.

284 Bellia, *supra* note 82, at 1382.

285 442 U.S. 735 (1979).

286 *Id.* at 745-46.

287 *See* Casey, *supra* note 77, at 993 ("The Court's description of a 1971 pen register [in *Smith*] highlights the dramatic change in the capability of a 2007 pen register.").

288 442 U.S. at 736 n.1; *see* Casey, *supra* note 77, at 992 ("Significantly, the device did not 'overhear' oral communications, and was not capable of determining whether or not the call was completed.").

289 *See* California v. Riley, 134 S. Ct. 2473, 2493 (2014) (distinguishing *Smith* in part because "call logs typically contain more than just phone numbers").

290 *See* Marc McAllister, *The Fourth Amendment and New Technologies: The Misapplication of Analogical Reasoning*, 36 S. ILL. U. L.J. 475, 522 (2012) ("[R]ulings associated with more traditional forms of surveillance do not always comport with society's actual expectations of privacy and often fail to account for relevant differences between the analogized cases.").

291 Scott Shane & Colin Moynihan, *Drug Agents Use Vast Phone Trove, Eclipsing N.S.A.'s*, N.Y. TIMES, Sept. 2, 2013, at A1; John Shiffman & Kristina Cooke, *Exclusive: U.S. Directs Agents to Cover up Program Used to Investigate Americans*, REUTERS (Aug. 5, 2013, 3:25 PM), http:// www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805.

292 547 U.S. 103 (2006).

293 *Id.* at 107; *see* Jeremy A. Blumenthal et al., *The Multiple Dimensions of Privacy: Testing Lay "Expectations of Privacy,"* 11 U. PA. J. CONST. L. 331, 334 (2009).

294 *Randolph*, 547 U.S. at 107.

295 *Id.* at 122-23 ("This case invites a straightforward application of the rule that a physically present inhabitant's express refusal of consent to a police search is dispositive as to him, regardless of the consent of a fellow occupant. Scott Randolph's refusal is clear, and nothing in the record justifies the search on grounds independent of Janet Randolph's consent.").

296 *Id.* at 128 (Roberts, C.J., dissenting) ("The correct approach to the question presented is clearly mapped out in our precedents: The Fourth Amendment protects privacy. If an individual shares information, papers, *or places* with another, he assumes the risk that the other person will in turn share access to that information or those papers *or places* with the government.") (emphasis in original).

297 *Id.* at 129-30 (Roberts, C.J., dissenting).

298 *Id.* at 131 (Roberts, C.J., dissenting); *see* Fradella et al., *supra* note 263, at 293 ("[J]udges make no attempt to discern actual societal opinions when adjudicating Fourth Amendment disputes."); Blumenthal et al., *supra* note 293, at 332 (judges often "made explicit psychological assumptions about perceptions and expectations of privacy, assumptions that are not necessarily supported by empirical findings").

299 Transcript of Oral Argument at 9-10, United States v. Jones, 132 S. Ct. 945 (2012) (No. 10-1259); *see* Arcila, *supra* note 258, at 40 (discussing this exchange).

300 Transcript of Oral Argument, *Jones*, 132 S. Ct. 945 (No. 10-12599).

301 A significant majority of individuals surveyed have a reasonable expectation of privacy from electronic tracking of one's vehicle. *See* Fradella et al., *supra* note 263, at 325.

302 *Randolph*, 547 U.S. at 120.

303 *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring) (citing Smith v. Maryland, 442 U.S. 735, 742 (1979); United States v. Miller, 425 U.S. 435, 443 (1976)).

304 *Id.*

305 *ID.* at 961 (Alito, J., concurring in judgment).

306 *Id.* at 962.

307 533 U.S. 27 (2001).

308 *Id.* at 36. *But see* City of Ontario v. Quon, 560 U.S. 746, 759 (2010) ("The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."); *see also* Owsley, *supra* note 15, at 11.

309 United States v. Davis, 754 F.3d 1205, 1213 (11th Cir. 2014).

310 *Id.* at 1215.

311 *Id.* at 1217.

312 California v. Riley, 134 S. Ct. 2473 (2014).

313 *Id.* at 2480.

314 *Id.*

315 *Id.* at 2481.

316 *Id.*

317 *Id.*

318 *Id.*

319 *Id.*

320 *Id.*

321 *Id.* at 2482.

322 *Id.* at 2485.

323 *Id.*

324 *Id.* at 2489.

325 *Id.*

326 *Id.* at 2490.

327 *Id.* at 2495.

328 425 U.S. 435 (1976).

329 *Id.* at 437.

330 *Id.* at 438-39.

331 *Id.* at 445.

332 *Id.* at 440.

333 *See* Blumenthal et al., *supra* note 293, at 334 ("Little relevant empirical research has been conducted on perceptions of privacy...."); Fradella et al., *supra* note 263, at 338 ("Much more research also needs to be conducted to assess the impact of changes in U.S. surveillance and search and seizure jurisprudence on the privacy rights of citizens.").

334 Fradella et al., *supra* note 263, at 338.

335 *Id.* at 366.

