Oklahoma Law Review

Volume 66 | Number 4

2014

Light in the Darkness: How the LEATPR Standards Guide Legislators in Regulating Law Enforcement Access to Cell Site Location Records

Susan Freiwald
University of San Francisco, freiwald@usfca.edu

LIGHT IN THE DARKNESS: HOW THE LEATPR STANDARDS GUIDE LEGISLATORS IN REGULATING LAW ENFORCEMENT ACCESS TO CELL SITE LOCATION RECORDS

SUSAN FREIWALD*

Introduction

The new ABA Standards for Criminal Justice: Law Enforcement Access to Third Party Records (LEATPR Standards) set out a worthy goal. They endeavor to "provide the framework for legislatures . . . to carry out th[e] critical task" of "establishing the appropriate level of protection" for those records held by institutional third parties to which law enforcement seeks access during criminal investigations.[1] This article measures the Standards' success by assessing the guidance they provide legislators[2] interested in updating pertinent law regarding one specific type of data. Scholars should not expect the Standards to yield the same conclusions they would have furnished had they been able to draft a set of standards by themselves.[3] The

* Susan Freiwald, Professor of Law, University of San Francisco School of Law. I thank research librarian John Shafer, my research assistant Everett Monroe, and my editors at the *Oklahoma Law Review* for their valuable help. I also thank the following people for their helpful feedback on drafts and the symposium presentation: Catherine Crump, Jim Dempsey, Hanni Fakhoury, Andrew Ferguson, David Gray, Stephen Henderson, Mark Jaycox, Stephanie Pell, Christopher Slobogin, and special thanks to Judge Stephen Smith. All views, and any errors, are entirely my own.

1. ABA STANDARDS FOR CRIMINAL JUSTICE: LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS 16 (2013) [hereinafter LEATPR STANDARDS]; *see also id.* at 2 ("[B]ecause the federal constitutional regulation has historically been slight, and because other regulation has occurred in an *ad hoc* manner, there is no existing framework via which legislatures . . . can make the difficult decisions regarding what records should be protected and the scope of such protection."). This article will refer to individual standards using the format 'STANDARD x.x.'

2. Although the Standards purport to offer guidance to agencies and courts acting in their supervisory capacity as well, *see id.*, this article will focus only on the guidance they offer to legislatures.

3. Because they reflect the collective wisdom of a panel of experts holding a spectrum of perspectives, the Standards should carry more presumptive weight than a scholarly article written by one or two people. Although jointly authored works usually reflect shared perspectives, a recent article deserves special attention because of its authors' different backgrounds, as well as its significant contributions. *See* 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)

Standards emerged after years of painstaking consensus building and compromise[4]—no individual committee member got entirely what he wanted.[5] Nonetheless, not every product of a committee turns out to have been worth the effort, which is why this article assesses the Standards' value.

This article measures the Standards' contribution by looking at the light they shed on the regulation of one particular investigative method, the legality of which could not be more in need of illumination: law enforcement's compelled disclosure of cell phone records that reveal customers'[6] locations. Over the past decade, a body of case law has addressed the procedural hurdle law enforcement agents must overcome to compel cell phone service providers (providers) to disclose records that indicate the cell towers or sites that a cell phone user's phone has used to communicate.[7] While agents can obtain such cell tower data (location data) in real-time, including as the cell phone user moves from place to place,[8]

(recommending statutory language for law enforcement access to cell site location information).

4. *See* LEATPR STANDARDS, *supra* note 1, at 1-2 (describing a three-year drafting process and two-year revision process before approval); Stephen E. Henderson, *Real-Time and Historic Location Surveillance After* United States v. Jones*: An Administrable, Mildly Mosaic Approach*, 103 J. CRIM. L. & CRIMINOLOGY 803, 810 (2013) ("The ABA process is appropriately thorough and rigorous, consisting of several stages at which all interested parties have a voice."); *see also id.* at 836 (describing further the ABA process).

5. At the live symposium at which I presented an early version of this article, some committee members expressed displeasure with some of the compromises made and provisions they specifically opposed that were nonetheless included. Because the Standards generating process mirrors the legislative process more than the scholarly process, academics should refrain from judging the Standards as they would a scholarly piece.

6. The records disclosed are not always customer records. *See infra* Part I.C (discussing questions about what constitutes a "record" under federal statutory law).

7. *See generally* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681 (2011) (describing recent cases); Pell & Soghoian, *supra* note 3 (same); *see also In re* Application of the United States for Historical Cell Site Data, 747 F. Supp. 2d 827, 830-36 (S.D. Tex. 2010), *vacated*, 724 F.3d 600 (5th Cir. 2013) (describing developments in cell phone tracking technology in detailed fact finding).

8. *See* Pell & Soghoian, *supra* note 3, at 134-41 (discussing legal backdrop for prospective or real-time location data acquisition); *see also* Adam Koppel, *Warranting a Warrant: Fourth Amendment Concerns Raised by Law Enforcement's Warrantless Use of GPS and Cellular Phone Tracking*, 64 U. MIAMI L. REV. 1061, 1081 n.160 (2010) (collecting cases); Steven B. Toeniskoetter, *Preventing a Modern Panopticon: Law Enforcement Acquisition of Real-Time Cellular Tracking Data*, RICH. J.L. & TECH., Summer 2007, at 16, 24, 29 (same).

this article focuses on law enforcement's acquisition of records stored with the provider that contain such location data (location records), so as to stay within the Standards' ambit.[9]

Any member of Congress[10] interested in the regulation of law enforcement access to location records stored by providers would first determine whether the current law requires updating. As Part I elaborates, the existing federal statutory treatment of the compelled disclosure of location records suffers from an extreme lack of clarity.

The relevant statute is the Stored Communications Act (SCA).[11] Congress passed the SCA in 1986 as part of the Electronic Communications Privacy Act,[12] when the cell phone industry was in its infancy.[13] The SCA does not expressly mention location records. It does not even resolve the threshold question of what counts as a record.[14] In the intervening twenty-eight years, Congress has not meaningfully updated the SCA's records access provisions, let alone clarified whether they apply to location records.[15] Even when courts have determined or assumed that the SCA does pertain, they have found the statute to be unclear about exactly what procedural hurdles it requires before law enforcement agents may compel access to location records, and they have thus reached quite different conclusions.[16] Surely location records require the "greater consistency" the

---

9. The distinction between historical records of location data and real-time access to location data is not straightforward. *See infra* Part I.C.

10. For brevity's sake, I discuss only how a member of Congress would approach the task of updating federal statutory law for law enforcement's compelled disclosure of location records. Current federal statutory surveillance law sets a floor for legislation by the states. *See* United States v. McKinnon, 721 F.2d 19, 21 n.1 (1st Cir. 1983).

11. Title II, § 201, Pub. L. No. 99-508, 100 Stat. 1860 (1986) (codified as amended at 18 U.S.C. §§ 2701-2711 (2012)). In addressing the compelled disclosure of location records, most judges have applied the SCA, but some have questioned whether the SCA even covers location data. *See infra* Part I.A.

12. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

13. *See infra* Part I.C.

14. *Id.*

15. Congress did raise the standard for access to non-content records from a relevance standard to an intermediate, less than probable cause standard in 1994. Communications Assistance for Law Enforcement Act, Title I, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended at 47 U.S.C. §§ 1001-1010). At that time, the director of the FBI indicated that the new law was making no change in how existing law regulated access to location records, but he did not specify that regulation. *In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 762-63 (S.D. Tex. 2005) [hereinafter S. Dist. Tex. Decision].

16. *See infra* Part I.B.

Standards' drafters describe as necessary for existing law.[17] Courts and commentators have called upon Congress to act.[18]

Assuming that interested members of Congress recognize the need to address the compelled disclosure of location records, they would likely turn to the federal appellate courts' interpretation of the Fourth Amendment to ensure that any legislation they draft satisfies constitutional requirements.[19] To explore whether congressional drafters would benefit, in addition, from consulting the Standards, Part II describes the two federal appellate cases that have addressed how the Fourth Amendment regulates the compelled disclosure of location records.[20] Rather than clearly direct federal legislators on how to draft constitutionally compliant regulations,[21] the federal appellate courts have issued divided opinions that clash concerning core constitutional questions. In the last three years, the Fifth and Third Circuits have reached opposite conclusions about whether the third party rule precludes claims by cell phone users to a Fourth Amendment interest in their location records.[22] In addition, neither appellate decision resolved whether cell phone users entertain reasonable expectations of privacy in their location data.[23] As Part II explains, both decisions effectively left that issue for magistrate judges to resolve, a delegation of responsibility that

17. LEATPR STANDARDS, *supra* note 1, at 5; *see also infra* text accompanying note 29.

18. *See, e.g.,* United States v. Cuevas-Perez, 640 F.3d 272, 294 (7th Cir. 2011) (Wood, J., dissenting), *vacated*, 132 S. Ct. 1534 (2012); *The Geolocational Privacy and Surveillance Act: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary*, 112th Cong. 7-9 (2012) (statement of Catherine Crump, Staff Attorney, American Civil Liberties Union) [hereinafter Crump Statement] (pressing Congress to regulate location data access to clarify and strengthen restrictions in the face of disparate practices and insufficient privacy protections across all levels of law enforcement); Pell & Soghoian, *supra* note 3, at 124, 133, 150 (calling the need for federal legislation "urgent" and "critical").

19. A few members of Congress have recognized the need. *See* S. 639, 113th Cong. (as introduced Mar. 21, 2013) (requiring a warrant to collect geolocation information, including cell site location data); H.R. 983, 113th Cong. (as introduced Mar. 6, 2013) (similar).

20. *In re* Application of U.S. for Historical Cell-Site Data, 724 F.3d 600 (5th Cir. 2013) [hereinafter Fifth Cir. Decision]; *In re* Application of U.S. for an Order Directing a Provider of Elec. Commc'ns Serv. to Disclose Records to Gov't, 620 F.3d 304 (3d Cir. 2010) [hereinafter Third Cir. Decision].

21. State legislators will, of course, be interested in federal constitutional law as well. A few states have begun, or attempted to begin, the process of updating their laws to address law enforcement access to location records. *See, e.g.*, S. 1052, 2013 Leg., 83d Reg. Sess. (Tex. 2013); S. 1434, 2011-2012 Leg., Reg. Sess. (Cal. 2012) (vetoed by Governor on Sept. 30, 2012).

22. *See infra* Part II.A.

23. *See infra* Part II.B.

lower court judges likely view as unwelcome.[24] Moreover, both decisions failed to define clearly what counts as a location record, which remains a glaring omission in the law.

With applicable statutory law confusing and constitutional law inconsistent and incomplete, even minimal guidance would be valuable to legislators. But the Standards provide much more than minimal guidance. Part III describes the Standards' significant contributions to a hypothetical legislative process in which legislators supplement the understanding of the law they derive from reading federal appellate and even lower court cases by consulting the Standards. For example, neither the SCA nor current interpretations of Fourth Amendment law directs courts to appreciate fully the personal nature of location information and the way in which records are created. Because the Standards draw on a wider body of law than Fourth Amendment principles, they offer a richer set of factors for legislators to consider. Part III also discusses how the Standards' text and commentary remind legislators of the narrow scope of the third party doctrine that has so occupied the federal appellate courts. In particular, the Standards emphasize that users waive privacy interests only when they actually voluntarily divulge their information to third parties, and even then only when those third parties in turn voluntarily divulge that information to law enforcement.[25] That scenario rarely applies in the context in which law enforcement access to location data arises. Finally, the Standards explicitly recommend additional procedural protections, such as notice, that the SCA does not currently provide and that courts engaged in constitutional analysis have so far neglected to discuss.[26]

The article concludes that the Standards offer significant insights to legislators interested in updating the law to address location records.

---

24. Stephen Wm. Smith, *Standing Up for Mr. Nesbitt*, 47 U.S.F. L. REV. 257, 262 (2012) ("So despite a pressing need for appellate court guidance to magistrate judges deluged with [ECPA] requests on a daily basis, almost none has been given."). I have argued that courts avoid engaging in necessary Fourth Amendment analysis of new communications technologies by engaging in short cuts, like the third party rule, because the constitutional inquiry requires a normative judgment that makes judges uncomfortable. *See* Susan Freiwald, *First Principles of Communications Privacy*, STAN. TECH. L. REV., June 2007, at 3, ¶¶ 36-49 [hereinafter Freiwald, *First Principles*]; *see also* Susan Freiwald, *The* Davis *Good Faith Rule and Getting Answers to the Questions* Jones *Left Open*, 14 N.C. J. L. & TECH. 341 (2013) [hereinafter Freiwald, *Good Faith Rule*] (describing how lower courts have avoided constitutional analysis in the wake of the *United States v. Jones* decision by denying the exclusionary remedy).

