CELL PHONE LOCATION DATA AND THE FOURTH AMENDMENT: A QUESTION OF LAW, NOT FACT

SUSAN FREIWALD*

I. INTRODUCTION

Despite how much we use new communications technologies like e-mail and cell phones, federal appellate courts have provided little guidance about what the Fourth Amendment[1] requires of law enforcement agents before they may obtain our electronic communications.[2] Several factors explain why federal appellate courts have considered so few constitutional challenges to "online surveillance" practices.[3] To begin with, the Electronic Communications Privacy Act ("ECPA") furnishes little incentive for defendants to bring *statutory* claims against law enforcement acquisition of their electronic communications because the ECPA provides no exclusionary remedy.[4] To suc-

* Professor of Law, University of San Francisco School of Law. I thank research librarian John Shafer and research assistants Kelly Mannion, Aaron Marienthal, and David Reichbach for their valuable help. Thanks to Erin Dolly for her editorial contributions on this paper. I could not have done the work I did on the case on which this paper is based without the invaluable discussions and support of Kevin Bankston and Jennifer Granick of the Electronic Frontier Foundation ("EFF"). I also thank my colleagues at USF and my friends at EFF and elsewhere who mooted me for oral argument (sometimes more than once).

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

2. The United States Court of Appeals for the Sixth Circuit issued a decision between the drafting of this Article and its publication that recognized a Fourth Amendment interest in e-mail stored with a service provider. *See* United States v. Warshak, 631 F.3d 266, 274 (6th Cir. 2010). For further discussion of the *Warshak* case and earlier decisions pertaining to the case against *Warshak*, see *infra* text accompanying notes 118–22. R

3. *See generally* Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9 (2004) [hereinafter Freiwald, *Online Surveillance*] (describing the statutory and constitutional rules pertaining to government surveillance of online communications).

4. *Compare* 18 U.S.C. § 2515 (2006) (providing a statutory suppression remedy for improper interceptions of wire and oral communications, but not electronic communications), *with id.* § 2708 ("The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter."). *See generally* Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L. J. 805, 807–08 (2003) (recommending a statutory suppression remedy for electronic communications).

cessfully have such evidence excluded from trial, defendants must establish a Fourth Amendment violation and overcome a good faith defense.[5] Citing a lack of precedent, courts have refused even to consider Fourth Amendment questions in some cases after crediting agents' claims that they acted in good faith.[6] While the lack of precedent will persist until a court issues a decision, that fact alone has not compelled a court to act.[7] Exacerbating the lack of challenges from defendants who likely perceive insurmountable odds, executive branch litigators have themselves strategically avoided appealing cases to preserve the prerogatives that a definitive constitutional ruling against them would eliminate.[8] The absence of cases from the last several decades means that when government lawyers do argue that their practices satisfy Fourth Amendment mandates, they rely on Supreme Court cases from the 1970s and 1980s that addressed primitive ancestors of the electronic communications technologies in use today.[9]

All that might have changed last year when the United States Court of Appeals for the Third Circuit issued a decision about whether to permit government agents to obtain, without a warrant, cell phone subscribers' location data—for example, records of the cell

5. *See, e.g.*, United States v. Ferguson, 508 F. Supp. 2d 7, 9–10 (D.D.C. 2007) ("The Fourth Amendment's exclusionary rule does not apply where the challenged evidence was obtained by an officer acting in objectively reasonable reliance on a statute even if that statute was later determined to be unconstitutional."); Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, ¶4, ¶13, http://stlr.stanford.edu/pdf/freiwald-first-principles.pdf [hereinafter Freiwald, *First Principles*] (noting that the lack of a statutory suppression remedy inhibits defendants from bringing these cases).

6. *See, e.g.*, *Warshak*, 631 F.3d at 288–92 (relying on *Illinois v. Krull*, 480 U.S. 340 (1987), in denying a motion to suppress stored e-mails on the basis of "good faith" reliance on statute); United States v. Suarez-Blanca, No. 1:07-CR-0023-MHS/AJB, 2008 WL 4200156, at *11–13 (N.D. Ga. Apr. 21, 2008) (explaining that even if government access to historical cell site location information violated the Fourth Amendment, the "good faith" exception would preclude any exclusionary remedy).

7. *Cf. In re* Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 736 F. Supp. 2d 578, 580 n.5 (E.D.N.Y. 2010) [hereinafter *CSI: Brooklyn*] (describing the lack of settled precedent in this area of law), *rev'd*, Order, *CSI: Brooklyn*, 736 F. Supp. 2d 578 (E.D.N.Y. Nov. 29, 2010), ECF No. 11. This Article will follow the naming convention set out in *CSI: Brooklyn*, *id.* at 580 n.4, instead of using the cumbersome titles each time I refer to cases involving location data.

8. *See id.* at 580 n.5 (discussing the government's failure to appeal cases); *see also* Catherine Crump & Christopher Calabrese, *Location Tracking: Muddled and Uncertain Standards Harm Americans' Privacy*, 88 CRIM. L. REP. 19 (2010) (concluding, from a study of Freedom of Information Act requests, that government lawyers strategically avoid appealing adverse rulings).

9. *See infra* Parts IV–V.

towers ("cell site information" or "CSI")[10] with which a mobile phone communicates—which indicate the phone's physical location (also known as "location data").[11] The government claimed the right to compel a service provider to disclose location data whenever government agents overcome the easier-to-meet procedural hurdles for non-contents records in the ECPA, instead of having to first obtain a warrant based on probable cause under the Fourth Amendment standard. In particular, the government claimed it could compel disclosure of stored location data so long as it obtained a court order, referred to as a "D order," under 18 U.S.C. § 2703(d), which requires "specific and articulable facts showing . . . reasonable grounds to believe that the . . . records . . . are relevant and material to an ongoing criminal investigation."[12] Lower courts in the case previously denied the government's application and rejected both its statutory and constitutional arguments.[13] Had the court in *CSI: Third Circuit* held that the Fourth Amendment requires a warrant before agents may compel a service provider to disclose location data, the court would have provided crucial constitutional guidance to lower courts. Federal district courts are currently considering location data applications and disagreeing about the proper rule.[14] If the court had actually analyzed reasonable expectations of privacy in new electronic communications, it would have yielded valuable insights for similar cases that involve online surveillance practices.

The majority in *CSI: Third Circuit*, however, did not provide a definitive Fourth Amendment analysis. Instead, it held that magistrate

10. Cell sites may be located on stand-alone towers or on top of pre-existing buildings. *See* PAUL BEDELL, WIRELESS CRASH COURSE 37–38 (2d ed. 2005). I will refer to cell sites as cell towers because the latter term seems easier to visualize.

11. *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 305–06 (3d Cir. 2010) [hereinafter *CSI: Third Circuit*].

12. *Id.* at 315 (quoting 18 U.S.C. § 2703(d) (2006)) (internal quotation marks omitted).

13. *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 534 F. Supp. 2d 585, 586, 612, 616 (W.D. Pa. 2008) [hereinafter *CSI: Pittsburgh*], *aff'd*, No. 07-524M, 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008), *vacated*, 620 F.3d 304 (3d Cir. 2010).

14. *See generally ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 81–85 & n.14 (2010) [hereinafter *June Hearings*] (statement of Stephen Wm. Smith, U.S. Mag. J.) (summarizing inconsistent decisions), *available at* http://judiciary.house.gov/hearings/printers/111th/111-109_57082.pdf; *Electronic Communications Privacy Act Reform: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 29 (2010) [hereinafter *May Hearings*] (statement of Albert Gidari, Partner, Perkins Coie LLP) (testifying about inconsistent decisions among magistrate judges within the same judicial district).

judges retain the *option* to impose a warrant requirement on government agents who seek location data *or* may instead permit them to satisfy the less demanding statutory standard before obtaining an order compelling disclosure.[15] The majority remanded the case to the magistrate judge who had first considered the government's application with instructions to choose the appropriate standard, warrant or D order, and then to determine whether the government's application satisfied the chosen requirement.[16] The court also directed the magistrate judge to make factual findings and provide an explanation if she demands a warrant.[17]

The Third Circuit construed the statute to permit magistrate judges to demand a warrant in appropriate cases but did not go further to find that the Fourth Amendment requires a warrant in all cases in which law enforcement seeks location data.[18] The majority, however, did address the Fourth Amendment by rejecting the government's argument that either a broad "third party" rule from *United States v. Miller*[19] or a broad "non-contents" rule from *Smith v. Maryland*[20] resolved the case in the government's favor.[21] As one of the very few federal appellate decisions to consider reasonable expectations of privacy in new communication technologies, the majority's constitutional reasoning should prove significant and influential.[22]

At the same time, and more in dicta, the majority narrowly construed the protection offered by a pair of Supreme Court cases from the 1980s, which considered how the Fourth Amendment regulates the use of tracking radios placed in cars or on their bumpers ("bumper-beepers").[23] Although the court remanded to the magistrate judge to determine whether the government's demand for loca-

15. *CSI: Third Circuit*, 620 F.3d at 319.

16. *Id.*

17. *Id.*

18. *Id.* Interestingly, a magistrate judge in the Southern District of Texas ruled on the constitutional question six weeks later. *In re* Application of the U.S. for Historical Cell Site Data, Nos. H-10-998M et al., 2010 WL 4286365, at *14 (S.D. Tex. Oct. 29, 2010) [hereinafter *CSI: Houston III*] ("Compelled warrantless disclosure of cell site data violates the Fourth Amendment . . . ."); *see also infra* note 385. R

19. 425 U.S. 435, 444 (1976) (holding that a defendant's Fourth Amendment interests were not implicated when a subpoena was issued to his bank to obtain records of his banking activity).