336 *Id.*

337 Christopher Slobogin & Joseph E. Schumacher, *Rating the Intrusiveness of Law Enforcement Searches and Seizures*, 17 LAW & HUM. BEHAV. 183, 198 (1993).

338 460 U.S. 276 (1983).

339 Fradella et al., *supra* note 263, at 366-67.

340 JENNIFER KING & CHRIS JAY HOOFNAGLE, RESEARCH REPORT: A SUPERMAJORITY OF CALIFORNIANS SUPPORTS LIMITS ON LAW ENFORCEMENT ACCESS TO CELL LOCATION INFORMATION 8 (2008), *available at* www.ftc.gov/os/comments/mobilevoice/534331-00005.pdf.

341 Fradella et al., *supra* note 263, at 366.

342 *See, e.g.*, State v. McAllister, 875 A.2d 866, 875 (N.J. 2005); State v. Thompson, 810 P.2d 415, 418 (Utah 1991) (the Utah Constitution provides individuals "a right to be secure against unreasonable searches and seizures of their bank statements"); Winfield v. Div. of Pari-Mutuel Wagering, Dep't of Bus. Regulation, 477 So. 2d 544, 548 (Fla. 1985) ("[T]he law in the state of Florida recognizes an individual's legitimate expectation of privacy in financial institution records."); Charnes v. DiGiacomo, 612 P.2d 1117, 1121-22, 1124 (Colo. 1980) (en banc) (distinguishing *Miller* and holding that "[a]n individual has an expectation of privacy in records of his financial transactions held by a bank in Colorado.");; People v. Jackson, 452 N.E.2d 85, 89 (Ill. App. Ct. 1983) ("[W]e reject the idea set out in *Miller* that a citizen waives any legitimate expectation in her financial records when she resorts to the banking system.").

343 *See, e.g.*, Commonwealth v. Melilli, 555 A.2d 1254, 1258 (Pa. 1989) (expressly rejecting *Smith v. Maryland*); Richardson v. State, 865 S.W.2d 944, 951-52, 952 n.6 (Tex. Crim. App. 1993) (rejecting *Smith v. Maryland*).

344 *See, e.g.*, People v. Sporleder, 666 P.2d 135, 144 (Colo. 1983) (en banc) (holding that the Colorado Constitution provides a telephone subscriber with a reasonable expectation of privacy in the numbers dialed such that they cannot be obtained without a search warrant based on probable cause); Shaktman v. State, 553 So. 2d 148, 151-52 (Fla. 1989) ("Because the pen register intrudes upon fundamental privacy interests [based on the Florida Constitution], the state has the burden of demonstrating both that the intrusion is justified by a compelling state interest and that the state has used the least intrusive means in accomplishing its goal."); State v. Rothman, 779 P.2d 1, 7 (Haw. 1989) ("[P]ersons using telephones in the State of Hawaii have a reasonable expectation of privacy, with respect to the telephone numbers they call on their private lines...."); State v. Thompson, 760 P.2d 1162, 1165-67 (Idaho 1988) (a pen register was a search pursuant to the Idaho Constitution and required a warrant); State v. Hunt, 450 A.2d 952, 956-57 (N.J. 1982) (the New Jersey Constitution affords individuals the right to privacy in their toll billing records and, by implication, pen register records); Commonwealth v. Beauford, 475 A.2d 783, 791 (Pa. Super. 1984) (holding that individuals have a reasonable expectation of privacy in the telephone numbers one dials and the Pennsylvania Constitution protects individuals against the installation of pen registers without a demonstration of probable cause); State v. Gunwall, 720 P.2d 808, 813 (Wash. 1986) (en banc) (holding that the Washington Constitution barred the use of a pen register without a search warrant); *see also* Richardson v. State, 865 S.W.2d 944, 953 (Tex. Crim. App. 1993) (en banc) (holding that a pen register may be a search pursuant to the Texas Constitution).

345 313 P.3d 732 (Idaho Ct. App. 2013).

346 *Id.* at 738 (discussing *Thompson*, 760 P.2d at 1165).

347 *Id.*

348 Kelly, *supra* note 3.

349 *See* Owsley, *supra* note 15, at 46.

350 Freiwald, *supra* note 93, at 999-1000; *see* Bellia, *supra* note 82, at 1382 ("Because application of the Fourth Amendment is in doubt, the statutory rules for acquisition of communications are all the more important. Those provisions, however, reflect significant gaps and ambiguities.").

351 *See* Bellia, *supra* note 82, at 1458 (noting that Congress "could not have anticipated that technological developments would place so many electronic communications in the hands of third parties" when the ECPA was enacted); Orin Kerr, *A User's Guide to the Stored Communications Act and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004) (addressing areas of potential reform); Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L REV. 1557, 1559 (2004) (explaining that the statute "has failed to keep pace with changes in and on the Internet and therefore no longer provides appropriate privacy protections").

352 Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, 4 (2007).

353 Arcila, *supra* note 258, at 49.

354 *See* 18 U.S.C. §2708 (2013); *see also* Freiwald, *supra* note 352, at 4.

66 HSTLJ 183

End of Document

© 2015 Thomson Reuters. No claim to original U.S. Government Works.