25. *See infra* Part III.C.

26. *See infra* Part III.B.

Because the law applicable to location records could not be more muddled and the guidance provided by the appellate decisions today could not be less complete, the Standards have come at just the right time.[27]

I. Federal Statutory Law on Location Records Cries Out for Clarification

The Standards' drafters recognize that technology and practices have far outstripped current law regarding law enforcement access to third party records.[28] They also suggest that current law pertaining to location records represents a particularly worthy candidate for reform. According to the Standards' commentary, "application of the federal statutory law is . . . uncertain as it requires application of several unclear statutes."[29]

Under federal law, the SCA provides different procedural hurdles for different surveillance practices and establishes a sliding scale framework under which law enforcement may obtain apparently less private information more easily, while access to more private information faces a higher hurdle.[30] The SCA requires law enforcement agents to make a showing of probable cause and obtain a warrant to acquire the most private information, such as the content of voicemails and emails.[31] However, to acquire "record[s] or other information pertaining to a subscriber to or customer" other than content,[32] law enforcement agents may make a lesser

---

27. *See, e.g.*, *In re* Application of U.S. for an Order Authorizing Disclosure of Historical Cell Site Information for Telephone Number [Redacted], No. 14-286 (JMF), 2014 WL 1395082, at *1 (D.D.C. Apr. 17, 2014) [hereinafter D.C. Decision] (having "reviewed approximately eighty-seven opinions that are publicly available on Westlaw and that substantively address the legal issues surrounding [cell site location information]," the court found that "these decisions are impossible to reconcile").

28. *See* LEATPR STANDARDS, *supra* note 1, at 2, 5.

29. *See* STANDARD 25-4.1(d); *see also In re* Application of U.S. for an Order Authorizing the Disclosure of Cell Site Location Info., No. 6:08-6038M-REW, 2009 WL 8231744, at *2 (E.D. Ky. Apr. 17, 2009) [hereinafter London Decision] (noting that "Congress has not directly spoken on the issue of [cell site location information] availability under the statutory melange presented," which establishes "the need for clarification from lawmakers"); Henderson, *supra* note 4, at 818 ("The federal statutory law regarding law enforcement access to third-party location information is a mess . . . .").

30. COMPUTER CRIME & INTELLECTUAL PROP. SECTION, DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 115-16 (3d. ed. 2009), *available at* http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf.

31. 18 U.S.C. § 2703(a) (2012). In a series of complicated distinctions beyond the scope of this article, however, the statute allows access to some content without a warrant. *Id*. § 2703(b).

32. *Id*. § 2703(c).

showing under 18 U.S.C. § 2703(d) (known as a D order).[33] Congress designed the D order standard to be less burdensome to satisfy than the probable cause standard, but harder to meet than a mere relevance standard.[34] The question is whether law enforcement agents may use a D order to obtain stored location information.

While location data has no doubt proven useful in criminal investigations,[35] its acquisition strongly implicates privacy concerns.[36] In recognition of the latter and as a matter of state law, the highest courts of New Jersey and Massachusetts have now required agents to obtain a warrant based on probable cause before they may compel providers to divulge location records.[37] Both decisions grounded their reasoning in their state constitutions, each of which reaches further to protect privacy than the Fourth Amendment.[38] Both decisions vividly described the privacy interests in stored location records. For example, the New Jersey Supreme Court recognized that "[w]ith increasing accuracy, cell phones can now trace our daily movements and disclose not only where individuals are located at a point in time but also which shops, doctors, religious services, and political events they go to, and with whom they choose to associate."[39] According to the Massachusetts Supreme Judicial Court, "Even [location information] limited to the cell site locations of telephone calls made and received may yield a treasure trove of very detailed and extensive

---

33. *Id.* § 2703(d). Agents may apply under different provisions if they combine their request for location records with requests for other information. COMPUTER CRIME & INTELLECTUAL PROP. SECTION, *supra* note 30, at 127.

34. H.R. REP. NO. 103-827, at 31-32 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3511-12.

35. *See* Crump Statement, *supra* note 18, at 4-6; Freiwald, *supra* note 7, at 702-26; Pell & Soghoian, *supra* note 3, at 120-21.

36. *See* Pell & Soghoian, *supra* note 3, at 163-74 (cataloguing and assessing ways that judges describe the privacy and autonomy harms from government acquisition of location data).

37. Commonwealth v. Augustine, 467 Mass. 230, 255 (Mass. 2014) (finding a reasonable expectation of privacy in cell-phone location information); State v. Earls, 70 A.3d 630, 643 (N.J. 2013) (same).

38. *See Augustine*, 467 Mass. at 244 (recognizing that the Massachusetts Constitution provides more protection of third party records than the Constitution); *Earls*, 70 A.3d at 632 ("Historically, the State Constitution has offered greater protection to New Jersey residents than the Fourth Amendment."); *see also id.* at 642 (explaining that New Jersey rejects the third party rule).

39. *Earls*, 70 A.3d at 632; *see also id.* at 642 ("[D]etails about the location of a cell phone can provide an intimate picture of one's daily life."); *Augustine*, 467 Mass. at 248 (approving of and quoting from *Earls*).

information about the individual's 'comings and goings' in both public and private places."[40] At the same time, state legislatures have recognized the threat to privacy and either passed or proposed state laws to require warrants for access to stored location data.[41] Despite an emerging trend towards a warrant requirement for location data under state law,[42] many magistrate judges have approved D orders for the compelled disclosure of location records, on both statutory and constitutional grounds.[43]

In several recent cases, however, magistrate judges have rejected applications requesting D orders for location records, holding that agents needed to make a showing of probable cause.[44] The government appealed two such cases; it appealed one from the Western District of Pennsylvania[45] (Pittsburgh Decision) to the Third Circuit and one from the Southern District of Texas[46] (Houston Decision) to the Fifth Circuit.[47] The decisions of the magistrates and of the appellate courts highlight the difficulties of interpretation that the SCA poses.

The Pittsburgh Decision raised significant questions about the SCA's coverage. In particular, Magistrate Judge Lenihan, who authored the Pittsburgh Decision, questioned whether § 2703(c), the SCA's records

40. *See Augustine*, 467 Mass. at 251 (finding it significant that location information covering a span of two weeks apparently took up at least sixty-four pages of material).

41. *See supra* note 21; *see also* Hanni Fakhoury, *New Massachusetts Decision Requires a Warrant for Cell Tracking*, ELEC. FRONTIER FOUND. (Feb. 19, 2014), https://www.eff.org/deeplinks/2014/02/massachusetts-requires-warrants-cell-tracking (describing pending state bills to require warrants for location records).

42. *See* Fakhoury, *supra* note 41.

43. *See, e.g.*, United States v. Ruby, No. 12CR1073 WQH, 2013 WL 544888, at *4-*6 (S.D. Cal. Feb. 12, 2013); United States v. Graham, 846 F. Supp. 2d 384, at 405-06 (D. Md. 2012); United States v. Gordon, No. 09-153-02 (RMU), 2012 WL 8499876, at *2 (D.D.C. Feb. 6, 2012); United States v. Suarez-Blanca, No. 1:07-CR-0023-MHS/AJB, 2008 WL 4200156 (N.D. Ga Apr. 21, 2008); *see also* Pell & Soghoian, *supra* note 3, at 143 ("Lower courts have, for the most part, accepted the government's use of a D Order to compel historical cell site information.").

44. *See infra* Part II.C.

45. *In re* Application of 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, 586 n.7 (W.D. Pa. 2008) [hereinafter Pittsburgh Decision], *vacated*, Third Cir. Decision, *supra* note 20.

46. *In re* Application of U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 846 (S.D. Tex. 2010) [hereinafter Houston Decision] (finding warrantless acquisition of historical cell site location information to violate the Fourth Amendment), *vacated*, Fifth Cir. Decision, *supra* note 20.

47. In each case, the district court affirmed the Magistrate Judge decision with little to no analysis. Fifth Cir. Decision, *supra* note 20, at 606 n.6; Third Cir. Decision, *supra* note 20, at 306 n.1.

provision, includes location records.[48] Both decisions also questioned whether a D Order furnished the appropriate legal hurdle for law enforcement agents to overcome before they may compel the disclosure of location records,[49] which is a question that the appellate courts did not clearly resolve. Finally, both decisions raised a troubling and persistent question: Must the information in a location record already be stored at the time the government requests it?

A. Does § 2703(c) Cover Location Records?

As mentioned, the SCA provides greater protection for the content of communications than for non-content information. The distinction derives from the 1979 case of *Smith v. Maryland* in which the Supreme Court found no Fourth Amendment interest implicated when law enforcement agents determined the numbers a target had dialed on his telephone.[50] It would have been a clear Fourth Amendment violation to obtain the content of his phone call without obtaining a court order based on probable cause and other requirements.[51] One could argue that, because data about the locations one has been indicates so much information about one's life, courts should view it as content data under the SCA.[52]

No courts have pursued that line of interpretation, however, so it remains a stretch. Currently, if the SCA applies, then location information would count as non-content information, and records of it would be available, if at all, under § 2703(c). Most courts to address the issue have assumed that § 2703(c) covers location records.[53]

In contrast, the Pittsburgh Decision found that § 2703(c) did not even pertain to location records.[54] In her decision, which all of the other

48. Pittsburgh Decision, *supra* note 45, at 604-07.

49. Houston Decision, *supra* note 46, at 845-46; Pittsburgh Decision, *supra* note 45, at 608-09.

50. 442 U.S. 735, 745 (1979).

51. *See id.* at 739, 743 (citing Katz v. United States, 389 U.S. 347 (1967)).

52. *See* Freiwald, *supra* note 7, at 742 (discussing constitutional protection of location data and recognizing that courts sometimes characterize data as "content" after they determine that it requires protection, rather than determining protection based on a prior characterization).

53. *See* D.C. Decision, *supra* note 27, at *2 (discussing the issue); Houston Decision, *supra* note 46, at 830 n.6 (collecting cases).

54. *See* Pittsburgh Decision, *supra* note 45, at 601-07.

magistrate judges in the district joined,[55] Magistrate Judge Lenihan described location records as information that a "tracking device" creates.[56] Congress defined mobile tracking devices broadly to include "an electronic or mechanical device which permits the tracking of the movement of a person or object."[57] It makes sense to view a cell phone as a tracking device when it creates a record of its user's movements from place to place, as cell phones do when they generate location records.[58] But the applicable definition of electronic communications explicitly excludes communications from a tracking device.[59] In the Pittsburgh Decision, Magistrate Judge Lenihan reasoned that the tracking device exclusion from the definition of electronic communication necessarily meant that stored tracking device information should be excluded from the scope of records pertaining to an electronic communication service.[60] On appeal, the Third Circuit rejected Judge Lenihan's analysis; both the government and the amici who addressed the statutory issues agreed that § 2703(c) covered location records.[61]

Although the legislative history has little to say about cell phones, and nothing to say about location data, it does establish that "the information involved is information about the customer's use of the service."[62] In another decision, Judge Smith, the author of the Houston opinion, squarely rejected the idea that *prospective* location data could be covered as a record under § 2703(c). Judge Smith reasoned that prospective cell site data

---

55. *See* Third Cir. Decision, *supra* note 20, at 308 ("This is unique in the author's experience of more than three decades on this court and demonstrates the impressive level of support Magistrate Judge Lenihan's opinion has among her colleagues . . . .").

56. Pittsburgh Decision, *supra* note 45, at 589, 601-07.

57. 18 U.S.C. § 3117(b) (2012). Unfortunately, this provision does not indicate the procedures law enforcement agents must follow to obtain records created by tracking devices.

58. Pittsburgh Decision, *supra* note 45, at 602 ("[I]t is, therefore, extremely difficult to see how a cell phone is not now *precisely* [a tracking device].").

59. 18 U.S.C. § 2510(12)(c) (2012).

60. Pittsburgh Decision, *supra* note 45, at 604; *see also In re* Application of U.S. for an Order Authorizing Use of a Pen Register with Caller Identification Device Cell Site Location Auth. on a Cellular Tel., 2009 WL 159187, at *3, *5 (S.D.N.Y. Jan. 13, 2009) (coming to the same conclusion).