20. 442 U.S. 735, 741–42, 745 (1979) (finding that a defendant has no reasonable expectation of privacy in phone numbers dialed).

21. *CSI: Third Circuit*, 620 F.3d at 317–18.

22. *See infra* text accompanying notes 118–23. R

23. *See CSI: Third Circuit*, 620 F.3d at 312–13 (discussing *United States v. Knotts*, 460 U.S. 276 (1983), and *United States v. Karo*, 468 U.S. 705 (1984)). Although the electronic tracking device beepers are not always attached to bumpers, they have been commonly referred

tion data intruded on reasonable expectations of privacy, the majority's language indicated that only if the records yielded information about the inside of the targets' home or curtilage would the investigation implicate the Fourth Amendment.[24] While the majority's language recognized that location data acquisition could intrude on reasonable expectations of privacy either directly or by permitting inferences, the court failed to recognize that even outside-the-home information can implicate Fourth Amendment rights. By contrast, in *United States v. Maynard*,[25] issued just three weeks before *CSI: Third Circuit*, the D.C. Circuit held that law enforcement use of a global positioning system ("GPS") tracking device on a car to obtain location information represents "prolonged surveillance" that requires a warrant under the Fourth Amendment.[26] The D.C. Circuit recognized that a GPS device reveals patterns of activity and permits the creation of an intimate picture of the target's life, whether or not such information yields insights or inferences about the inside of the target's home.[27] The Third Circuit's more cabined view of Fourth Amendment protection surely explains much of the court's reluctance to decide that a warrant is required in all cases of cell-site location surveillance.[28]

In fact, the majority in *CSI: Third Circuit* might claim that even if it had been inclined to resolve the constitutional question more broadly, the statutory interpretation doctrine of constitutional avoidance advises against deciding the case on constitutional grounds where another plausible interpretation is available.[29] Because the majority found a statutory way to resolve the conflict,[30] the judges may contend that one need no further explanation for their failure to

---

to as "bumper-beepers." *See* Margaret B. Gramoglia, Comment, *Electronic Tracking Devices and the Fourth Amendment*—United States v. Michael, 16 GA. L. REV. 197, 197 n.3 (1981).

24. *CSI: Third Circuit*, 620 F.3d at 312–13. The concurrence clarified that rule, but presumably could not get the other judge (or judges) to include that language directly in the majority opinion. *Id.* at 320 (Tashima, J., concurring).

25. 615 F.3d 544 (D.C. Cir.), *cert. denied*, 131 S. Ct. 671 (2010).

26. *Id.* at 562–63, 568.

27. *Id.* at 563; *see also CSI: Houston III*, Nos. H-10-998M et al., 2010 WL 4286365, at *14 (S.D. Tex. Oct. 29, 2010) (following *Maynard* and denying warrantless requests for location data as in violation of the Fourth Amendment); *CSI: Brooklyn*, 736 F. Supp. 2d 578, 581–85 (E.D.N.Y. 2010) (applying the *Maynard* approach to location data obtained from cell phones), *rev'd*, Order, *CSI: Brooklyn*, 736 F. Supp. 2d 578 (E.D.N.Y. Nov. 29, 2010), ECF No. 11.

28. *See CSI: Third Circuit*, 620 F.3d at 312–13 ("The *Knotts/Karo* opinions make clear that the privacy interests at issue are confined to the interior of the home.").

29. *See, e.g.*, Edward J. DeBartolo Corp. v. Fla. Gulf Coast Building & Constr. Trades Council, 485 U.S. 568, 575 (1988) ("'[E]very reasonable construction must be resorted to, in order to save a statute from unconstitutionality.'" (quoting Hooper v. California, 155 U.S. 648, 657 (1895))).

30. *CSI: Third Circuit*, 620 F.3d at 319.

more directly address the Fourth Amendment question. The author of the majority opinion indicated at oral argument that she had no intention of reaching the constitutional question when the case could be decided on statutory grounds.[31] The concurring judge on the panel, however, faulted the other two judges for asking the magistrate judge to determine whether a warrant was required without sufficient guidance about the Fourth Amendment's requirements.[32] With a few exceptions,[33] magistrate judges seem hesitant to conduct the constitutional analysis themselves and express the need for the authority and uniformity that an appellate decision would provide.[34]

Beyond *CSI: Third Circuit*, the lack of clear guidance on Fourth Amendment questions creates significant problems. Because of the good faith rule, discussed above,[35] the absence of privacy-protective decisions permits the executive branch to conduct intrusive online surveillance effectively free of constitutional constraints.[36] Those privacy-invading practices will continue until either the courts step up or

31. *See* Oral Argument at 30:30–31:00, *CSI: Third Circuit*, 620 F.3d 304 (No. 08-4227), *available at* http://www.ca3.uscourts.gov/oralargument/audio/08-4227-ApplicationofUSA.wma (Judge Sloviter indicating that she has "set aside the Constitution" in recognition of the need to decide the case on statutory grounds if possible); *see also id.* at 3:55–4:05 (Judge Sloviter noting the obligation to make a decision based on the statute if possible). The other judge in the majority, Judge Roth, was absent from the oral argument, so she expressed no opinion on her preference, if any, for statutory resolution.

32. *CSI: Third Circuit*, 620 F.3d at 319–20 (Tashima, J., concurring) ("I do not believe that these contradictory signals give either magistrate judges or prosecutors any standards by which to judge whether an application for a [D order] is or is not legally sufficient.").

33. *See CSI: Houston III*, Nos. H-10-998M et al., 2010 WL 4286365, at *6–14 (S.D. Tex. Oct. 29, 2010) (finding, in a comprehensive opinion, that warrantless acquisition of location data violates the Fourth Amendment); *CSI: Brooklyn*, 736 F. Supp. 2d 578, 582–95 (E.D.N.Y. 2010) (carefully analyzing cell phone users' expectations of privacy), *rev'd*, Order, *CSI: Brooklyn*, 736 F. Supp. 2d 578 (E.D.N.Y. Nov. 29, 2010), ECF No. 11. Even the magistrate judge in *CSI: Pittsburgh*, whose decision covered more than thirty reporter pages and was joined by four other magistrate judges, did not decide the Fourth Amendment question definitively, but instead concluded that permitting warrantless access to location data would "raise[ ] serious Fourth Amendment concerns" and so construed the statute to avoid it. *CSI: Pittsburgh*, 534 F. Supp. 2d 585, 616 (W.D. Pa. 2008) (quoting *In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 765 (S.D. Tex. 2005) [hereinafter *CSI: Houston I*]), *aff'd*, No. 07-524M, 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008), *vacated*, 620 F.3d 304 (3d Cir. 2010).

34. *See, e.g.*, *CSI: Houston I*, 396 F. Supp. 2d at 765 (urging the government to appeal the decision on cell site location so that a higher court can provide more authoritative guidance on this important matter); *see also June Hearings*, *supra* note 14, at 83 n.14 (statement of Stephen Wm. Smith, U.S. Mag. J.) ("Unfortunately, with a single exception in five years, [the plea in *CSI: Houston I*] has fallen on deaf ears."). R

35. *See supra* text accompanying notes 5–6. R

36. In other words, the executive branch behaves in ways I believe violate the Fourth Amendment, but no clear precedent effectively constrains executive branch investigative practices. *But see* United States v. Warshak, 631 F.3d 266, 289 n.17 (6th Cir. 2010) (noting that in light of the decision finding the statutory provision unconstitutional, "the good-

Congress steps in to revise the ECPA. As Congress currently considers reform of the surveillance laws, individual members have indicated an unwillingness to rein in law enforcement powers significantly or inhibit national security protection.[37] Historically, Congress has dragged its heels in protecting communications privacy until the courts have demanded it.[38] Congress spent over a decade convening hearings about the need to regulate wiretapping but did not pass the Wiretap Act until 1968, just after the Supreme Court decided two cases in 1967 that announced explicit Fourth Amendment requirements for the practice.[39] Until the federal appellate courts clarify how the Fourth Amendment regulates new communication technologies, Congress will not feel constitutional constraints.[40] Quite the contrary, Congress will hear regularly from executive branch officials that new technologies lack Fourth Amendment protection entirely.[41]

---

faith calculus has changed, and a reasonable officer may no longer assume that the Constitution permits warrantless searches of private emails").

37. *See, e.g.*, Memorandum on the Elec. Commc'ns Privacy Act: Promoting Privacy in the Digital Age from Senate Judiciary Comm. Minority Staff 9 (Sept. 17, 2010) (on file with the Maryland Law Review) [hereinafter Minority Staff Memorandum] ("A probable cause standard for retrospective information would devastate law enforcement's ability to use this data, which is critical for the investigation and prosecution of serious offenses such as drug smuggling.").

38. Prior to the passage of the Wiretap Act in 1968, some believed that without Supreme Court guidance, Congress would never act. *See, e.g.*, Yale Kamisar, *The Wiretapping-Eavesdropping Problem: A Professor's View*, 44 MINN. L. REV. 891, 924 (1960) ("Until the High Court is heard from, the whole area of wiretapping and federal-state relations must be regarded as quite unsettled."); Edward Bennett Williams, *The Wiretapping-Eavesdropping Problem: A Defense Counsel's View*, 44 MINN. L. REV. 855, 870 (1960) ("Experience has demonstrated the difficulty of obtaining adequate legislation. If there is to be reform, it must begin with the courts.").