61. *See* Third Cir. Decision, *supra* note 20, at 307-08 ("[T]here is no dispute that historical [location data] . . . falls within the scope of § 2703(c)(1)."); *see also id.* at 310 (finding it irrelevant that location data may be information from a tracking device because it derives from a wire communication).

62. S. Dist. Tex. Decision, *supra* note 15, at 758 (citing S. REP. NO. 99-541, at 38 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3592).

appears to be unrelated to any *customer* (as opposed to law enforcement) use of the provider's services because subscribers do not use the phone to track their own movements in real time.[63] Judge Smith went on to suggest that historical location information could count because "[c]ell phone companies might legitimately compile such data for customized marketing and billing purposes."[64] That analysis raises the question of whether location data compiled for law-enforcement use rather than related to customer use would fall outside the scope of § 2703(c). I return to that issue below.[65]

In a more recent decision, Magistrate Judge Facciola from the District of Columbia renewed the question by considering the different ways location data may be generated.[66] Judge Facciola explained that location data associated with a wire communication would not be subject to the tracking device exclusion applicable to electronic communications. On the other hand, if a provider gives location data to the government generated through "sending and receiving text messages, using applications like Facebook and Twitter, checking e-mails, or using the GPS function on the phone," then that information could fall outside the SCA's scope.[67]

In summary, as Magistrate Judge Lenihan did, a judge could construe location records to fall outside the coverage of § 2703(c). The judge could view location data as content information, as information from a tracking device and therefore not an electronic communication, or as information unrelated to a customer's use of a provider's services. Judge Lenihan assumed that if the SCA does not cover location records, the background rule of Fed. R. Crim. Pro. 41, requiring notice to the target (at some point) and a warrant based on probable cause, would apply to government demands for them.[68] That seems right, unless one can successfully establish

---

63. *Id.* at 759.

64. *Id.* at 759 n.16.

65. *See infra* text accompanying notes 162-77.

66. *See* D.C. Decision, *supra* note 27, at *2. See *infra* text accompanying notes 103-108 for a discussion of the different ways location data may be generated.

67. *See* D.C. Decision, *supra* note 27, at *2. Judge Facciola indicated that he could not decide on the government's applications without a better understanding of the provider's practices and the exact location information they would furnish to the government, which could well differ from the information the government requested. *Id.* at *3; *see also* Freiwald, *supra* note 7, at 716-20 (noting that the government has emphasized its narrow requests for location data but that providers' disclosures will reflect their costs and will not likely be circumscribed without a court order requiring that).

68. Pittsburgh Decision, *supra* note 45, at 607; *see also* Third Cir. Decision, *supra* note 20, at 309 (same).

that acquisition of location records raises no Fourth Amendment concerns.[69] As Part II argues, current federal appellate interpretations have made that question entirely opaque. Before turning to that question, I consider the debate over the procedural hurdle the SCA requires for records covered by § 2703(c).

B. Does a D Order Suffice for Access to Location Records Under the SCA?

By interpreting § 2703(c) in conflicting ways, courts have sown confusion for anyone trying to understand the law and given mixed direction to magistrate judges about how to rule on government applications. Section 2703(c) permits "governmental entit[ies]" to

> require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber of customer of such service (not including the contents of communications) only when the governmental entity —
>
> (A) obtains a warrant . . .
>
> (B) obtains a [D Order];
>
> (C) has the consent of the subscriber or customer to such disclosure;
>
> (D) [is investigating telemarketing fraud]; or
>
> (E) [seeks certain limited information not including location data].[70]

In cases not involving consent, the only available routes to obtain location data the provisions leave open are satisfaction of either the D order standard or the probable cause standard.[71] Which path magistrate judges

---

69. *Cf.* Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 69-74 (2004) (discussing how to treat government acquisition of online information, such as web browsing data and search terms, not clearly covered by the current statutory categories and disagreeing with Professor Orin Kerr that the presumption should be that such information lacks any protection (citing Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 645-47 (2003))). If one considered location data the product of a tracking device, one could require a warrant for installation of the tracking device, pursuant to 18 U.S.C. § 3117, as Magistrate Judge Lenihan suggested. *See* Pittsburgh Decision, *supra* note 45, at 613-14.

70. 18 U.S.C. § 2703(c)(1) (2012).

71. Provisions (D) and (E) do not apply to the investigations this Article considers.

may require agents to navigate turns out to be subject to significant disagreement.

1. Require a Warrant

Judge Dennis, the dissenting judge on the Fifth Circuit panel that decided the appeal from the Houston Decision, interpreted the SCA in a way that would have been straightforward and easy to apply. Judge Dennis viewed the SCA as ambiguous, but would have held 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."[72] Judge Dennis found the warrant procedure appropriate under the principle of constitutional avoidance, because "non-consensual, warrantless compulsion of cell site location records raises serious and debatable constitutional questions," which courts could avoid by requiring a warrant.[73] Though Judge Dennis' opinion discussed at length how law enforcement's access to location records could impinge on users' privacy interests,[74] he emphasized that he based his holding on statutory interpretation.[75] Were that holding the law, magistrate judges would know to require a warrant whenever law enforcement agents sought to acquire any location data from a provider. As a dissent, however, it does not bind lower courts.

2. Require a D Order

Executive branch litigators have consistently advocated that magistrate judges must grant orders to compel providers to disclose location records whenever law enforcement agents make the statutory showing for D orders.[76] To obtain a D order, an agent must submit an application that "offers specific and articulable facts showing that there are reasonable grounds to believe that the . . . information sought [is] relevant and material to an ongoing criminal investigation."[77] As mentioned above, the D order standard is easier to meet than probable cause, which courts generally interpret to require "a showing of a fair probability of evidence of criminal

72. Fifth Cir. Decision, *supra* note 20, at 630 (Dennis, J., dissenting).

73. *Id.* at 632 (Dennis, J., dissenting).

74. *Id.* at 622-24. See *infra* Part II for a discussion of the appellate courts' constitutional analysis.

75. Fifth Cir. Decision, *supra* note 20, at 617 (Dennis, J., dissenting) ("I would affirm on statutory grounds the order denying the government's [D Order] application with respect to historical cell site location data.").

76. *See, e.g.*, Third Cir. Decision, *supra* note 20, at 315.

77. 18 U.S.C. § 2703(d) (2012).

activity."[78] As the next Part will discuss, if users have a Fourth Amendment interest that law enforcement agents intrude upon when they compel the disclosure of location records, then a D order alone does not satisfy the Fourth Amendment, but a warrant based on probable cause likely would.[79]

The government has often succeeded in promoting its view in the lower courts. Several magistrate judges have written opinions agreeing that a D order showing suffices for government access to location records.[80] In each case, these courts have found that the government does not intrude on users' Fourth Amendment interests when it compels the disclosure of location records, so Congress is free to legislate whatever requirements it chooses.[81] Then, as a matter of statutory interpretation, these courts have accepted the government's position that Congress has directed magistrate judges to grant D orders compelling location records disclosure whenever agents meet the statutory showing and never to require more.[82] While this approach also offers a clear path for lower court judges, albeit one that is less protective of privacy, it has not yet received an imprimatur from an appellate court.[83]

---

78. Pittsburgh Decision, *supra* note 45, at 585 n.1; *see generally* Freiwald, *supra* note 7, at 696-98 (discussing the practical differences between the two standards, including that the D order showing permits access to information about people who are not themselves suspected of crimes).

79. *See infra* Part II. Notice to the target may be required as well. *See In re* Application of U.S. for & [sic] Order: (1) Authorizing Use of a Pen Register & Trap & Trace Device; (2) Authorizing Release of Subscriber & Other Info.; & (3) Authorizing Disclosure of Location-Based Servs., 727 F. Supp. 2d 571, 580-81 (W.D. Tex. 2010) (explaining that Rule 41 is not satisfied if the government fails to provide notice to the target (citing FED. R. CRIM. P. 41(f)(2)(C))).

80. *See supra* note 43. A few district courts have even reversed magistrate judges who required a probable cause showing. *See In re* Application of U.S. for an Order: (1) Authorizing Installation & Use of a Pen Register & Trap & Trace Device, & (2) Authorizing Release of Subscriber & Other Info., 622 F. Supp. 2d 411 (S.D. Tex. 2007); *In re* Applications of U.S. for an Order Pursuant to Title 18, U.S. Code, Section 2703(d), 509 F. Supp. 2d 76 (D. Mass. 2007).

81. *See, e.g.*, United States v. Benford, No. 2:09 CR 86, 2010 WL 1266507, at *3 (N.D. Ind. Mar. 26, 2010).

82. *See, e.g.*, *In re* Application of U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), 830 F. Supp. 2d 114, 147-48 (E.D. Va. 2011).

83. One appellate court has affirmed that location data does not impinge on Fourth Amendment privacy interests, but did not address compelled disclosure to records because the case concerned real time access to location information. United States v. Skinner, 690 F.3d 772, 779 (6th Cir. 2012).

The Fifth Circuit and Third Circuit accepted neither straightforward view of the statute. As the next two subsections describe, the Third Circuit adopts a complicated balancing scheme that leaves magistrate judges largely in the dark about how to proceed. The Fifth Circuit's approach covers a small subset of location data and gives little direction about the vast amount of data it leaves unaddressed. Surely lower courts could use an update to the law to light the way forward.

3. Permit Magistrate Judges to Choose to Require a Warrant

According to the Third Circuit majority, a showing under the D order standard provides a necessary but not sufficient condition for the granting of an order to compel the disclosure of location records.[84] The majority based the statutory construction argument on the text of § 2703(d), which contains the following language:

> 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 . . . are relevant and material to an ongoing criminal investigation.[85]

Because Congress used the phrase "only if" instead of "if" before the specific and articulable facts language, and because Congress indicated that courts "may" issue D orders instead of "shall" issue such orders, the Third Circuit held that "the statute as presently written gives [magistrate judges] the option to require a warrant showing probable cause" before granting an order to compel the disclosure of location records.[86] The opinion cautioned that magistrate judges should exercise the option to require a warrant "sparingly" because, while Congress explicitly included the D order option, the court derived the warrant option from Congress' failure to explicitly say that it was not available.[87]

The Third Circuit majority gave magistrate judges, including Judge Lenihan, who had authored the Pittsburgh Decision, precious little guidance on how to choose which standard to impose. The opinion devoted a few pages to considering the Fourth Amendment interests implicated by

84. Third Cir. Decision, *supra* note 20, at 316-20; *see also* Fifth Cir. Decision, *supra* note 20, at 606-07.

85. 18 U.S.C. § 2703(d) (2012).

86. Third Cir. Decision, *supra* note 20, at 319.

87. *Id.*

compelled disclosure of location records,[88] but came to no conclusions. The court did direct Judge Lenihan, if she decided to require a warrant on remand, to "make fact findings and give a full explanation that balances the Government's need (not merely desire) for the information with the privacy interests of cell phone users."[89] The Third Circuit majority imposed a significant burden on Judge Lenihan,[90] in particular, and on magistrate judges, in general. According to the Third Circuit, magistrate judges who receive D Orders for location records are to engage in a balancing process that neither Congress nor the appellate court was willing to undertake.[91]

Other appellate court judges have indicated significant concerns about according magistrate judges that much responsibility. Judge Tashima, the concurring judge on the Third Circuit panel, described the majority's approach as "vest[ing] magistrate judges with arbitrary and uncabined discretion to grant or deny issues of § 2703(d) orders at the whim of the magistrate."[92] In his amicus submission to the Fifth Circuit, Professor Orin Kerr argued that magistrate judges lack authority under Article III to issue the constitutional analysis that the Third Circuit opinion requires.[93]

---

88. *Id.* at 310-13; *see also infra* Part III.

89. Third Cir. Decision, *supra* note 20, at 319.

90. Judge Lenihan never got a chance to issue an opinion on remand because the government moved to withdraw its application almost one year after the Third Circuit Decision. Motion to Seal, *In re* Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, No. 2:07-mj-00524-TFM-LPL (W.D. Pa. July 28, 2011), ECF No. 39. Judge Lenihan granted the government's request to withdraw its application, but denied its request to do so under seal. *In re* Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, No. 2:07-mj-00524-TFM-LPL (W.D. Pa. Aug. 9, 2011).