39. Freiwald, *Online Surveillance*, *supra* note 3, at 74–76 (describing the period leading up to passage of the Wiretap Act). R

40. Indeed, unless the Fourth Amendment applies, congressional legislators may view any protection they give to location data as entirely optional. *See, e.g.*, Minority Staff Memorandum, *supra* note 37, at 6 ("[The Electronic Communications Privacy Act's] current provisions already go far beyond those required by the Fourth Amendment to protect the privacy interests of users of telecommunications services, a point which is rarely acknowledged by supporters of ECPA changes."). It is not clear whether the Third Circuit majority agreed with that view when it wrote, "[C]onsiderations for and against a [probable cause] requirement would be for Congress to balance." *CSI: Third Circuit*, 620 F.3d 304, 319 (3d Cir. 2010). If so, that would seem to contradict other parts of the decision where the majority recognized the possibility of location data investigations violating the Fourth Amendment. *See, e.g.*, *CSI: Third Circuit*, 620 F.3d at 318 (discussing the need to consider language in *Karo* in which the Supreme Court discussed the need for "'Fourth Amendment oversight'" (quoting United States v. Karo, 468 U.S. 705, 716 (1984))). In those cases, courts could overturn any congressional balancing if not sufficiently cognizant of Fourth Amendment interests. R

41. *See, e.g.*, *June Hearings*, *supra* note 14, at 62 (statement of Richard Littlehale, Assistant Special Agent in Charge, Technical Services Unit, Tennessee Bureau of Investigation) R

The Third Circuit panel must have been aware of the costs of declining to provide a definitive Fourth Amendment ruling. In addition to the Supreme Court's narrow view of the bumper-beeper cases, I believe that two other factors contributed to the Third Circuit's reluctance to address the Fourth Amendment directly. First, determining reasonable expectations of privacy is challenging, at best,[42] particularly in the context of new communications technology. Lower courts have tended to avoid conducting a full-scale expectations-of-privacy analysis by resorting to the same analytical short cuts[43] that the government urged the Third Circuit to use.[44] As mentioned, the majority declined the government's invitation to reverse the lower courts by simply characterizing the location records as unprotected "non-contents data" or "third party records."[45] Second, which proved to be more of a stumbling block, the court was uncertain about the scope and power of location information. *CSI: Third Circuit* bears obvious similarities to the Supreme Court's June 2010 decision in *City of Ontario v. Quon*.[46] Although the *Quon* Court assumed it, the Court refused to actually determine whether users have a reasonable expectation of privacy in their text messages, observing that "[t]he judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."[47] The Third Circuit seemed to share a similar concern that it may be too early to say whether location data implicates the Fourth Amendment, although for the majority, the problem was that the record was

---

(noting that the ECPA grants more privacy than needed to "communications records"); *Anti-Terrorism Investigations and the Fourth Amendment After September 11, 2001: Hearing Before the Subcomm. on the Constitution of the H. Comm. on the Judiciary*, 108th Cong. 12 (2003) (statement of Viet D. Dinh, Assistant Att'y Gen. for the Office of Legal Policy, Dep't of Justice) *available at* http://ftp.resource.org/gpo.gov/hearings/108h/87238.pdf (describing how some of the procedural requirements in the ECPA, although they do not include a warrant, notice, civil remedy or suppression remedy, "exceed those imposed by the Fourth Amendment").

42. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 34 (2001) (suggesting the *Katz* test "has often been criticized as circular, and hence subjective and unpredictable"); Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 383–86 (1974) ("[*Katz*] offers neither a comprehensive test of fourth amendment coverage nor any positive principles by which questions of coverage can be resolved.").

43. Freiwald, *First Principles*, *supra* note 5, ¶¶ 36–49. R

44. *See CSI: Third Circuit*, 620 F.3d at 317–18 (discussing the government's arguments for a broad third-party rule); Brief for the United States at 11, 26–28, *CSI: Third Circuit*, 620 F.3d 304 (No. 08-4227), 2009 WL 3866618.

45. *See supra* text accompanying notes 19–21. R

46. 130 S. Ct. 2619 (2010).

47. *Id.* at 2629. The Court went on to question whether it had the knowledge and experience with text messages that the Court had in 1967 regarding telephone conversations. *Id.*

incomplete.[48] As the chief counsel for Microsoft told Congress a few weeks after the Third Circuit's decision, however, if the courts take too long to address new technology, they create the risk not only that the technology they do address will be obsolete but also "that the Fourth Amendment will never really catch up."[49]

In this Article, I will address three hurdles to federal appellate resolution of the Fourth Amendment question in the location privacy cases: (1) concern about the novelty of the technology and lack of experience with its use as a surveillance tool,[50] (2) an unduly constrained view of the bumper-beeper cases as protecting only information about activities inside the home and curtilage,[51] and (3) the inordinate appeal of short cuts (the non-contents and third party rules) to a meaningful reasonable expectation of privacy analysis.[52] Although the majority resisted taking analytical short cuts in *CSI: Third Circuit*, the government has achieved some success with them and continues to champion the short cuts in other cases.[53] These three hurdles will continue to inhibit Fourth Amendment resolution of location data cases. Moving past these hurdles undoubtedly will benefit resolution of related cases and provide the much needed constitutional guidance that only the courts can provide.

In Part II, I will provide more background about the *CSI: Third Circuit* case, including what makes it unusual. Part III will elaborate on location data technology; it will describe what location data records may contain and how powerfully that information intrudes into our private lives. Part IV will discuss the bumper-beeper cases and will argue that, given the richness of location information, the *Maynard* court articulated a more defensible understanding of how the bumper-beeper precedents apply. Under a proper understanding

48. *See CSI: Third Circuit*, 620 F.3d at 312 ("We see no need to decide [whether the location information could encroach upon reasonable expectations of privacy] without a factual record on which to ground the analysis."); *id.* at 318 ("The record does not demonstrate whether [locating cell phones within a relatively small area] can be accomplished with present technology, and we cannot predict the capabilities of future technology.").

49. *See* Audio File: Hearing Before S. Comm. on the Judiciary, The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age, at 88:30–89:10 (2010) [hereinafter *September Senate Hearings*] (oral statement of Brad Smith, Esq., General Counsel of Microsoft Corporation), *available at* http://www.senate.gov/fplayers/CommPlayer/commFlashPlayer.cfm?fn=judiciary092210&st=xxx.

50. *See infra* Part III.

51. *See infra* Part IV.

52. *See infra* Part V.

53. *See, e.g.*, United States v. Benford, No. 2:09 CR 86, 2010 WL 1266507, at *3 (N.D. Ind. Mar. 26, 2010) (finding no Fourth Amendment interest in location data because it was voluntarily turned over to a third party); United States v. Suarez-Blanca, No. 1:07-CR-0023-MHS/AJB, 2008 WL 4200156, at *9 (N.D. Ga. Apr. 21, 2008) (same).

of the Fourth Amendment, magistrate judges should require warrants based on probable cause for location data in all cases, notwithstanding language by the Third Circuit that suggested such power should be exercised "sparingly."[54] Part V will argue that the Third Circuit properly rejected application of the *Smith* and *Miller* precedents to location data because acquisition of that data violates reasonable expectations of privacy. I will also briefly articulate a modified approach to the reasonable expectations of privacy analysis that considers the nature of the surveillance itself and the associated need for close judicial supervision.[55] I will conclude that courts should decide, based on constitutional law, that applications for location data must satisfy the probable cause standard of the warrant requirement. As a result, and contrary to the majority in *CSI: Third Circuit*, magistrate judges should require government applicants to obtain a warrant based on probable cause as a matter of law, and not as a matter of fact after "balanc[ing] the Government's need (not merely desire) for the information with the privacy interests of cell phone users."[56]

II. BACKGROUND OF *CSI: THIRD CIRCUIT*

The litigation began in November 2007, when the government applied for a court order to compel a cellular phone service provider to turn over its location data records for a particular subscriber ("target").[57] In an opinion joined by four other magistrate judges, a magistrate judge in the Western District of Pennsylvania denied the application because the federal agents had not furnished probable cause for a warrant.[58] Instead, applicants had sought to satisfy only the less demanding D order standard of the Stored Communications Act ("SCA"),[59] which is applicable to non-contents records of an elec-

54. *See CSI: Third Circuit*, 620 F.3d 304, 319 (3d Cir. 2010) (describing the choice to require a warrant as "an option to be used sparingly because Congress also included the option of a [D] order.").

55. *See* Freiwald, *First Principles*, *supra* note 5, ¶¶ 71–76 (applying the four factor test to stored e-mail content data). R

56. *CSI: Third Circuit*, 620 F.3d at 319.

57. Brief for the United States, *supra* note 44, at 4. R

58. *CSI: Pittsburgh*, 534 F. Supp. 2d 585, 616 (W.D. Pa. 2008), *aff'd*, No. 07-524M, 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008), *vacated*, 620 F.3d 304 (3d Cir. 2010). Inconsistency among individual magistrate judges within jurisdictions has made it difficult for service providers to know how to comply with the law. *See May Hearings*, *supra* note 14, at 29 (statement of Albert Gidari, Partner, Perkins Coie LLP) ("[T]he proper legal standard [for access to location information] is more confusing when federal magistrates sitting in the same federal district in a state disagree . . . [.]"). R

59. 18 U.S.C. §§ 2701–12 (2006). The SCA is the second of three titles of the ECPA. Pub. L. No. 99-508, sec. 201, 100 Stat. 1848, 1860–68 (1986).

tronic communication service provider.[60] In fact, the magistrate judge found that the non-contents records provision of the SCA, which applies to "a record or other information pertaining to a subscriber to or customer of [an electronic communication] service,"[61] did not cover location data. The court first explained that the definition of "electronic communications" specifically excludes information obtained from a "tracking device."[62] It further reasoned that cell phones qualify as a kind of "tracking device," thus prohibiting the collection of cell phone generated location data under a D order.[63] The magistrate judge found that the authority to compel location data must come from outside the SCA.[64] In so finding, the court joined other courts that have imposed the warrant requirement of Rule 41 of the Federal Rules of Criminal Procedure ("Rule 41"), in part to avoid Fourth Amendment problems.[65] The government appealed that denial to the district court, arguing that the magistrate judge was required to grant the application if she found the D Order requirements met.[66]

---

60. *CSI: Pittsburgh*, 534 F. Supp. 2d at 588–89 (citing 18 U.S.C. § 2703(c)).

61. 18 U.S.C. § 2703(c).

62. *CSI: Pittsburgh*, 534 F. Supp. 2d at 601; *see also* 18 U.S.C. § 2510(12)(C) (excluding "any communication from a tracking device" from the definition of "electronic communication").

63. *CSI: Pittsburgh*, 534 F. Supp. 2d at 602–03 & n.44; *see also* 18 U.S.C. § 3117(b) (defining "tracking device" as "an electronic or mechanical device which permits the tracking of the movement of a person or object").

64. *CSI: Pittsburgh*, 534 F. Supp. 2d at 607.

65. *Id.* at 616 ("'Absent any sign that Congress has squarely addressed and resolved those concerns in favor of law enforcement, the more prudent course is to avoid an interpretation that risks a constitutional collision.'" (quoting *CSI: Houston I*, 396 F. Supp. 2d 747, 765 (S.D. Tex. 2005))). The court noted that Rule 41 had traditionally been used to authorize tracking device investigations. *Id.* at 592. Congress amended Rule 41 in 2006 specifically to include tracking devices. *Id.*; *see also* FED. R. CRIM. P. 41(f)(2) Committee Notes on Rules—2006 Amendment. The magistrate judge's decision did not specify whether such orders would include notice to the target or what other remedies would be available for improper investigations. One recent decision, however, has asserted that the government must furnish notice to the target, not merely to the provider, to comply with the tracking device provisions of Rule 41. *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) [hereinafter *CSI: Austin*] (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))).

66. *See* Gov't Memorandum of Law in Support of Request for Review at 5–8, *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008) (No. 07-524M), 2008 WL 3861765 [hereinafter *CSI: Intermediate*] (arguing that the plain language of the statute compels the court to reverse the magistrate judge's holding).

As arguably permitted by the SCA,[67] the government had not provided notice to the target of the investigation.[68] Interestingly, the target whose records the government sought was not actually the suspect of a crime but rather someone whose cell phone had been used by a suspect in a narcotics investigation.[69] Obviously, the target could not mount an opposition to the government's demand for her location data when she had no idea it had taken place; the application was under seal and the provider was not permitted to inform her.[70] Rather than hear arguments only from the government, the district court took the unusual, but not unprecedented,[71] step of inviting briefs from those who would oppose the government's application. In particular, the court invited briefing from the Electronic Frontier Foundation ("EFF"),[72] an online civil liberties activist group that represented several other similar groups ("Civil Liberties Amici");[73] the

67. *CSI: Third Circuit*, 620 F.3d 304, 307 (3d Cir. 2010) (explaining that notice is not required under the statute (citing 18 U.S.C. § 2703(c)(3))). *But see In re* Sealing & Non-Disclosure of Pen/Trap/2703(D) Orders, 562 F. Supp. 2d 876, 886–87 (S.D. Tex. 2008) ("[E]lectronic surveillance gag orders of unlimited duration must be the exception rather than the rule."); *June Hearings*, *supra* note 14, at 87–90 & n.28 (statement of Stephen Wm. Smith, U.S. Mag. J.) (discussing the problem of imposing gag orders on service providers that are not justified by the SCA). R

68. *CSI: Third Circuit*, 620 F.3d at 307; *see also CSI: Pittsburgh*, 534 F. Supp. 2d at 586 (describing the cell phone service provider's disclosure of location information as "covert").

69. *CSI: Pittsburgh*, 534 F. Supp. 2d at 588 & n.11. I will refer to the subscriber whose location data the government sought using the female pronoun, and I will use the male pronoun to refer to targets in general.

70. *Id.* at 588; *see also* 18 U.S.C. § 2705(b) (permitting the government to request a nondisclosure order). *See generally* Crump & Calabrese, *supra* note 8 (discussing how the fact that almost all location data cases are under seal indefinitely and ex parte inhibits public knowledge of investigative practices). R

71. *See generally* Linda Sandstrom Simard, *An Empirical Study of Amici Curiae in Federal Court: A Fine Balance of Access, Efficiency, and Adversarialism*, 27 REV. LITIG. 669, 687 (2008) ("[W]hen judges perceive a need for additional information they will occasionally request amicus participation.").

72. *Cell Tracking*, ELECTRONIC FRONTIER FOUND., www.eff.org/issues/cell-tracking (last visited Mar. 26, 2011) (providing information about cases in which courts have invited EFF to counter government position). *See generally* Kevin S. Bankston, *Only the DOJ Knows: The Secret Law of Electronic Surveillance*, 41 U.S.F. L. REV. 589, 612–13 (2007) (describing cases in which magistrate judges and district courts had requested input from EFF on electronic surveillance cases).

73. Brief of Amici Curiae Electronic Frontier Foundation et al. in Opposition to the Government's Request for Review, *CSI: Intermediate*, 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008) (No. 07-524M), 2008 WL 3861767 [hereinafter Civil Liberties Amici, D.C. Brief]. The American Civil Liberties Union, the ACLU-Foundation of Pennsylvania, INC., and the Center for Democracy and Technology joined the EFF. *Id.*

public defender for the Western District of Pennsylvania;[74] and me, an academic with pertinent experience.[75] All three amici urged the district court to affirm the denial of the government's application,[76] which it did, without separate analysis, after considering all the submissions.[77]

When the government appealed to the Third Circuit, it repeated its claim that the Fourth Amendment does not apply to location data.[78] The government also argued that, as a matter of statutory law, magistrate judges must grant every government application for location data that satisfies the D order standard applicable to non-contents records.[79] The Civil Liberties Amici agreed with the government that the non-contents records provision applied to location data,[80] and rejected the lower courts' finding that, as data from a tracking

74. Brief of Amici Curiae Federal Public Defender in Opposition to the Government's Request for Review, *CSI: Intermediate*, 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008) (No. 07-524M), 2008 WL 3861768 [hereinafter Public Defender, D.C. Brief].

75. Brief of Amici Curiae Susan Freiwald in Favor of Affirmance, *CSI: Intermediate*, 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008) (No. 07-524M), 2008 WL 3861766 [hereinafter Freiwald, D.C. Brief]. At that time, I had written law review articles that had been cited in other location data cases. *See, e.g.*, *In re* Application of the U.S. for an Order Authorizing (1) Installation & Use of a Pen Register & Trap & Trace Device or Process, (2) Access to Customer Records, & (3) Cell Phone Tracking, 441 F. Supp. 2d 816, 826 n.20 (S.D. Tex. 2006) (citing Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act*, 69 S. CAL. L. REV. 949, 982–89 (1996) [hereinafter Freiwald, *Uncertain Privacy*]) (explaining that advances in technology should require the government to change its surveillance procedures); *In re* Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. and/or Cell Site Info., 396 F. Supp. 2d 294, 319 (E.D.N.Y. 2005) (same). The magistrate judge had also cited one of my articles. *See CSI: Pittsburgh*, 534 F. Supp. 2d at 586 n.7, 615 n.81 (citing Freiwald, *First Principles*, *supra* note 5); *see also* Susan Freiwald & Patricia L. Bellia, *The Fourth Amendment Status of Stored E-mail: The Law Professors' Brief in* Warshak v. United States, 41 U.S.F. L. REV. 559 (2007) (describing Fourth Amendment arguments I made with co-amicus in a stored e-mail case). R

76. *See* Civil Liberties Amici, D.C. Brief, *supra* note 73, at 3 ("[T]he Court can and must require the government to meet the requirements to obtain a Rule 41 warrant before issuing an order compelling the disclosure of stored CSLI."); Public Defender, D.C. Brief, *supra* note 74, at 1 ("Judge Lenihan's conclusion . . . is the only resolution of the issues . . . that can protect the privacy rights of all citizens . . . ."); Freiwald, D.C. Brief, *supra* note 75, at 1 (explaining that the Fourth Amendment requires the court to affirm the magistrate judge's ruling). R R R

77. *CSI: Intermediate*, 2008 WL 4191511, at *1 (holding that the magistrate judge's order was not clearly erroneous and therefore denying the government's appeal).

78. Brief for the United States, *supra* note 44, at 7. R

79. *Id.* at 10–14.