91. Third Cir. Decision, *supra* note 20, at 319 ("[W]e are stymied by the failure of Congress to make its intention [regarding whether to require a warrant] clear."); *id.* at 320 (Tashima, J., concurring) (complaining that the majority's interpretation "provides *no* standards for the approval or disapproval for an application for an order under § 2703(d)").

92. *Id.* at 320 (Tashima, J., concurring).

93. Amicus Curiae Brief of Professor Orin S. Kerr in Support of the Appellant in Favor of Reversal, Fifth Cir. Decision, *supra* note 20 (No. 4:11-MC-00223), 2012 WL 10205105, at 12-16; *see also* Orin Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 VA. L. REV. 1241, 1260-77 (2010). *But see* Fifth Cir. Decision, *supra* note 20, at 604 n.4 (finding no constitutional problem because district courts review magistrate judges' opinions de novo); Smith, *supra* note 24, at 266 (countering that magistrate judges have to stand up to protect citizens' rights in the face of intrusive surveillance). For more on the Fifth Circuit's discussion of the procedural questions Professor Kerr posed in his amicus brief, see Recent Case, *Fourth Amendment-Warrantless Searches-Fifth Circuit Upholds Stored Communications Act's Nonwarrant Requirement for Cell-Site Data as Not Per Se*

If and when Congress heeds calls to update or revise how federal statutory law regulates law enforcement requests to compel the disclosure of location records,[94] it will look to the guidance appellate courts provide. Legislators will certainly pay attention to those courts' analysis of the applicable constitutional provisions. I turn to those analyses in Part II. First though, I consider how the Fifth Circuit's approach to the statutory question raised as many (or more) questions as it answered.

4. Require a D Order for a Small Subset of Data

The Fifth Circuit disagreed with the Third Circuit and interpreted § 2703(c) to require that courts grant applications for D Orders to obtain disclosure of location records whenever the government "meets the 'specific and articulable facts' standard."[95] At first glance, the decision's language appears consistent with the government's argument that magistrate judges have no discretion to deny such applications.[96]

But a closer look reveals that the Fifth Circuit's opinion, like the Third Circuit's, actually leaves considerable leeway to magistrate judges, with precious little guidance. It accomplished that by first narrowing the scope of its inquiry. At the outset, the Fifth Circuit read the lower court's opinion as concluding that the D order provision "was categorically unconstitutional with respect to an entire class of records [i.e., location records]."[97] The court then determined that "we are only asked to decide whether every instance of one particular factual circumstance—§ 2703(d) orders for historical cell site information—is unconstitutional."[98]

The Fifth Circuit's reading of the Houston Decision seems particularly uncharitable for what was effectively an as-applied challenge to the statute.[99] And, by strongly rejecting the idea that location data should be

---

Unconstitutional-In re Application of the United States for Historical Cell Cite Data*, 724 F.3d 600 (5th Cir. 2013)*, 127 HARV. L. REV. 1220, 1222 (2014).

94. *See, e.g.*, Fifth Cir. Decision, *supra* note 20, at 615 (recommending that cell phone users lobby their "elected representatives to enact statutory protections").

95. *Id.* at 607.

96. *See id.* ("[T]he court does not have the discretion to refuse to grant the order."); *id.* at 607 n.8 ("The text of the statute shows that Congress does not want magistrate judges second-guessing its calculus.").

97. *Id.* at 603-04.

98. *Id.* at 604.

99. It was as-applied in the sense that Judge Smith based his holding on the facts of the application before him, as well as extensive judicial fact finding about location data in general. *See* Houston Decision, *supra* note 46, at 831-35. It was not actually a challenge because, like all cases involving location records requests, it arose as a result of an *ex parte*

treated as a single category, the opinion raises important questions about how to further categorize location data for purposes of any future privacy statute. Most important at this point in the discussion, however, is that the Fifth Circuit disposed of the case by finding that a limited subset of the information the government sought could be obtained under the D order standard and by not addressing the rest.

The Fifth Circuit opined that D orders to obtain location records "for specified cell phones at the points at which the user places and terminates a call are not categorically unconstitutional."[100] The majority admitted that in some cases, law enforcement acquisition of even initiation and termination records that pertain only to the target's calls may implicate constitutional interests: "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."[101] In so holding, the Fifth Circuit reversed the lower court's decision on an extremely narrow ground, but gave little guidance as to when a D order would be sufficient to obtain historical records.

The majority opinion explicitly excluded from its coverage orders that request the following: location data pertaining to calls made by the recipient of calls from the target, location data about sites used during a call (duration data), location data about sites used when a phone is idle (idle state or registration data), and GPS data.[102] The decision did not explicitly exclude location data obtained when a cell phone receives calls, sends or receives a text message or otherwise accesses the internet, but its holding certainly did not cover it either.

---

application by the government. The district court's affirmance of Judge Smith's decision was more sweeping in scope. *See In re* Applications of U.S. for Historical Cell Site Data, No. 4:11-MC-00223, slip op. at *1 (S.D. Tex. Nov. 11, 2011) (holding, without further specification, that "data disclosing the location of the telephone at the time of particular calls may be acquired only by a warrant issue on probable cause" and that "[t]he standard under the [SCA D Order] is below that required by the Constitution").

100. Fifth Cir. Decision, *supra* note 20, at 615.

101. *Id.* at 604.

102. *Id.* at 615; *cf.* State v. Earls, 70 A.3d 630, 637 (2013) ("Cell phones can be tracked when they are used to make a call, send a text message, or connect to the Internet—or when they take no action at all, so long as the phone is not turned off.") (citing *ECPA Reform & the Revolution in Location Based Techs. & Servs.: Hearing Before the Subcomm. on the Const., Civil Rights, & Civil Liberties of the H. Comm. of the Judiciary*, 111th Cong. 13-14 (2010) (statement of Matt Blaze, Professor, Univ. of Pa.)).

All of the explicitly or implicitly excluded types of location data are capable of storage by providers and therefore susceptible to acquisition through compelled disclosure by law enforcement agents. For example, Judge Smith noted in the Houston Decision that the government's applications had specifically requested location data for the times when the target receives a call, as well as duration data and idle state (registration) data.[103] The government has applied for and apparently received such data in other cases.[104] The Third Circuit opinion noted that the application in the case at hand requested GPS data and that the DOJ's application template has a place to request GPS data when requesting location data.[105] One of the other cases that required probable cause for access to location data reported that the government's application had requested the location data recorded every time the target sent and received text messages.[106] As

103. Houston Decision, *supra* note 46, at 829 (quoting the applications to request "the cellsite/sector(s) used by the mobile telephone to obtain service for a call or when in an idle state"); *see also id.* ("In other words, the Government seeks continuous location data to track the target phone over a two month period, whether the phone was in active use or not."); Application at 3, Houston Decision, *supra* note 46 (No. 4:10-mj-00998) (seeking location data for the origin, termination, and, if reasonably available, during the duration of the call). Although the Fifth Circuit indicated that the government was willing to exclude idle state data from the scope of its applications, Fifth Cir. Decision, *supra* note 20, at 602 n.1, there is no record of its amending its application to do so. It may be that Judge Smith should refuse to grant any order the government resubmits if it continues to request duration or idle state data because that would exceed the scope of what the Fifth Circuit sanctioned.

104. *See, e.g.*, United States v. Benford, No. 2:09 CR 86, 2010 WL 1266507, at *1 (N.D. Ind. Mar. 26, 2010) (describing information sought as data "identifying which cell tower communicated with the cell phone while it was turned on"); London Decision, *supra* note 29, at *1 (quoting application as requesting "cell site activations at call origination for outbound calls, at call termination for incoming calls, and, if reasonably available, during both outbound and incoming calls"); Commonwealth v. Augustine, 467 Mass. 230, 239 (D. Mass. 2014) (noting that location information was associated with "calls made and received by the defendant's cellular telephone handset—including . . . unanswered calls—as well as the latitude and longitude of the cell sites to which those calls connected in order to conduct those calls"). The government has refused to disclose the actual location information it received, so it is difficult to know what was actually produced. *See, e.g.*, *id.* at 268 n.12 (describing how the Massachusetts Supreme Court gave up its request to review the sixty-four pages of location information at issue when the government objected to its disclosure).

105. Third Cir. Decision, *supra* note 20, at 311 (noting that the Government's sample application for a D Order for location records specifically requests GPS data and that, although the Government disclaimed interest in obtaining GPS data, "the Government does not argue that it cannot or will not request information from a GPS device through a § 2703(d) order").

106. *In re* Application of U.S. for an Order Authorizing Release of Historical Cell-Site Info., 736 F. Supp. 2d 578, 578 (E.D.N.Y. 2010) [hereinafter Brooklyn I Decision]; *see also*

mentioned above, Judge Facciola recently discussed the possibility that users generate location data by sending e-mail, surfing the web and using social media.[107] Technical experts have confirmed that mobile devices communicate with cell towers whenever they download data, and that carriers log such communications in databases.[108]

By concluding that it is not *per se* unacceptable for a court to require a provider to disclose the smallest subset of location data, the Fifth Circuit failed to guide magistrate judges about the great bulk of current and pending location data requests. The need for legislation could not be greater. While Congress is at it, it should also determine whether records must record only past information.

C. Location Records for Future Data?

The SCA's legislative history offers no guide to what Congress meant to include in § 2703(c). In 1986, when the SCA was passed, Congress was conscious of only the first developments in the cell phone industry.[109] There were hardly any cell towers at the time, and cell phones themselves were almost prohibitively expensive.[110] Since then, Americans have integrated cell phone use into their daily lives to an astonishing degree.[111] Yet, Congress has done nothing to clarify the standards applicable to government acquisition of location data.[112]

The Fifth Circuit litigation revealed that the government does not view location records as containing solely historical information. In its applications to Judge Smith, the government requested that the targeted

---

In re Application of U.S. for an Order Authorizing Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 114 (E.D.N.Y. 2011) [hereinafter Brooklyn II Decision] (ruling on a resubmission of the application by the government for the same information).

107. *See* D.C. Decision, *supra* note 27, at *3.

108. *See supra* note 102; *see also* Pell & Soghoian, *supra* note 3, at 128.

109. S. REP. NO. 99-541, at 1-2 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3556.

110. *See* CTIA—THE WIRELESS ASS'N, SEMI-ANNUAL WIRELESS INDUSTRY SURVEY 2 (2013), *available at* http://files.ctia.org/pdf/CTIA_Survey_YE_2012_Graphics-FINAL.pdf (reporting 1,531 cell sites in June of 1986, compared to 301,779 in 2012); Frank Vizard, *Phones on a Roll*, POPULAR MECHANICS, Jan. 1986, at 95, 95 (describing the cost of car model cell phones as ranging from $1000 to $3000).

111. Klayman v. Obama, 957 F. Supp. 2d 1, 34-36 (D.D.C. 2013) (documenting tremendous growth in the cell phone industry over the last decade and the changes in the way we use mobile phones).

112. *See* Fifth Cir. Decision, *supra* note 20, at 628 n.11 (citing H.R. REP. NO. 106-932, at 17 (2000)) (acknowledging a continued lack of clear legal standards for government collection of location data).

providers deliver records covering the past sixty days of location data.[113] In addition, the government asked for an order that required the providers to collect and store location information in the future, and to forward those newly created records, upon receipt and storage, to the requesting law enforcement agency on an ongoing basis.[114] In one application in particular, the applying agent asked for such future-created records under the sole authority of § 2703(c),[115] which covers only "a record or other information pertaining to a subscriber to or customer of [an electronic communication service]."[116]

Reviewing courts have rejected the idea that § 2703(c) may be used to obtain prospective location information.[117] They have found that location records, which provide "historical" location information, must be in the provider's possession at the time the order is made.[118] That interpretation accords with the consensus among academics, that the SCA covers "retrospective surveillance" only.[119] It also appeals to common sense: when one obtains a record of something in storage, that item should *already* be recorded in storage. The Privacy and Civil Liberties Oversight Board came to the same conclusion when it interpreted a statute permitting access to telephone calling "records" to require those records to exist at the time the

113. *See, e.g.*, Application at 2, Fifth Cir. Decision, *supra* note 20 (No. 4:10-mj-00981).

114. Brief of Amicus Curiae Susan Freiwald in Support of Affirmance, Fifth Cir. Decision, *supra* note 20 (No. 11-20884), 2012 WL 10205104, at 5-7 [hereinafter Freiwald Brief].

115. Application at 3 n.5, Fifth Cir. Decision, *supra* note 20 (No. 4:10-mj-00998).

116. 18 U.S.C. § 2703(c) (2012).

117. *See, e.g.*, United States v. Espudo, 954 F. Supp. 2d 1029, 1035-37 (S.D. Ca. 2013) (declining to treat location information as a record under the SCA despite government's argument that providers store the information, even for a few seconds, before transmitting it); London Decision, *supra* note 29, at *3, *8 ("The SCA has no prospective application.").

118. *See, e.g.*, Brooklyn I Decision, *supra* note 106, at 579 n.1; London Decision, *supra* note 29, at *3; *see also ECPA Reform & the Revolution in Location Based Techs. & Servs.: Hearing Before the Subcomm. on the Const., Civil Rights, & Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 86, 86 n.25 (2010) (statement of Stephen Wm. Smith, U.S. Mag. J.).

119. *See, e.g.*, Kevin S. Bankston, *Only the DOJ Knows: The Secret Law of Electronic Surveillance*, 41 U.S.F. L. REV. 589, 608 (2007); Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 815 & n.53 (2003); Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1567 (2004).

government requested them and not to permit telephone companies to provide newly generated records on a daily basis to the NSA.[120]

Whether the government may obtain real-time information as records under § 2703(c) matters if it is easier to get records than real-time information. If the government's view of the statute is correct, and it may compel the disclosure of records pursuant to a D order, then that is easier to obtain than what courts have required for access to real-time location data—either warrants or hybrid orders of D orders plus pen register orders.[121] Particularly in jurisdictions that require warrants for access to real-time location data, government agents may take advantage of the confusion around whether "records" can include instantaneously created records on an ongoing basis and circumvent the warrant requirement.[122] One court labelled as subterfuge attempts to "misuse" the SCA to get "freshly-created records" of location data as an "end-run around the legal limits on real-time access."[123] Perhaps that explains the government's applications to Judge Smith, who had written several opinions explaining why he requires a warrant based on probable cause for government access to real-time location data.[124]

The government's ability to take advantage of the lower protection for historical data as compared to real-time location data adds urgency to the question of whether the two types of data should be treated the same in any

120. *See* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 81-87 (2014), *available at* http://www.pclob.gov/All%20Documents/Report%20on%20the%20Telephone%20Records%20Program/PCLOB-Report-on-the-Telephone-Records-Program.pdf (interpreting section 215 of the Patriot Act).

121. A pen register order requires a government attorney only to certify to the court that the "information likely to be obtained . . . is relevant to an ongoing criminal investigation." 18 U.S.C. § 3123(a)(1) (2012). Because it is so easy to get a pen register order, a hybrid order should not be much harder to obtain than a D Order alone, but a warrant would be harder to obtain.

122. *See, e.g.*, *Espudo*, 954 F. Supp. 2d at 1034 (refusing to permit the Government to convert an application for real-time location data into one for records by claiming that the provider held the records "however briefly" before delivering them).

123. London Decision, *supra* note 29, at *10 n.15; s*ee also Espudo*, 954 F. Supp. 2d at 1037 (observing that "taking the Government's argument that real-time cell site location data is an historical record to its logical end" could lead to the government trying to use the easier-to-satisfy requirements of the SCA to avoid the legal constraints on wiretapping).

124. See *infra* text accompanying notes 165-67 for a discussion of how the Fifth Circuit decision declined to address prospective records questions by narrowing the scope of its inquiry.

case.[125] Both Judge Smith and Judge Lenihan discussed at length how it makes little sense to view an investigation into historical location data as less intrusive than one involving real-time data.[126] Other magistrate judges have agreed,[127] as have several academic commentators.[128] Congress will need to consider those arguments when and if it decides to legislate. For now, the lack of clear legal rules to address challenging practices adds yet more weight to the case for doing so.

II. Appellate Cases Provide Conflicting and Limited Guidance on Constitutional Law

The LEATPR Standards' drafters recognize that any legislature interested in drafting provisions for law enforcement access to third party records will want to consult existing law[129] and also ensure that anything it drafts satisfies constitutional requirements.[130] Part I elaborated on how the confusing and incomplete nature of existing federal statutory law on compelled access to location records made it a great candidate for legislative action. This Part explains how the Fifth Circuit and Third Circuit decisions provide Congress poor guidance on how the Fourth

---

125. *See, e.g.*, *Espudo*, 954 F. Supp. 2d at 1035 (describing the Government's contention, at oral argument, "that there is no cognizable difference between historical and real-time cell site location data").

126. Houston Decision, *supra* note 46, at 839 (finding the "degree of invasiveness" the same "between prospective and historical location tracking"); Pittsburgh Decision, *supra* note 45, at 607 n.55.

127. *See, e.g.*, Brooklyn I Decision, *supra* note 106, at 585 ("The picture of Tyshawn Augustus's life the government seeks to obtain is no less intimate simply because it has already been painted."); *In re* Applications of U.S. for Orders Pursuant to Title 18, U.S. Code, § 2703(d) to Disclose Subscriber Info. & Historic Cell Site Info. for Mobile Identification Nos.: (XXX) XXX-AAAA, (XXX) XXX-BBBB, & (XXX) XXX-CCCC, 509 F. Supp. 2d 64, 74 (D. Mass. 2007) (noting that the same Fourth Amendment concerns apply to both prospective and historical tracking devices).

128. *See, e.g.*, Freiwald, *supra* note 7, at 738-40; Henderson, *supra* note 4, at 831. *But see* Pell & Soghoian, *supra* note 3 (arguing that, apart from policy and constitutional questions, Congress is not likely to pass a warrant standard for access to historical location data, so privacy advocates should accept a lower procedural hurdle along with other protections, like minimization, notice, and reporting, that protect privacy and provide transparency).

129. STANDARD 25-4.1(d) (recommending that legislatures consider the extent to which "existing law . . . restricts or allows access to and dissemination of such information or of comparable information").

130. STANDARD 25-2.2 ("A legislature . . . may not authorize a protection less than that required by the federal Constitution . . . .").

Amendment regulates location records, compounding the need for guidance from the Standards.

A. Appellate Cases Disagree About Whether Targets Lack a Fourth Amendment Interest in Location Records Because a Third Party Stores Them

The lower courts that have accepted the government's claim that magistrate judges must grant D order applications for location records when they satisfy the reasonable and articulable facts standard have rejected users' claims to a Fourth Amendment interest in their location data. Often, courts have found users to have waived any Fourth Amendment privacy interest they might have had in their location data when they chose to share it with their providers.[131] The courts call this a "third party rule," drawn from the Supreme Court cases of *Smith v. Maryland*[132] and *United States v. Miller*.[133] In *Smith*, the Court denied the defendant's claim that law enforcement agents violated the Fourth Amendment when, without first obtaining a warrant, they had the phone company install a pen register to record the telephone numbers the defendant's phone dialed.[134] In *Miller*, the Court rejected the defendant's claim that agents had violated his Fourth Amendment rights when they compelled his bank to disclose his bank records, also without first obtaining a warrant.[135] Applying the same assumption of risk analysis the Supreme Court used in *Smith* and *Miller*, lower courts have reasoned that the target of an investigation may not complain if his location data is divulged to law enforcement, when a third party (the provider) does the divulging.[136] According to those courts, by permitting the provider access to his location data, a user has waived any expectation of privacy in that data.[137]

Some courts and several scholars have criticized the extension of the third party doctrine from *Smith* and *Miller*, both of which the Supreme

131. *See, e.g.*, United States v. Graham, 846 F. Supp. 2d 384, 400 (D. Md. 2012); United States v. Suarez-Blanca, No. 1:07-CR-0023-MHS/AJB, 2008 WL 4200156, at *8 (N.D. Ga. Apr. 21, 2008).

132. 442 U.S. 735 (1979).

133. 425 U.S. 435 (1976).

134. *Smith*, 442 U.S. at 742-44.

135. *Miller*, 425 U.S. at 444-46.

136. *See, e.g.*, *Graham*, 846 F. Supp. 2d at 397-401. See *infra* Part III.C for a discussion of how the Standards better distinguish between voluntary and compelled disclosure.

137. *See, e.g.*, *Graham*, 846 F. Supp. 2d at 401.

Court decided in the 1970s, into the modern age.[138] The Sixth Circuit rejected the government's attempted application of the doctrine to stored email in the 2010 *Warshak* case.[139] The Sixth Circuit determined that the third party doctrine does not apply when the third parties are internet service providers (ISPs) who act as "intermediaries" when they deliver and store their customers' emails, just as the postal service acts regarding mail and the phone company acts regarding phone calls.[140] In December of 2013, Judge Leon, in the District Court for the District of Columbia, similarly found that the *Smith* case simply did not apply, despite the government's urging that it squarely governed the National Security Agency's (NSA's) metadata collection program.[141] Recently, Justice Sotomayor explicitly criticized the third party doctrine in *United States v. Jones*,[142] the 2012 case finding a Fourth Amendment search when law enforcement agents used a GPS device to obtain location data.[143]

The Third Circuit Decision squarely rejected application of the third party doctrine to the location data context,[144] while the Fifth Circuit Decision did not apply it to location data as directly and comprehensively as the government had pressed.[145] Unfortunately for legal clarity, and just like with their statutory interpretation, the appellate court opinions neither

---

138. *See, e.g.*, Houston Decision, *supra* note 46, at 840-41; Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-mail*, 2008 U. CHI. LEGAL F. 121, 145-56; Stephen E. Henderson, *After* United States v. Jones*, After the Fourth Amendment Third Party Doctrine*, 14 N.C. J.L. & TECH. 431, 434-47 (2013); Erin Murphy, *The Case Against the Case For Third-Party Doctrine: A Response to Epstein and Kerr*, 24 BERKELEY TECH. L.J. 1239 (2009).

139. United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010).

140. *Id.* at 286.

141. Klayman v. Obama, 957 F. Supp. 2d 1, 30-37 (D.D.C. 2013). *But see* ACLU v. Clapper, 959 F. Supp. 2d 724, 751-52 (S.D.N.Y. 2013) (applying *Smith* to uphold the NSA's metadata program against Fourth Amendment challenge).

142. United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

143. *Id.* at 950-51. Because the GPS tracking device operated in real time, however, *Jones* was not a stored records case. Freiwald, *Good Faith Rule*, *supra* note 24, at 352 (casting doubt on the impact of Justice Sotomayor's language). Christopher Slobogin still regards *Jones* as a third party case because he views it as rejecting the idea that one loses privacy in information by exposing it outside to third parties. *See* Christopher Slobogin, *Making the Most of* United States v. Jones *in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST. L. & PUB. POL'Y 1, 6-7, 7 n.30 (2012).

144. Third Cir. Decision, *supra* note 20, at 317.

145. *Compare* Fifth Cir. Decision, *supra* note 20, at 615, *with* Brief of United States at 17-18, Fifth Cir. Decision, *supra* note 20 (No. 11-20884), 2012 WL 604860.

agreed with each other nor offered clear guidance to lower courts or legislators.

According to the Third Circuit, the provider's storage of the target's location records did not obviate the target's claim that warrantless compelled disclosure of those records violated her Fourth Amendment rights.[146] The court reasoned that cell phone customers are not likely to be aware that their "providers *collect* and store historical location information."[147] The court found that users "'voluntarily and knowingly'" convey only the numbers that they dial when they make cell phone calls and receive "'no indication'" that "'making [those] call[s] will also locate the caller[s].'"[148] As a result, they do not assume the risk of disclosure under the third party doctrine.

In its decision, the Fifth Circuit analyzed the third party doctrine by distinguishing the *Warshak* case.[149] Unlike an ISP, which delivers the communications of two parties without itself being a party to those communications, the Fifth Circuit found that a "cell service provider collects and stores historical cell site data for its own business purposes, perhaps to monitor or optimize service on its network or to accurately bill its customers for the segments of its network that they use."[150] Because providers are parties to the transactions that create location records, the Fifth Circuit found that such records are business records that lack Fourth Amendment protection under the third party doctrine of *Smith* and *Miller*.[151]

Coming six months earlier, the Fifth Circuit did not address Judge Leon's argument in *Klayman* that compelled disclosure of location data was not analogous to the installation of a pen register in *Smith v. Maryland*.[152] Judge Leon engaged in extensive analysis of how much information users reveal through use of their cell phones and how extensive location data may therefore be.[153] That analysis recalled the Houston Decision, in which Judge Smith colorfully concluded, "If the telephone numbers dialed in

146. Third Cir. Decision, *supra* note 20, at 317-18.

147. *Id.* at 317.