80. *Id.* at 9–13; Brief of Amici Curiae Electronic Frontier Foundation et al. in Support of Affirmance of the District Court at 1, *CSI: Third Circuit*, 620 F.3d 304 (3d Cir. 2010) (No. 08-4227), 2009 WL 3866619 [hereinafter Civil Liberties Amici, Third Circuit Brief].

device, the records fell outside that provision's purview.[81] For both sides, whether or not to characterize cell phones as tracking devices with regard to location data did not detract from the fact that cell phone providers provide electronic communications services, and that location data is contained in "records pertaining" to that service.[82] The Third Circuit eventually agreed.[83]

But while both sides agreed that law enforcement acquisition of location data proceeds under 18 U.S.C. § 2703(d) (the D order standard), they vehemently disagreed about what that standard means. The crucial language of 2703(d) reads,

> A court order for disclosure . . . may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the . . . records or other information sought, are relevant and material to an ongoing criminal investigation.[84]

The government argued that "shall issue" means that when an agent presents sufficient information to obtain a D order to the magistrate judge, the judge must grant the application for location data.[85] The Civil Liberties Amici, however, argued that "only if" meant that the "relevant and material" standard sets a floor for disclosure, and that judges could require more of a showing from the government, such as

---

81. Brief for the United States, *supra* note 44, at 9–13, 16–23; Civil Liberties Amici, Third Circuit Brief, *supra* note 80, at 2 n.1 (finding the "tracking device" question irrelevant). I will not analyze this argument except to note that many magistrate judges have agreed that location data does not fall under the non-contents provision of the SCA. *See, e.g.*, *CSI: Austin*, 727 F. Supp. 2d 571, 578 (W.D. Tex. 2010) ("The definition contained in [18 U.S.C.] § 3117, and incorporated into FED. R. CRIM. P. 41, compels the conclusion that a cell phone is a tracking device when it is used to locate a person and track their movements."); *CSI: Pittsburgh*, 534 F. Supp. 2d 585, 602 n.44 (W.D. Pa. 2008) (collecting cases), *aff'd*, No. 07-524M, 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008), *vacated*, 620 F. 3d 304 (3d Cir. 2010). R R

82. *See* Brief for the United States, *supra* note 44, at 26–27; Civil Liberties Amici, Third Circuit Brief, *supra* note 80, at 2 & n.1, 7. R R

83. *CSI: Third Circuit*, 620 F.3d 304, 307–08 (3d Cir. 2010) ("[T]here is no dispute that historical CSLI is a 'record or other information pertaining to a subscriber . . . or customer,' and therefore falls within the scope of § 2703(c)(1)." (alteration in original) (quoting 18 U.S.C § 2703(c)(1) (2006))).

84. 18 U.S.C. § 2703(d).

85. Brief for the United States, *supra* note 44, at 10 & n.9. The federal public defender raised the question in its amici brief of whether the government had even satisfied the D order standard in its original application. *See* Public Defender, D.C. Brief, *supra* note 74, at 11 n.6 (suggesting that, "irrespective of the standard to be applied," the court should require the Government to furnish "a more precise description" of the location data sought). R R

probable cause, when needed.[86] Both sides supported their arguments with a detailed analysis of the statutory text[87] and legislative history.[88]

The Civil Liberties Amici urged the Third Circuit to construe the statute as permitting magistrate judges to require probable cause in some cases in order to avoid serious constitutional questions that would be raised otherwise.[89] Alternatively, the Civil Liberties Amici argued that, were the Third Circuit to address the constitutional question, it should hold that government acquisition of location data intrudes on an individual's reasonable expectations of privacy, implicates the Fourth Amendment, and requires the protections of the warrant requirement.[90] But the Civil Liberties Amici emphasized that the doctrine of constitutional avoidance should compel the court to avoid the necessity of such a ruling.[91]

I did not address how to construe the statute in my brief to the Third Circuit.[92] Instead, I argued that the Fourth Amendment requires government agents to obtain at least a warrant based on probable cause whenever they seek location data because those demands are searches under the Fourth Amendment that intrude on targets' reasonable expectations of privacy.[93]

As this brief synopsis illustrates, the interaction of statutory interpretation and constitutional analysis may make *CSI: Third Circuit* seem

86. Civil Liberties Amici, Third Circuit Brief, *supra* note 80, at 4 ("By choosing the phrase 'only if' rather than simply 'if' . . . Congress made clear that a court *may* issue but is not *required* to issue a D Order when the Government has made its specific and articulable facts showing."). R

87. *See* Brief for the United States, *supra* note 44, at 9–14 (arguing that the language of 18 U.S.C. § 2703 "unambiguously" grants the government the authority to request cell user location information and no other statute limits that power); Civil Liberties Amici, Third Circuit Brief, *supra* note 80, at 4–7 (arguing that the plain language and the "Rule Against Superfluities" require a permissive reading of the statute). R R

88. *See* Brief for the United States, *supra* note 44, at 11–12; Civil Liberties Amici, Third Circuit Brief, *supra* note 80, at 7–8. R R

89. Civil Liberties Amici, Third Circuit Brief, *supra* note 80, at 9–13 ("[I]f the Court adopts the Government's mandatory reading, it will run headlong into serious constitutional questions affecting the rights of every cell phone user."). R

90. *Id.* at 13–22.

91. *See id.* at 11–12 ("[W]hen deciding which of two plausible statutory constructions to adopt, *a court must consider the necessary consequences of its choice.* If one of them would raise a multitude of constitutional problems, the other should prevail . . . ." (alteration in original) (emphasis added) (quoting Clark v. Martinez, 543 U.S. 371, 380–81 (2005))).

92. Brief of Amicus Curiae Susan Freiwald in Support of Affirmance, *CSI: Third Circuit*, 620 F.3d 304 (3d Cir. 2010) (No. 07-524M) [hereinafter Freiwald, Third Circuit Brief]. The public defender did not file a brief in *CSI: Third Circuit*.

93. *Id.* at 2–13.

unreasonably complex.[94] The core issue the case raises, however, remains: What procedural hurdle(s) must government investigators overcome before they may compel a cell phone service provider to disclose location data? To summarize, the government and two amici suggested three ways to decide the case. Under the government's view, magistrate judges *must* use the specific and articulable facts standard of Section 2703(d) of the SCA and are not permitted to require that government agents make more of a showing before granting orders for location data. Under the Civil Liberties Amici view, magistrate judges *may* impose the D order standard but *may* require the government to satisfy the more demanding probable cause warrant standard when needed. Under my view, which closely tracked the lower courts' view, magistrate judges *must* require agents to satisfy the probable cause warrant standard before they may grant orders compelling disclosure of location data. As discussed, the majority in *CSI: Third Circuit* chose the middle path, adopting the Civil Liberties Amici's reasoning and holding that magistrate judges retain the discretion, as a matter of statutory construction, to choose which standard to require.[95]

Before turning to the nature of location data, it makes sense to understand what difference the standard makes, and what makes this case different from prior cases. Under a probable cause standard, the information sought must itself be evidence of a crime.[96] Some courts, however, have construed the probable cause requirement more broadly, finding the standard met when the target's phone is used in committing a crime or the target is to be arrested.[97] Under a D order standard, however, the government may seek any information that is materially relevant to an ongoing investigation. That would seem to

94. *See* Orin Kerr, *Third Circuit Rules That Magistrate Judges Have Discretion to Reject Non-Warrant Court Order Applications and Require Search Warrants to Obtain Historical Cell-Site Records*, VOLOKH CONSPIRACY (Sept. 8, 2010, 2:23 PM), http://volokh.com/2010/09/08/third-circuit-rules-that-magistrate-judges-have-discretion-to-reject-court-order-application-and-require-search-warrants-to-obtain-historical-cell-site-records/ (describing it as "quite tricky" to understand what the Third Circuit meant, and coming to a different conclusion than this Article based on a different analysis of the Fourth Amendment precedents).

95. *CSI: Third Circuit*, 620 F.3d at 319 ("[T]he statute as presently written gives the [magistrate judge] the option to require a warrant showing probable cause . . . .").

96. *See, e.g.*, *In re* Application of the U.S. for an Order Authorizing the Release of Prospective Cell Site Info., 407 F. Supp. 2d 134, 135 (D.D.C. 2006) [hereinafter *CSI: DC*] (noting a difference in the standards because probable cause requires a finding that the information sought is itself evidence of a crime rather than relevant and material to the investigation).

97. *See CSI: Austin*, 727 F. Supp. 2d 571, 581–84 (W.D. Tex. 2010) (expressing skepticism about some of the alternative interpretations of probable cause in other location data contexts).

permit acquisition of location data that will not yield evidence of crime but that instead will yield information that will aid the investigation.[98] The D order standard, then, permits much broader inquiries into a much wider range of targets. As mentioned, the target in *CSI: Third Circuit* was not herself a suspect of a crime.[99] According to the magistrate judge's opinion, the target of the application was the subscriber of a cell phone apparently "used by" the suspect in a criminal investigation, but the government "provid[ed] no specific information connecting these two individuals, or connecting the Criminal Suspect to the [target's] cell phone."[100] The target may have been a friend or associate of the criminal suspect or even someone whose phone the suspect had stolen and used.[101] Perhaps the government sought her location information to yield other suspects or to learn more about their activities, but not because the location information would itself yield evidence of a crime. Under the lower D order standard, the government has apparently conducted wide-ranging inquiries that have yielded location data for a large number of suspects.[102] Although the ex parte and sealed nature of the government's requests make understanding the full scope of such inquiries impossible,[103] anecdotal evi-

98. *See CSI: Brooklyn*, 736 F. Supp. 2d 578, 584 (E.D.N.Y. 2010) (discussing the use of D Orders to gain evidence that will merely lead to other evidence), *rev'd*, Order, *CSI: Brooklyn*, 736 F. Supp. 2d 578 (E.D.N.Y. Nov. 29, 2010), ECF No. 11; *see also CSI: Austin*, 727 F. Supp. 2d at 585 (rejecting the government's application because "tracking [the cell] phones would [not] result in the discovery of evidence of a crime" and would only "'help yield relevant evidence in this case.'").

99. *See CSI: Pittsburgh*, 534 F. Supp. 2d 585, 588 & n.11 (W.D. Pa. 2008) (explaining that the government sought her information "on the basis of its asserted relevance to an ongoing criminal investigation of another individual"), *aff'd*, No. 07-524M, 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008), *vacated*, 620 F. 3d 304 (3d Cir. 2010).

100. *Id.* at 588 n.11.

101. Would the magistrate judge have a basis to object if the information sought was nonetheless relevant?

102. *See* Crump & Calabrese, *supra* note 8, at 5 (describing a recent case in which the FBI sought and received tracking information, without a warrant, for 180 people in addition to the criminal defendant); *see also id.* at 6–7 (describing a cell phone provider's website dedicated to automatically providing law enforcement agents access to location data records (citing Michael Isikoff, *The Snitch in Your Pocket*, NEWSWEEK, Feb. 19, 2010, http://www.newsweek.com/2010/02/18/the-snitch-in-your-pocket.html)). R

103. *See In re* Sealing & Non-Disclosure of Pen/Trap/2703(d) Orders, 562 F. Supp. 2d 876, 894–95 (S.D. Tex. 2008) (limiting sealing of an order to 180 days, with possible renewal, so as not to violate the public's First Amendment right of access); *May Hearings*, *supra* note 14, at 32–33 (statement of Albert Gidari, Partner, Perkins Coie LLP) (expressing the need for transparency regarding government practices so the public "can assert their rights"); Stephen Wm. Smith, *Kudzu in the Courthouse: Judgments Made in the Shade*, 3 FED. CTS. L. REV. 177, 208–12 (2009) (discussing the need for public knowledge of electronic surveillance cases and explaining that these cases have improperly remained under seal indefinitely). R

dence suggests that use of the lower standard has facilitated much more information gathering than the probable cause warrant standard would permit. Such fishing expeditions run directly counter to the Fourth Amendment's core concern, which is preventing the use of intrusive investigative techniques to obtain information about those upon whom insufficient suspicion has fallen.[104] Secret investigations of those who will never find out because they will never be charged with a crime also clearly violate due process.[105]

While many prior cases have addressed government access to location data, most of them have concerned prospective data rather than historical data.[106] Over the last few years, dozens of federal district courts have considered what procedural hurdles govern law enforcement compulsion of real-time or prospective location data from cell phone service providers.[107] While some cases have permitted law enforcement access to the data without a warrant,[108] many have not, and have instead held that the Fourth Amendment requires a warrant

104. *See, e.g.*, Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 801 (1994) (explaining that the core purpose of the Fourth Amendment is to enable only "reasonable" searches); Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 610–19 (1999) (explaining that the Framers' original intent was to prevent general warrants).

105. *See June Hearings*, *supra* note 14, at 88 (statement of Stephen Wm. Smith, U.S. Mag. J.) ("[W]hen searches are shrouded in permanent secrecy, as in most cases of electronic surveillance, due process becomes a dead letter." (footnote omitted)); Crump & Calabrese, *supra* note 8, at 5 (explaining that the current trend of sealing these orders violates the First Amendment and the common law right of access). R R

106. Despite this general trend, a few recent lower court cases have addressed historical location data. *Compare, e.g.*, *CSI: Houston III*, Nos. H-10-998M et al., 2010 WL 4286365, at *14 (S.D. Tex. Oct. 29, 2010) (finding a Fourth Amendment interest in location data), *and CSI: Austin*, 727 F. Supp. 2d 571, 579 (W.D. Tex. 2010) (same), *with* United States v. Benford, No. 2:09 CR 86, 2010 WL 1266507, at *3 (N.D. Ind. Mar. 26, 2010) (finding no Fourth Amendment interest), *and* United States v. Suarez-Blanca, No. 1:07-CR-0023-MHS/AJB, 2008 WL 4200156, at *9 (N.D. Ga. Apr. 21, 2008) (same).

107. *See June Hearings*, *supra* note 14, at 93–94 (statement of Stephen Wm. Smith, U.S. Mag. J.) (categorizing all reported cell site decisions according to type of information sought). R

108. These cases have required both a court order under 18 U.S.C. § 2703(d) and a pen register order under 18 U.S.C. § 3123, a combination which has been called a "hybrid" order. *See* Steven B. Toeniskoetter, *Preventing a Modern Panopticon: Law Enforcement Acquisition of Real-Time Cellular Tracking Data*, 13 RICH. J.L. & TECH. 16, 24, 29 (2007), http://law.richmond.edu/jolt/v13:4/article16.pdf (describing cases involving hybrid orders). Courts have generally specified that they base their approval on the government's representations that the information sought is narrowly constrained; they generally do not provide a mechanism to ensure that the information the providers furnish stays so constrained, and they provide no after-the-fact judicial review. See *infra* Part III.B.2 for a discussion of these rulings and an argument that courts should not defer to executive branch self-restraint in cases of electronic surveillance.

to obtain such forward-looking data.[109] Some have permitted agents to obtain forward-looking location data without a warrant but only when the data sought is sufficiently limited in scope.[110] Almost none have generated appellate decisions.[111] *CSI: Third Circuit* involved access to stored, or historical, data only.[112] Acquiring data out of storage rather than in real-time means that different statutory provisions apply, and a specific statutory prohibition against obtaining the data too easily does not govern.[113] The question is whether the distinction that the SCA makes when it treats stored data as less worthy of protection than data acquired in real-time is of *constitutional* significance. In other words, does the Fourth Amendment distinguish between stored and forward-looking data and deprive the former of the protection it affords the latter? The government says "yes," largely because historical data means data stored by a third party service provider.[114] As discussed, the *CSI: Third Circuit* majority rejected the government's claim, and I elaborate on my agreement with the Third Circuit in Part V.A.1.

CSI: Third Circuit also diverges from a line of cases involving access to the *contents* of e-mail and text messages stored with the service provider. In those cases, although the government sought stored, his-

---

109. *See June Hearings*, *supra* note 14, at 84 (statement of Stephen Wm. Smith, U.S. Mag. J.) ("Surveying the published opinions, it is fair to conclude that the majority held that probable cause is the appropriate standard for government access to prospective cell site information."). R

110. *See, e.g.*, *In re* Application of U.S. for an Order for Disclosure of Telecomms. Records & Authorizing the Use of a Pen Register & Trap & Trace, 405 F. Supp. 2d 435, 450 (S.D.N.Y. 2005) [hereinafter *CSI: SDNY*] ("If the Government seeks to obtain other information, it should provide additional briefing on why such information is permissible under the relevant authorities.").

111. An exception is *United States v. Forest*, 355 F.3d 942, 951 (6th Cir. 2004), *vacated sub nom.* Garner v. United States, 543 U.S. 1100 (2005).

112. 620 F.3d 304, 305 (3d Cir. 2010).

113. D orders may be used for historical data only because the statutory language refers to "records." 18 U.S.C. § 2703(d) (2006); *see also* Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1566–67 (2004) (discussing the broad range of information made accessible to law enforcement by the statutory language). Prospective data acquisition requires a pen register order. *See generally*, Toeniskoetter, *supra* note 108 (providing a thorough analysis of statutes and cases concerning access to location data in real time). R

114. Note that the government does not concede that prospective location data is constitutionally protected either, but it does consistently argue that historical data lacks such protection. For example, the government's standard application form specifies that by providing probable cause, "the Government does not concede that such cell site records . . . may only be obtained via a warrant issued on probable cause." Standard Affirmation in Support of Application, 2 n.1, *available at* http://www.aclu.org/pdfs/freespeech/18cellfoia_release_CRM-200800622F_06012009.pdf.

torical data, it sought the contents of communications rather than location data. Those contents are most directly analogous to words printed in letters or spoken in telephone calls, both of which receive strong constitutional protection.[115] Location information forms a weaker analogy to letters and phone calls, in large part because of its novelty. Letters display addressing information on the outside of the envelope and maintain the contents of the letter within. Traditional wire line telephone calls break down into telephone numbers dialed, the contents of the call, and limited other associated data.[116] But the location of each cell tower with which your cell phone communicates as you move from place to place (or stay in one place) creates an entirely new type of data that does not neatly tie to more traditional technologies.[117]

In recent years, federal appellate courts have addressed Fourth Amendment protection for the contents of messages in electronic storage. In *Warshak v. United States*,[118] the government asserted that a white collar criminal defendant had no reasonable expectation of privacy in several years' worth of e-mails stored with his e-mail service provider.[119] A panel of the Sixth Circuit rejected the government's claim and held instead that the government generally needed to obtain a warrant to compel disclosure of the e-mails because the defendant retained a reasonable expectation of privacy in them, notwithstanding their storage with a third party.[120] Although the Sixth Circuit en banc vacated the panel's decision and held that Warshak lacked standing to obtain an injunction,[121] the court revisited the

115. *See* Katz v. United States, 389 U.S. 347, 352–53 (1967) (holding that the Fourth Amendment protects telephone calls); *Ex parte* Jackson, 96 U.S. 727, 733 (1877) (finding that the Fourth Amendment protects sealed letters).