148. *Id.* (quoting Brief of Amicus Curiae Electronic Frontier Foundation, the American Civil Liberties Union, the ACLU-Foundation of Pennsylvania, Inc., and the Center for Democracy and Technology in Support of Affirmance of the District Court, Third Cir. Decision, *supra* note 20 (No. 07-524M), 2009 WL 3866619).

149. Fifth Cir. Decision, *supra* note 20, at 611.

150. *Id.* at 611-12.

151. *Id.*

152. Klayman v. Obama, 957 F. Supp. 2d 1, 30-37 (D.D.C. 2013).

153. *Id.* at 33-37.

Smith v. Maryland were notes on a musical scale, the location data sought here is a grand opera."[154]

Nor did the Fifth Circuit contend with Judge Smith's argument that Congress' passage of the Wireless Communication and Public Safety Act (WCPSA)[155] in 1999 provided location records special status.[156] According to Judge Smith, Congress' prohibition on the disclosure of "call location information" without customers' express prior authorization gives users a proprietary interest in their location records that they lack in ordinary business records.[157] The Fifth Circuit's opinion dismissed Judge Smith's argument as an attempt to determine reasonable expectations of privacy based on a statute.[158] As a later, specific statement by Congress about the nature of records containing location information, WCPSA arguably offers more valuable insight than the SCA into society's views of location privacy.[159]

The Fifth Circuit did recognize substantial limits on the applicability of the third party doctrine to location data.[160] The court distinguished cases in which the government required the third party to collect and store the information,[161] and applied the doctrine only when the "third party collects information in the first instance for its own purposes" (rather than for law-enforcement purposes) and the government later claims that it can obtain the information.[162] The decision included a quote from *Smith* that could be interpreted to weaken the line it appeared to draw: "'The 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

---

154. Houston Decision, *supra* note 46, at 846.

155. Wireless Communication and Public Safety Act of 1999, Pub. L. No. 106-81, § 5, 113 Stat. 1286, 1288 (codified as amended at 47 U.S.C. § 222 (2012)).

156. Houston Decision, *supra* note 46, at 841-43.

157. *Id.* at 842-43 (citing legislative history that evidenced concern for privacy interests in location information).

158. Fifth Cir. Decision, *supra* note 20, at 608 n.10.

159. *See* Recent Case, *supra* note 93, at 1226 ("The WCPSA thus suggests that Congress intended that individuals' privacy interest in location data be given particular weight in privacy assessments.").

160. Fifth Cir. Decision, *supra* note 20, at 611.

161. *Id.* at 610.

162. *Id.*; *see also* Recent Case, *supra* note 93, at 1223 (reading the decision to find "cell-site location data" to be "unprotected business records [when] the records are created by the cell service provider, the records memorialize transactions to which the provider is a party, the government does not require or encourage the preparation or retention of such records, and the user voluntarily conveys the data to the service provider").

difference.'"[163] But the opinion went on to repeat that location records are business records subject to the third party doctrine because "the Government merely comes in after the fact and asks a provider to turn over records the provider has already created."[164]

As discussed above, the government's applications had requested that, after receipt of the D order, the providers collect duration and recipient information, store it, and then forward that information to the requesting law enforcement agency.[165] Not only would the government's expansive definition of a "record" strain the statutory meaning, but it also would not constitute a business record, subject to the third party doctrine, under the Fifth Circuit's definition. That may explain why the Fifth Circuit did not grant the government's request for any location data except initiation and termination data.[166] Unfortunately, by not specifically addressing the government's application, the Fifth Circuit left the constitutional question somewhat unclear.[167]

In sum, the Third Circuit rejected application of the third party doctrine to users' Fourth Amendment claims in their location data, but the Fifth Circuit accepted it. The latter rejected Fourth Amendment claims only as to location information collected at the start and end of a call initiated by the target.[168] The Fifth Circuit clearly indicated that it was not addressing applications for location information "for the duration of the call or when the phone is idle" or about "the recipient of a call" from the target phone.[169] The government's application raised the question of the Fourth Amendment status of acquisition of that type of information, while other cases have concerned access to location information associated with text messages and internet use. The Fifth Circuit's opinion merely left the door open to such

163. Fifth Cir. Decision, *supra* note 20, at 610 (quoting Smith v. Maryland, 442 U.S. 735, 745 (1979)); *see also* United States v. Miller, 425 U.S. 435, 443 (1976) (opining that there would be no Fourth Amendment violation even if banks were storing information at the behest of the government).

164. Fifth Cir. Decision, *supra* note 20, at 612.

165. *See supra* text accompanying note 114.

166. Fifth Cir. Decision, *supra* note 20, at 615 (holding that D Orders "for specified cell phones at the points at which the user places and terminates a call are not categorically unconstitutional").

167. I made reference to the government's applications in my brief, *see* Freiwald Brief, *supra* note 114, and read from them at oral argument.

168. Fifth Cir. Decision, *supra* note 20, at 615.

169. *Id.* The decision did not clearly cover location information collected when the target receives calls.

claims without encouraging them. The resulting lack of clarity leaves little to guide either lower courts or Congress.

The Fifth Circuit's reading of the third party doctrine also preserves Fourth Amendment claims about location data collected after the government's request for an order or collected at the behest of the government. It preserves claims arising from when the provider acts as an intermediary rather than a party, such as when collection of data does not advance the providers' own business interests.[170] It remains unclear how to draw those lines through current practices. For example, when the government requests information about a cell phone user who is not the provider's subscriber, any records so collected would seem to advance only the government's interests—as distinguished from the provider's business interests—and therefore fall outside of the Fifth Circuit's third party exception to Fourth Amendment protection.[171]

B. The Appellate Courts Did Not Conclude Whether Compelled Disclosure of Location Data Intrudes on Reasonable Expectations of Privacy

Prior to *Jones*, when the Supreme Court determined that law enforcement agents conducted a Fourth Amendment search because they physically trespassed by installing a GPS device on Jones' car to track his movements,[172] courts determined whether the Fourth Amendment applied based on whether an investigation intruded on reasonable expectations of privacy.[173] The Supreme Court affirmed in *Jones* that the reasonable expectations of privacy test remains the appropriate test for those investigations, like the compelled disclosure of location data, that do not involve physical trespasses.[174] This subsection discusses the few doctrines

---

170. Judge Lenihan doubted whether the collection of most types of location data satisfied the Fifth Circuit's standard for falling within the third party doctrine. Pittsburgh Decision, *supra* note 45, at 615 (finding providers retain location data "principally, if not exclusively, in response to Government directive" rather than to "serve any business purpose for the customer or for the provider in serving the customer"); *see also* Klayman v. Obama, 957 F. Supp. 2d 1, 31-32 (D.D.C. 2013) (discussing the cooperative relationship that has developed between the telecom companies and government surveillance officials).

171. *See* Nathaniel Gleicher, Comment, *Neither a Customer Nor a Subscriber Be: Regulating the Release of User Information on the World Wide Web*, 118 YALE L.J. 1945 (2009) (describing how the SCA may not extend some protections to those who are neither subscribers nor customers).

172. United States v. Jones, 132 S. Ct. 945, 950-51 (2012).

173. *See* Kyllo v. United States, 533 U.S. 27, 33 (2001) (citing Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).

174. *Jones*, 132 S. Ct. at 953; *id.* at 954-55 (Sotomayor, J., concurring); *Klayman*, 957 F. Supp. 2d at 29 (using reasonable expectations of privacy to analyze Fourth Amendment

the appellate courts used to determine whether agents intruded on reasonable expectations of privacy, further limiting the guidance those cases provide to legislatures.

The Third Circuit's analysis focused on two Supreme Court cases from the 1980s concerning police tracking by radio-beepers installed on the defendants' belongings.[175] The Supreme Court found no intrusion into reasonable expectations of privacy when the device tracked the defendant on public highways in *United States v. Knotts*.[176] The Court found such an intrusion in *United States v Karo* when the surveillance revealed to agents that the defendant was at home—a fact not open to visual surveillance.[177] The Third Circuit viewed as significant whether an order requiring production of location data could reveal the target's location in her home.[178] Although Judge Lenihan found that location data intrudes on privacy interests in the home,[179] the Third Circuit concluded that the record did not yield sufficient evidence to determine that the location records the government sought would have extended into the home.[180] The majority's decision certainly suggested that the magistrate judge should determine that question on remand,[181] but it did not explicitly require it.[182] The concurring judge would have directed magistrate judges to refuse to grant a location data order for an application meeting the D order showing only when "the order would violate the Fourth Amendment absent a showing of probable cause because it allows police access to information which reveals a cell phone user's location within the interior or curtilage of his home."[183]

The Fifth Circuit entertained at some length the question of whether location information permitted law enforcement agents to determine that a

---

claims regarding government searching through telephony metadata because plaintiffs lacked a possessory interest in their phone data).

175. Third Cir. Decision, *supra* note 20, at 312.

176. 460 U.S. 276, 281-82 (1983).

177. 468 U.S. 705, 719 (1984).

178. Third Cir. Decision, *supra* note 20, at 311-12.

179. Pittsburgh Decision, *supra* note 45, at 613 (finding that "practical limitations on the abilities of [providers] to filter their [location data] would almost certainly result in over-inclusive disclosures, and thus in transgressions of Constitutional boundaries").

180. Third Cir. Decision, *supra* note 20, at 313.

181. *See id.* at 317 (complaining that the government's position would preclude the Magistrate Judge 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").

182. *See supra* text accompanying note 89.

183. Third Cir. Decision, *supra* note 20, at 320 (Tashima, J., concurring).

target was in her home.[184] In the Houston Decision below, Judge Smith based his requirement of a warrant for access to location data primarily on his determination that location data had become sufficiently precise to reveal information inside the home.[185] Specifically, Judge Smith found that "[o]ver the course of two months, it is inevitable that dozens if not hundreds of calls and text messages of a typical user will be sent from home, office, or other place out of public view" subject to Fourth Amendment protection.[186] The Fifth Circuit noted the arguments on both sides of the question, but ultimately did not resolve whether location data revealed inside-the-home information because it disposed of the constitutional question presented based on the third party doctrine.[187]

The only affirmative constitutional analysis the appellate courts have ratified for determining reasonable expectations of privacy in location data , then, is based on the doctrine that the Fourth Amendment protects our privacy interests in the home and surrounding areas. The Third Circuit affirmed that doctrine's vitality and did not elaborate on other ways to analyze reasonable expectations of privacy.[188] The Fifth Circuit certainly did not deny the doctrine, but neither did the court demonstrate its application.[189] It did not analyze reasonable expectations of privacy in location data because it used the third party doctrine and a narrowing construction of the question presented to limit its inquiry.

C. The Appellate Courts Have Not Affirmed Lower Courts' Expanded Analyses

The magistrate judges who have found that law enforcement's compelled disclosure of location data implicates Fourth Amendment privacy interests have often considered other approaches to the constitutional analysis. Those approaches could guide legislators interested in coming up with provisions to regulate law enforcement access to location records. However, none of those approaches has received the imprimatur of an appellate court.