116. *See generally* Freiwald, *Uncertain Privacy*, *supra* note 75 (discussing the different attributes associated with telephone calls and their legal treatment). R

117. For example, the government consistently calls location data "non-contents data," but that characterization is both too simplistic, see *infra* Part V.A.2, and in some cases, clearly wrong, see *May Hearings*, *supra* note 14, at 30 (statement of Albert Gidari, Partner, Perkins Coie LLP) (noting that for some applications, location information must be seen as "content" because "the user is conveying his or her location to another user essentially as a communication—'here I am'"). R

118. Warshak v. United States, 490 F.3d 455 (6th Cir. 2007), *vacated en banc*, 532 F.3d 521 (6th Cir. 2008).

119. *Id.* at 460–61, 478.

120. *Id.* at 480–82. Along with Professor Patricia L. Bellia, I submitted an amicus brief to the Sixth Circuit on behalf of Professors of Electronic Privacy Law and Internet Law. Brief for Professors of Electronic Privacy Law and Internet Law as Amici Curiae Supporting the Appellee and Urging Affirmance, *Warshak*, 490 F.3d 455 (No. 06-4092), 2006 WL 4670944; *see also* Freiwald & Bellia, *supra* note 75 (discussing *Warshak* and the amicus brief). R

121. *Warshak*, 532 F.3d at 523, 525–26 (vacating the judgment because Warshak's claim was "not ripe for judicial resolution"). The en banc court suggested that Warshak should

question after Warshak's trial and affirmed the first panel's finding that users' have a Fourth Amendment interest in stored e-mail.[122] Similarly, the Ninth Circuit's decision in *Quon v. Arch Wireless Operating Co.*, which the Supreme Court's subsequent decision reversed and remanded, found that Quon retained a reasonable expectation of privacy in the contents of his text messages stored with a service provider.[123]

As mentioned, the SCA, which is dramatically outdated by new technology, clearly distinguishes between content data and non-content records and imposes lower procedural hurdles on government access to the latter.[124] The question is whether the SCA's distinction is of *constitutional* significance. In other words, does the Fourth Amendment deprive non-content data of protection while affording protection to content data? The government says "yes," based on an overly broad reading of *Smith v. Maryland*, which withheld Fourth Amendment protection from the telephone numbers a target dialed.[125] The *CSI: Third Circuit* majority rejected the government's claim, and I elaborate on my agreement with the Third Circuit in Part V.A.2.

Instead of a short-cut version that relies either on a third-party rule or a non-contents rule, a full Fourth Amendment analysis must consider the reasonable expectations of privacy that cell phone users have in their location data.[126] That analysis requires an appreciation of (1) how precisely the data may identify where the target has been and (2) how fully the data allows agents to recreate the target's private life. In the next Part, I address both of those questions by discussing the power and intrusiveness of location data acquisition.

---

have tried to obtain damages by bringing a claim under 42 U.S.C. § 1983 instead. *Id.* at 532.

122. United States v. Warshak, 631 F.3d 266, 283–88 (6th Cir. 2010) (finding a reasonable expectation of privacy in stored e-mail).

123. Quon v. Arch Wireless Operating Co., 529 F.3d 892, 904–08 (9th Cir. 2008) *rev'd and remanded sub nom.* City of Ontario v. Quon, 130 S. Ct. 2619 (2010) (finding that text message users are entitled to privacy in their messages just as telephone callers are entitled to the privacy of their telephone calls).

124. *Compare* 18 U.S.C. §§ 2703(a)–(b) (2006), *with id.* § 2703(c).

125. Smith v. Maryland, 442 U.S. 735, 741–46 (1979).

126. *See* Kyllo v. United States, 533 U.S. 27, 33 (2001) (describing use of the reasonable expectation of privacy test and attributing it to "Justice Harlan's oft-quoted concurrence" in *Katz*); Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (establishing the reasonable expectation of privacy test). For an argument that the traditional reasonable expectation of privacy analysis should be supplemented by a four-factor test that considers the nature of the electronic surveillance at issue, see *infra* Part V.C.

III. WHAT LOCATION DATA REVEALS

A. The Data's Richness and Precision

The frequency and periodicity of a cell phone's communications with its cell towers determines how often the data refreshes.[127] In other words, a cell phone's communication with cell towers determines how many data points there will be in a given time period. Those data points can be used to paint a picture of where a target has been during that period. Each additional data point furnishes more insight into where a person has gone, and as the data becomes more finely grained, government officials can better determine when a person has arrived and departed from each place and, accordingly, how long he has remained there. The more complete the picture the data points provide, the more fully location data intrudes upon private activities.[128] The proximity of cell towers to each other contributes to how accurately each data point will disclose the target's location when each data point, however often, is captured.[129] Cell towers' proximity to each other determines the precision of the location data, which also contributes to the nature of the activities that such data may disclose. The more precisely one can identify where someone has been, the more intrusive the information. As I will discuss, however, copious data from which one can draw inferences makes up for the lack of precision of each data point.[130]

1. Location Data Richness—Periodicity

Cellular telephones send their communications by radio waves to cell sites—transmitting stations in stand-alone towers or on other buildings—that are strategically placed throughout the provider's service area.[131] As a cell phone (and its user) moves from place to place, the cell phone's signal shifts from tower to tower to achieve the best signal. In order to determine which tower to use, the cell phone regularly communicates with nearby towers to test the available signals. When a user places or receives a call on his cell phone, the phone's radio transmitter must communicate with nearby cell towers so that

127. *See infra* Part III.A.1.

128. *See generally* CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT (2007) (decrying law enforcement's use of intrusive surveillance techniques in public places); Christopher Slobogin, *Proportionality, Privacy, and Public Opinion: A Reply to Kerr and Swire*, 94 MINN. L. REV. 1588 (2010) (describing the principle of proportionality between intrusiveness of search and constitutional regulation).

129. *See infra* Part III.A.2.a.

130. *See infra* Part III.B.3.

131. *See generally* BEDELL, *supra* note 10 (offering a detailed explanation of the process). R

the appropriate one (or ones) may handle the call.[132] The cell phone and the tower need to make these connections quite frequently. Although the frequency of such connections may vary by provider and change over time, it appears that they are made as frequently as every seven seconds.[133] The question becomes: how frequently do such connections generate records that providers retain? The "periodicity" of the location information,[134] or how often it is refreshed and recorded, determines how finely grained the location picture will be.

a. Initiation and Termination Data

From cases that address location data, it appears that the government always seeks and obtains initiation and termination data. Initiation data refers to the record of the nearest cell tower to the target when a call begins, and termination data refers to such a record when the call ends. Some courts have distinguished between calls placed by the target and calls the target receives on the ground that the former represent more affirmative conduct by the target.[135] Many courts, however, have treated initiation and termination data the same.[136] In *CSI: Third Circuit*, for example, the government provided an "exemplar" in its filings and stated in its brief that its application requested "the *type of records* shown in the record exemplar."[137] The exemplar listed the date, time, and cell tower used at the beginning and end of

132. *June Hearings*, *supra* note 14, at 20 (statement of Matt Blaze, Associate Professor of Computer and Information Science, University of Pennsylvania). R

133. *CSI: Pittsburgh*, 534 F. Supp. 2d 585, 590 (W.D. Pa. 2008), *aff'd*, No. 07-524M, 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008), *vacated*, 620 F. 3d 304 (3d Cir. 2010); *see also* Thomas Farely & Ken Schmidt, *Cellular Telephone Basics: Registration—Hello, World!*, PRIVATELINE (Jan. 1, 2006), http://www.privateline.com/mt_cellbasics/vii_amps_call_processing/a_registration (noting that during the "registration" process between a mobile phone and available cell towers, "[t]he mobile re-scans every seven seconds or when signal strength drops before a pre-determined level").

134. *See May Hearings*, *supra* note 14, at 29 (statement of Albert Gidari, Partner, Perkins Coie LLP) (using the term "periodicity" to refer to "how frequently location information is to be acquired during the course of a day" and noting the possibility that carriers could report location information every fifteen minutes). R

135. *See, e.g.*, United States v. Suarez-Blanca, No. 1:07-CR-0023-MHS/AJB, 2008 WL 4200156, at *8–9 (N.D. Ga. Apr. 21, 2008) (noting that the government sought location data for outgoing calls originated by the target, not incoming calls, and stating that "in dialing certain numbers, the defendants . . . voluntarily agreed to turn over information about which towers were being used in placing these calls").

136. Courts have distinguished calls made by police to the target specifically to locate the phone, from all other calls to or from the target. *See infra* Part III.A.1.b. (discussing "pinging").