As a secondary basis for the Houston Decision, Judge Smith opined that location records are subject to Fourth Amendment protection under a prolonged surveillance theory, according to which the government's request

184. Fifth Cir. Decision, *supra* note 20, at 608-09.
185. Houston Decision, *supra* note 46, at 835-38.
186. *Id.* at 836.
187. Fifth Cir. Decision, *supra* note 20, at 610.
188. Third Cir. Decision, *supra* note 20, at 312.
189. Fifth Cir. Decision, *supra* note 20, at 609.

for two months of data was more intrusive into reasonable expectations of privacy than a shorter inquiry.[190] As it came after the Houston Decision, Judge Smith did not rely on *Jones*, but rather on the reasoning of the appellate court in *United States v. Maynard*, the decision the Supreme Court affirmed on appeal in *Jones*.[191]

Neither the Third nor the Fifth Circuit used the prolonged surveillance doctrine in its reasoning. The Third Circuit Decision predated *Maynard* so obviously did not refer to it. The Fifth Circuit Decision rejected the idea that it would "create a new rule" based on the fact that the records requested "cover more than some specified time period." [192] In its brief to the Fifth Circuit, the government argued that the court should not recognize the prolonged surveillance doctrine as binding because only concurring Justices had approved it, although five concurring Justices had done so.[193]

The magistrate judges also considered the nature of information sought in their analysis. For example, both Judge Smith and Judge Lenihan discussed the revealing nature of location information. Judge Lenihan "observe[d] that the location information so broadly sought is extraordinarily personal and potentially sensitive."[194] Judge Smith agreed with Magistrate Judge Orenstein that cell phone tracking may be more intrusive and revealing than tracking by a GPS device because people take their cell phones with them everywhere they go, including often to their bedsides.[195]

The lower courts also referred, briefly, to the secret nature of location record acquisition; disclosures generally happen without targets knowing about them. As Judge Lenihan explained, "[T]he *ex parte* nature of the proceedings, the comparatively low cost to the Government of the information requested, and the undetectable nature of a [provider's]

190. Houston Decision, *supra* note 46, at 838.

191. *Id.* at 838-39 (deriving the prolonged surveillance doctrine from United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), *aff'd sub nom.* United States v. Jones, 132 S. Ct. 945 (2012)). Judge Smith gave credit to a previous decision for its reliance on *Maynard* to resolve the constitutional question. *See id.* (citing Brooklyn I Decision, *supra* note 106, at 585).

192. Fifth Cir. Decision, *supra* note 20, at 615.

193. Reply Brief of United States at 16, Fifth Cir. Decision, *supra* note 20 (No. 11-20884), 2012 WL 10205101.

194. Pittsburgh Decision, *supra* note 45, at 586; *see also id.* at 609 (opining that the procedural hurdle to be overcome depends on the "nature of the records or information sought").

195. Houston Decision, *supra* note 46, at 840 (citing Brooklyn I Decision, *supra* note 106, at 590-91); *see also* Brooklyn II Decision, *supra* note 106, at 119.

electronic transfer of such information, render these requests particularly vulnerable to abuse."[196] Judge Lenihan also discussed the risk that monitoring location data would have a chilling effect on First Amendment protected associational activities.[197]

In considering reasonable expectations of privacy, several of the magistrate judges referred to their obligation to engage in a normative analysis about what the emerging law *should* be. Judge Lenihan quoted language in which Justice Harlan, in dissent, indicated that "[t]he critical question, therefore, is whether under our system of government, as reflected in the Constitution, we should impose on our citizens, the risk of the electronic listener or observer without at least the protection of a warrant requirement."[198] In finding the SCA unconstitutional because it permitted access to location data without a probable cause warrant, Judge Orenstein, of the Eastern District of New York, refused to "abandon[] the critical and continuing task of identifying the expectations of privacy our society is prepared to recognize as reasonable."[199] Judge Garaufis, also of the Eastern District of New York, in coming to the same conclusion as Judge Orenstein, reasoned that under a proper "'normative inquiry,'" users have a reasonable expectation of privacy in their cumulative location records.[200]

Interestingly, in finding reasonable expectations of privacy and requiring a probable cause warrant for compelled access to stored email by ISPs, the Sixth Circuit, in *Warshak*, engaged in the same type of normative analysis.[201] But *Warshak* is an appellate case that gives clear guidance to a Congress interested in updating the electronic surveillance laws. By avoiding a normative analysis of location data, or any sustained analysis of how to evaluate reasonable expectations of privacy in location data, the

196. Pittsburgh Decision, *supra* note 45, at 586, 586 n.7 (citing Freiwald, *First Principles*, *supra* note 24, ¶ 10). I argued in the article cited that when the four factors of continuous, indiscriminate, intrusive, and hidden characterize a law enforcement investigation, then the highest form of judicial oversight should apply. Freiwald, *First Principles*, *supra* note 24, ¶ 76; *see also* Freiwald, *supra* note 7, at 746-48 (arguing that the four-factor analysis yields the conclusion that compelled disclosure of location records that cover a period time should require a warrant based on probable cause).

197. Pittsburgh Decision, *supra* note 45, at 612.

198. *Id.* at 612 n.70 (quoting United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting)).

199. Brooklyn I Decision, *supra* note 106, at 596.

200. Brooklyn II Decision, *supra* note 106, at 124 (quoting Smith v. Maryland, 442 U.S. 735, 741 n.5 (1979)).

201. *See* Freiwald, *supra* note 7, at 745-46 (discussing *Warshak*'s normative analysis).

appellate courts have provided no similar guidance and instead left Congress in the dark.[202]

III. The Standards Provide Valuable Guidance to Congress

The LEATPR Standards provide a framework for members of Congress interested in drafting an entirely new law or amending the SCA to address law enforcement's compelled disclosure of location records from service providers. The Standards direct legislators first to consider what level of privacy a particular type of records should have, and from there they provide guidance on how to select the appropriate procedural hurdle and other statutory protections based on the level of privacy protection.[203] This Part addresses how the Standards' guidance on how to select a privacy level and what privacy protections to provide adds significantly to the guidance that appellate court opinions furnish on location records access by law enforcement.

A. The Standards Advise Consideration of a Richer Body of Factors

As discussed in Part II, two appellate cases to date have given conflicting and severely limited guidance on the Fourth Amendment protection of location data. They have disagreed on whether the third party doctrine obviates protection. They have also failed to determine whether, and if so when, users entertain reasonable expectations of privacy in location information, besides engaging in a limited discussion of the nonpublic space doctrine. The lower courts have expanded the analysis considerably more, but in nonbinding decisions that the appellate courts have not affirmed.

The Standards, because they make recommendations to policy makers who are free to legislate above the floor set by the Fourth Amendment, advise interested legislators to consider a wider range of factors than even those the magistrate judges have so far considered. Because they draw from a variety of sources, the Standards encourage lawmakers to take a broader view of the issues, which if taken seriously, would significantly enrich the discussion of electronic surveillance regulation.[204]

---

202. *See* Recent Case, *supra* note 93, at 1223-27 (citing Freiwald, *First Principles*, *supra* note 24) (arguing that the Fifth Circuit should have conducted a normative analysis instead of merely a positive one).

203. *See generally* Henderson, *supra* note 4 (reviewing in detail how the Standards would apply to location data).

204. *See id.* at 813, 815-18 (describing the factors to be considered in the context of location records).

For example, in determining the proper privacy category for location records, the Standards advise legislators to consider, in addition to current law,

> present and developing technology and the extent to which:
>
> (a) the initial transfer of such information to an institutional third party is reasonably necessary to participate meaningfully in society or in commerce, or is socially beneficial, including to freedom of speech and association;
>
> (b) such information is personal, including the extent to which it is intimate and likely to cause embarrassment or stigma if disclosed, and whether outside of the initial transfer to an institutional third party it is typically disclosed only within one's close social network, if at all; [and]
>
> (c) such information is accessible to and accessed by non-government persons outside the institutional third party.[205]

Regarding location records, paragraph (a) would have legislators look much more closely at the creation of location records than either current statutory or constitutional law. As a matter of the former, nothing in the text of the SCA turns on how records are created. As for constitutional law, paragraph (a) encourages legislatures to recognize a fundamental criticism of the third party doctrine: that it presumes that people assume the risk of compelled disclosure when they share information, without inquiring into whether they had a choice not to share the information.[206] As Judge Leon recognized in *Klayman*, which is a preliminary decision by a district court and does not concern compelled disclosure of location records, Americans now use their cell phones to a staggering degree, and many people rely solely on their cell phones for their voice and text communications.[207] Paragraph (a) directs legislators to engage in deeper analysis of the conditions under which users disclose location data to their providers than the Fifth Circuit did when it reasoned that voluntary use of a cell phone was sufficient to waive a constitutional privacy interest in some location data.

Notably, paragraph (a) does not require legislators to determine that the disclosure of location data is unavoidable in order to accord such data more

---

205. STANDARD 25-4.1(a)-(c).

206. STANDARD 25-4.1(a) commentary.

207. Klayman v. Obama, 957 F. Supp. 2d 1, 34 n.51 (D.D.C. 2013); *see also* STANDARD 25-4.1(a) commentary (citing similar statistics).

privacy protection. The Standards' drafters recognize that people should not be viewed as voluntarily relinquishing their private information when they must do so to participate meaningfully in society. They also recognize a value in participating meaningfully in commerce, so they instruct legislators to be sympathetic to claims that users want to take advantage of technological innovation without having to give up their privacy.

In addition, by having legislatures consider whether they want to encourage the transfer of information to providers because doing so furthers speech, associational, or other socially beneficial values, the Standards' drafters focus on the subjective chill that excessive surveillance creates. Recent Supreme Court decisions have rejected privacy claims that could not definitively establish surveillance[208] or monetize the harm from disclosure of information,[209] but the Standards remind legislators that other legal authority provides a basis to protect privacy so as not to have undue surveillance inhibit valuable activities.[210] The Standards' drafters make clear that location records represent just the type of records that have benefited society, and that the Supreme Court has recognized the value of cell phone use for self-expression and self-identification, though only in dicta.[211]

In paragraph (b), the Standards' drafters focus legislators' attention on the characteristics of the information in the records, such as whether it is personal, intimate, or embarrassing.[212] Other than distinguishing between records relating to telecommunication fraud and records containing basic subscriber information, both of which receive less protection, the SCA treats all records the same so long as they pertain to the user's or subscriber's use of a provider's system.[213] Under the appellate courts'

208. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1148-50 (2013) (denying plaintiffs standing because they failed to establish that the NSA had acquired their communications pursuant to section 702 of the Foreign Intelligence Surveillance Act Amendments Act of 2008).

209. Doe v. Chao, 540 U.S. 614, 620 (2004) (requiring plaintiffs to prove "actual damages" to receive recovery for disclosure of their social security numbers in violation of the Privacy Act of 1974).

210. STANDARD 25-4.1(a) commentary (citing lower court cases discussing chill and noting that "with mobile telephony the contribution to the freedoms of expression and association are quite strong").

211. *Id.* (citing City of Ontario v. Quon, 560 U.S. 746, 760 (2010) (dictum)).

212. STANDARD 25-4.1(b).

213. 18 U.S.C. § 2703(c) (2012).

constitutional analysis,[214] the characteristics of the information listed in paragraph (b) are arguably related to an analysis of whether the records divulge that the target was inside her home.[215] Similarly, the Fifth Circuit explicitly carved out from Fourth Amendment protection, through use of the third party doctrine, business records that the provider collects for its own purposes,[216] which may, by implication, exclude some personal or intimate information collected out of mere curiosity or to violate privacy.[217] But neither appellate court affirmed the more expansive inquiry that the magistrate judges conducted into the revealing and sensitive nature of the information that location data can reveal, particularly when it covers a prolonged period.

The Standards' drafters affirmed the legitimacy of the prolonged surveillance approach to location records that Judge Smith and other magistrates had found helpful. In elaborating on paragraph (b), the drafters recognize that location information over a significant period reveals an intimate picture that a target does not expect anyone else, except perhaps her spouse, to see.[218] They also affirmed making a much more thoughtful inquiry into what the location data reveals.

Paragraph (c) of Standard 25-4.1 directs legislators to consider the extent to which the information at issue is "accessible to and accessed by non-government persons" besides the provider.[219] According to the Standards commentary, the drafters do not mean to "further tip the scales" beyond the analysis in paragraph (b), but rather to recognize that when people make some otherwise personal information available to many other private parties, "law enforcement need not alone 'shield its eyes.'"[220] The Standards commentary does not apply paragraph (c) to location data or any other category of records. It cautions that the factor is "dependent upon the

---

214. *See* Third Cir. Decision, *supra* note 20, at 311-13, 317; Fifth Cir. Decision, *supra* note 20, at 608-10.

215. *See* United States v. Kyllo, 533 U.S. 27, 37-39 (2001) (opining that, in the home, all details are intimate, a position discussed in the commentary to Standard 25-4.1(b)).

216. Fifth Cir. Decision, *supra* note 20, at 611-12.

217. *See* Adam Gabbatt, *NSA Analysts 'Wilfully Violated' Surveillance Systems, Agency Admits*, GUARDIAN (Aug. 24, 2013), http://www.theguardian.com/world/2013/aug/24/nsa-analysts-abused-surveillance-systems (reporting NSA analysts' abuse of agency surveillance systems to spy on love interests).

218. STANDARD 25-4.1(b) commentary (citing United States v. Maynard, 615 F.3d 544, 563 (D.C. Cir. 2010)).

219. STANDARD 25-4.1(c).

220. STANDARD 25-4.1(c) commentary (quoting California v. Ciraolo, 476 U.S. 207, 213 (1986)) (referring to the Fourth Amendment's plain view doctrine).

norms and actions within a particular jurisdiction"[221] and that legislatures should consider "social norms and practical realities" and "not merely that private persons theoretically could access information, but that they in fact do so."[222]

The commentary to paragraph (b) suggests that the drafters may view disclosure of location data in social network contexts as influencing the privacy protection applicable to the compelled disclosure of location records.[223] I would read that to mean that if someone makes location data publicly available online, then that limits the privacy protection of that specific information, if it is available in a provider's records as well.[224] Otherwise, the public viewing of some people's limited location data would be able to reduce the privacy of other people's much more extensive location data gathered in a secret manner through compelled disclosure.[225]

B. The Standards Remind Legislators to Consider a Range of Protections

As Parts I and II discussed, debates about how current law regulates access to location records have concerned whether judges may or must impose a probable cause standard before agents may obtain an order to compel disclosure of location records, or whether they may or must accept a reasonable and articulable facts showing. Section 2703(c) specifically excuses law enforcement agents from providing notice to targets that their providers have disclosed their location data;[226] the appellate courts have not considered other procedural protections besides the showing needed to obtain the court order.

The Standards address the showing that agents must make before they may obtain an order to compel disclosure of location records.[227] The

221. *Id.*

222. *Id.*

223. *Id.*

224. Professor Henderson's article supports that limited view, as he notes that he does not see any evidence of this factor supporting a lack of privacy in location records. Henderson, *supra* note 4, at 817.

225. The ambiguity here highlights a problem with categorization by general type of information rather than by method of access. For approaches promoting regulation by method of access, see Freiwald, *supra* note 7; David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62 (2013). The Standards do not preclude further categorization, however. *See* Henderson, *supra* note 4, at 832 (citing Slobogin, *supra* note 143, at 24-27, 35) ("[M]y preference, like that of Christopher Slobogin, is to vary the regulation solely by time.").

226. 18 U.S.C. § 2703(c)(3) (2012).

227. *See* Henderson, *supra* note 4, at 813, 815-18.

Standards' framework matches procedural hurdles to the privacy categories that lawmakers choose for a category of records based on their consideration of the relevant factors.[228] Without doing a full analysis myself, I would agree with Stephen Henderson's recent conclusion that most location records would fall under the highly private category.[229] Professor Henderson would treat information for a period of up to twenty-four hours as moderately private,[230] and information for a single point in time as not private.[231] For highly protected information, the Standards recommend a court order based on "a judicial determination that there is probable cause to believe the information in the record contains or will lead to evidence of a crime."[232] That formulation would certainly need to be supplemented by further restrictions on scope so as not to permit fishing expeditions.[233]

In addition, the Standards state that notice should be provided to the focus of the record, generally within thirty days of disclosure, for all highly and moderately protected information.[234] In elaborating on the recommendation that legislators require notice for both types of protected information, the Standards commentary refers approvingly to Judge Smith's pioneering work on the excessive secrecy of current electronic surveillance practices.[235] The Standards recommendation would go a long way toward

---

228. *See id.*

229. *Id.* at 819.

230. *Id*. The Standards recommend a court order based on reasonable suspicion, which is what the reasonable and articulable facts standard is modeled upon, for moderately protected records. STANDARD 25-5.2(a)(ii); STANDARD 25-5.3(a)(ii). The Standards bracket a choice to provide a court order or a prosecutorial certification based on relevance for moderately protected records. STANDARD 25-5.2(a)(iii), (iv); STANDARD 25-5.3(a)(ii).

231. Henderson, *supra* note 4, at 819. In my article analyzing compelled disclosure of location records under the Fourth Amendment, I doubted that agents would know in advance that they were seeking circumscribed information. Freiwald, *supra* note 7, at 747. If they do focus on information for one particular time, perhaps a lesser showing than probable cause would be acceptable so long as other protections were in place. *See* Pell & Soghoian, *supra* note 3, at 183-93 (describing notice, minimization, and reporting requirements for a location data statute).

232. STANDARD 25-5.2(a)(i); STANDARD 25-5.3(a)(i).

233. *See* Pell & Soghoian, *supra* note 3, at 180-81 (recommending a nexus requirement to go along with their procedural hurdle for access to historical location data); *see also id*. at 183-93 (recommending other procedural rules to rein in investigations and provide privacy and transparency).

234. STANDARD 25-5.7 commentary.

235. *Id.* at n.358 (citing Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, 6 HARV. L. & POL'Y REV. 313, 314 (2012)).

promoting the transparency and accountability that Judge Smith recommended in his article.[236] Moreover, by providing notice to all who are the focus of records, and not just those whom law enforcement subsequently prosecutes on the basis of what it finds, the Standards' approach promises to solve the significant problem Judge Smith identified: innocent people never find out that their privacy has been invaded.[237]

As further procedural protections against abusive practices, the Standards remind legislators to consider "more demanding restraints" for access to records containing highly protected information.[238] The Standards suggest requiring: "additional administrative approval, additional disclosure, greater investigative need, or procedures for avoiding access to irrelevant information."[239] The Standards' list draws from protective procedures that Congress imposed on wiretapping and eavesdropping in the 1968 Wiretap Act.[240] It reminds Congress that when practices raise the risk of abuse, a requirement of probable cause is not the only protection available.[241]

C. The Standards Promote a Properly Limited Scope for the Third Party Doctrine

When the Fifth Circuit considered the third party doctrine, it rejected the Third Circuit's conclusion that users were not sufficiently aware of the collection and storage of their location data to have assumed the risk of its disclosure—at least as to initiation and termination data.[242] The Fifth Circuit's opinion found that modern cell phone users know that their cell phones use cell towers because users are aware that they may be out of range of their providers' network and because their providers' terms of service and privacy policies disclose that such providers use location

236. *See* Henderson, *supra* note 4, at 821 ("Such notice would be a significant improvement to federal law." (citing Smith, *supra* note 235)).

237. *See* Smith, *supra* note 235, at 332. *Compare* Or. Prescription Monitoring Program v. DEA, No. 3:12-cv-02012-HA, 2014 WL 562938, at *4 n.2 (D. Or. Feb. 11, 2014) (noting the likely lack of challenges to the DEA's practice of acquiring stored prescription data from a central database when the DEA does not notify subjects of its access), *with* Susan Freiwald & Sylvain Métille, *Reforming Surveillance Law: The Swiss Model*, 28 BERKELEY TECH. L.J. 1261, 1299-1300 (2013) (noting that under Swiss surveillance law, the target of records surveillance receives after-the-fact notice in all cases).

238. STANDARD 25-5.3(b).

239. *Id.*

240. STANDARD 25-5.3(b) commentary.

241. I have promoted the additional protections of the Wiretap Act for online surveillance practices as well. Freiwald, *supra* note 69, at 74-84.

242. Fifth Cir. Decision, *supra* note 20, at 613 (calling the Third Circuit's analysis a "crabbed understanding . . . [that] would lead to absurd results").

information to route calls.[243] The court found that users voluntarily convey location data when they make calls because they choose to get phones, to select particular providers, and to make calls; they know that calls convey location information and that providers retain that information, which they will turn over to the police when presented with a court order.[244]

The Fifth Circuit's reasoning applies the third party doctrine to deny privacy protection to location records in an expansive and erroneous manner that the Standards do not replicate. Instead, the Standards recognize that there are only two ways for a cell phone user to assume the risk that her provider will disclose her records: (1) when she knowingly and voluntarily consents to such disclosure[245] or (2) when the provider, voluntarily and on its own initiative, discloses the user's records.[246] In the absence of either of those circumstances, the Standards' framework applies, notwithstanding that location records constitute the provider's business records.

According to the Standards, law enforcement should be able merely to request particular location records when the "focus of the record has knowingly and voluntarily consented to that specific law enforcement access"[247] or that person gave "generalized consent to law enforcement access, and . . . it was possible to decline the generalized consent and still obtain the desired service from the provider requesting consent, and the focus of the record had specifically acknowledged that it was possible."[248] According to the Standards commentary, for highly and moderately protected information such as location records, law enforcement agents should have to point to *individualized* agreements to show that users waived their privacy rights by agreeing to law enforcement access.[249] The Standards' drafters do not agree with the Fifth Circuit's logic that by using a provider whose terms of service and privacy policies indicate that law enforcement has access to location records, users thereby waive any privacy rights in those location records.

The Standards recognize that a user may waive her privacy rights in her location records when her provider voluntarily conveys them to law

243. *Id.* (finding also that terms of service and privacy policies indicate that the providers store location data and may share it with the government).

244. *Id.* at 614.

245. STANDARD 25-5.1(a)-(b).

246. STANDARD 25-2.1(f)(ii).

247. STANDARD 25-5.1(a).

248. STANDARD 25-5.1(b).

249. STANDARD 25-5.1(b) commentary.

enforcement "entirely upon its own initiative."[250] The Standards carve out provider-initiated disclosures from coverage because such disclosures count as private conduct, which Congress may choose to regulate,[251] but which do not fall under the purview of criminal procedure.[252] The Commentary clarifies that "[t]he situation is markedly different, however, when law enforcement initiates a specific contact with a particular third party, and that contact leads to a records transfer."[253] In the latter case, the provider should be treated as an agent of the government, and the protections of the Standards should apply.[254]

The commentary to paragraph (a) explicitly dispenses with the idea that the assumption of risk doctrine applies equally when law enforcement compels the provider to disclose records as to the case when the provider initiates disclosure himself. The commentary explains that even though one accepts the risk that law enforcement will obtain information one chooses to disclose to another, "it begs the question to presume that there must therefore be no restraint upon law enforcement access, for it is the law that defines what risk is thereby assumed."[255] Maintaining the crucial distinction, the commentary continues to explain that "[e]ven were there to be no restraint upon voluntary third party-initiated dissemination, it would not follow that there should be no restraint upon law enforcement-initiated access."[256]

The Standards' distinction properly reins in the third party doctrine to keep it from depriving users, whose records are the subject of compelled disclosure orders, of privacy protections. It also more properly aligns with the genesis of the third party doctrine. In the *Miller* case, when the Supreme Court first enunciated the doctrine, it based its reasoning on the *Hoffa*/*White* line of cases.[257] But those cases concerned the risk that the person to whom the defendant disclosed information himself voluntarily

250. STANDARD 25-2.1(f)(ii) commentary (referring to Standard 25-2.1(f)(ii), under which the Standards "do not relate to . . . [a provider] deciding of its own initiative and volition to provide information to law enforcement").

251. In fact, the SCA currently permits providers to disclose records to anyone except governmental entities. 18 U.S.C. § 2703(c) (2012).

252. STANDARD 25-2.1(f)(ii) commentary.

253. *Id.*

254. *Id.*

255. STANDARD 25-4.1(a) commentary.

256. *Id.*

257. *See* Bellia & Freiwald, *supra* note 138, at 154-56.

initiates the disclosure. The *Hoffa*/*White* line did not involve the risk of compelled disclosure by law enforcement.[258]

By stretching the third party doctrine to find that users assume the risk that their providers will be compelled to disclose their records, the Fifth Circuit and many lower courts have denied privacy protection where the Standards would provide it. In addition, they have avoided engaging in a searching inquiry into the nature of the relationship between the providers and law enforcement that the Standards also promote. They have accepted too quickly that by mere use of an essential tool of modern communication, users have lost the ability to raise legal claims to the privacy of their location information. The Standards would not have legislators make that same analytical error.

Conclusion

The Standards provide important insights to legislators who want to fill the gap that is the current law on law enforcement access to location records. They encourage law makers to extend their gaze well beyond the extremely limited consideration of whether location records would reveal information about the inside of the home to take account of a much wider range of significant questions about the nature of location records. They correct several flaws in the Fifth Circuit's approach to assumption of risk, including the notion that mere use of a provider coupled with likely constructive knowledge of the possibility of law enforcement access to records are sufficient to deprive a user of privacy protection in even a limited amount of location data. Finally, they remind Congress that, while it matters what showing law enforcement agents must make to a judge before obtaining an order for location records, other procedural protections, such as notice, meaningfully contribute to transparency and accountability and help rein in abusive practices.

258. For that reason, I have argued, with a co-author, for the same distinction between provider-initiated disclosure and compelled disclosure that the Standards promotes. *Id.* at 169.