137. Brief for the United States, *supra* note 44, at 32 n.17 (emphasis added). The government described the exemplar as "from the same wireless carrier from which the government seeks to obtain records in this proceeding." *Id.* at 8 n.6. R

each call, including both incoming calls to and outgoing calls from the target.[138]

b. Data from Pinging

Some cases have further distinguished between calls made by the target's friends and associates and those made by the government in order to generate a record that helps to locate the target. When the government calls the target's cell phone, courts call it "pinging"[139] (which is the same word that is used in the network context to signify when one person uses a computer to determine whether another is online).[140] Some courts have permitted warrantless access to location data only after noting that the government did not engage in pinging.[141] In the many other cases in which the creation of data by pinging did not arise, there is no way to know whether the location data sought nonetheless contained such records.[142]

c. Duration Data

Government agents in many cases have sought records of location data that are generated during the call itself, rather than just at its start and end.[143] Duration data, or records of communications with cell towers that take place during a call, provide further details about a target's movements or lack thereof. For example, if the loca-

138. *Id.* at 8. The exemplar also listed the identification number ("PTN") of the caller or called party and whether it was international, forwarded, inbound, or outbound. Exemplar, Brief for the United States, *supra* note 44, Exhibit C. R

139. *See, e.g.*, United States v. Forest, 355 F. 3d 942, 947, 951 (6th Cir. 2004), *vacated sub nom.* Garner v. United States, 543 U.S. 1100 (2005); *see also May Hearings*, *supra* note 14, at 22 (statement of Albert Gidari, Partner, Perkins Coie LLP) ("It is not uncommon for law enforcement to ask for a phone to be pinged every 15 minutes."). R

140. *See Dictionary of Computing: Packet InterNet Groper*, WEBSTER'S ONLINE DICTIONARY, http://www.webster-dictionary.org/definition/Packet+InterNet+Groper (last visited Mar. 25, 2011) (explaining the meaning of the term "ping," short for Packet InterNet Groper, in the computer network context).

141. *See, e.g.*, United States v. Suarez-Blanca, No. 1:07-CR-0023-MHS/AJB, 2008 WL 4200156, at *9 (N.D. Ga. Apr. 21, 2008) (distinguishing *Forest* on the grounds that not only did the government not seek government-created records but it also sought only those records created when the targets initiated the calls themselves); *In re* Application of the U.S. for an Order: (1) Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, & (2) Authorizing Release of Subscriber & Other Info., 622 F. Supp. 2d 411, 418 (S.D. Tex. 2007) [hereinafter *CSI: Houston II*] (granting an order to obtain location data after noting that there was no indication that the government sought to repeatedly place calls to the target).

142. *See infra* Part III.B.1 (discussing uncertainty regarding the content of location data records).

143. *See, e.g.*, *CSI: DC*, 407 F. Supp. 2d 134, 134, 140 (D.D.C. 2006) (rejecting an application that sought data "if reasonably available, during the progress of a call").

tion data includes only initiation and termination information, then it will reveal the nearest cell tower to the target when he starts an hour long call and then when the call ends sixty minutes later. If, however, the location data is refreshed periodically during the course of the call, then it will furnish information about where the target was throughout the hour he spent on the telephone and provide information about how long he stayed at each place.[144] The government has requested and apparently been furnished with duration data in several location data cases, and courts have not tended to view the availability of that data differently from initiation and termination data.[145] That seems odd given that duration data may significantly increase the amount and richness of the data available.

d. Registration Data

Recording "registration data" creates an even more dramatic expansion in the quantity of data. Cell phones generate registration data whenever they communicate with cell towers, whether or not they are engaged in a call.[146] That way, when a call comes through, the service provider's network can quickly locate the phone and place a call to it or from it through the nearest cell tower. In fact, it appears that the only way to stop the production of registration data is to block the radio signal from the cell phone, which is not achieved solely by turning the phone off, but requires further active intervention.[147] Phone customers have little reason to disable the radio signal, unless they are on a plane and specifically required to do so. Thus registration data can be produced at small intervals twenty-four hours a day.[148] If that data were recorded and made available for a particular target, it could create a picture made up of tiny dots that achieved a

144. *See* WAYNE JANSEN & RICK AYERS, NAT'L INST. OF STANDARDS & TECH., GUIDELINES ON CELL PHONE FORENSICS: RECOMMENDATIONS OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY 63 (2007) ("A change of cell identifier between the beginning and the end of a call, over a series of calls, may also indicate a general direction of travel or pattern of behavior.").

145. *See, e.g.*, cases cited *infra* note 152. R

146. *See June Hearings*, *supra* note 14, at 20 (statement of Matt Blaze, Associate Professor of Computer and Information Science, University of Pennsylvania) ("Cell phones periodically identify themselves to the nearest base station (that with the strongest radio signal) as they move about the coverage area."); JANSEN & AYERS, *supra* note 144, at 33–37 (discussing the difficulty of preventing a phone from sending out radio signals to cell towers). R R

147. *See* JANSEN & AYERS, *supra* note 144, at 33–37 (discussing "Airplane Mode" and other techniques used to block a cell phone's radio signals). R

148. Cell phones may be left on even when they are recharging. *See CSI: Austin*, 727 F. Supp. 2d 571, 582 (W.D. Tex. 2010) (expressing concern that "receipt of [location data] will permit the government to 'follow' the phone user's movements 24 hours a day, 7 days a week, wherever they go, whatever they are doing.").

virtual map of all the places the person went and how much time he spent at each place along the way.[149]

As with the other types of data that determine its periodicity, registration data has turned up in cases that have considered the procedural hurdles imposed on government access to location data.[150] With rare exception, courts have not tended to discuss how much more informative (and intrusive) location data becomes when it includes registration data.[151] Although some decisions have granted orders to obtain location data with the explicit understanding that the location records sought would not include registration data, these decisions have nonetheless permitted access to duration data.[152] One district court refused to permit access to registration data prospectively, but had no problem granting access to historical registration data without a warrant.[153] The availability of registration and duration data dramatically increases the richness of location information and the intrusiveness of its acquisition.[154]

149. *June Hearings*, *supra* note 14, at 44 (statement of Michael Amarosa, Senior Vice President, TruePosition, Inc.) (describing the information furnished by location data as providing "definitive information relating to the size, detail, location and activity of illegal conduct" that "can compile current activities, mobile events and interactions with other devices" and "be viewed in a map-based graphic format."). The extent to which the cell phone tower data revealed by the dots corresponds to the target depends on the data's precision, as I discuss in the next Part. It may also be substantially enhanced by inferences, as I discuss in Part III.B.3. R

150. *See, e.g.*, *CSI: Houston III*, Nos. H-10-998M et al., 2010 WL 4286365, at *1 (S.D. Tex. Oct. 29, 2010) ("[T]he Government seeks continuous location data to track the target phone over a two month period, whether the phone was in active use or not."); United States v. Benford, No. 2:09 CR 86, 2010 WL 1266507, at *1 (N.D. Ind. Mar. 26, 2010) (describing the information sought as data "identifying which cell tower communicated with the cell phone while it was turned on"); *In re* Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & a Caller Identification Sys. on Tel. Numbers, 402 F. Supp. 2d 597, 598 (D. Md. 2005) (same); *CSI: Houston I*, 396 F. Supp. 2d 747, 748 (S.D. Tex. 2005) (same).

151. *See, e.g.*, *Benford*, 2010 WL 1266507, at *1 (failing to discuss the fact that the application sought data for whenever the target's phone was on). *But see CSI: Houston III*, 2010 WL 4286365, at *7 ("Even if no calls or texts were ever made, the phone's presence within the home at a given time would likely be revealed by the automatic registration process.").

152. *See, e.g.*, *In re* Application of the U.S. for an Order (1) Authorizing the Installation & Use of a Pen Register & Trap & Trace Device & (2) Authorizing Release of Subscriber Info. and/or Cell Site Info., 411 F. Supp. 2d 678, 682–83 (W.D. La. 2006) [hereinafter *CSI: Shreveport*]; *CSI: SDNY*, 405 F. Supp. 2d 435, 437–38 (S.D.N.Y. 2005).

153. *CSI: Houston II*, 622 F. Supp. 2d 411, 418 n.8 (S.D. Tex. 2007) (describing "'call-detail records,'" to which the court granted warrantless access so long as the records were historical, including location information "used by the phone to obtain service for a call or when in an idle state.").

154. *See CSI: Houston III*, 2010 WL 4286365, at *8 ("In this case, the records sought by the Government are likely far more intrusive [than records for a single day]—not a single snapshot at a point in time, but a continuous reality TV show, exposing two months' worth of a person's movements, activities, and associations in relentless detail.").

The *CSI: Third Circuit* litigation suggests that courts may err when they rely on government representations about the limits of the location data they seek. According to the majority's decision, the government's application to the magistrate judge of the Western District of Pennsylvania sought both duration and registration data.[155] The majority quoted from the application, which appeared redacted in the appendix, as seeking "historical cellular tower data . . . (including, without limitation, . . . call handoffs, call durations, registrations and connection records)."[156] Yet, the government represented in its papers[157] and at oral argument that it sought only initiation and termination information and not registration or duration data.[158] In fact, the government responded to a hypothetical at oral argument about what location data would reveal during a journey from Washington, D.C. to Philadelphia by stating that location data would be recorded only when actual calls were placed.[159] The magistrate judge found that if registration data were provided, it would have furnished cell tower records every seven seconds of that same trip.[160] Duration data would have furnished such information for each period during which the target was on the cell phone.[161] Whether the discrepancy between the application and the government's representations about it reflects a misunderstanding[162] about the application or a view that agents

155. *CSI: Third Circuit*, 620 F.3d 304, 308 (3d Cir. 2010).

156. *Id.* (internal quotation marks omitted).

157. *See* Brief for the United States, *supra* note 44, at 8 (citing the exemplar submitted to the district court as proof that the information sought by the government is limited to date, time, telephone number, the cell tower used to connect to the call, the cell tower used at the end of the call, and the duration of the call); Government's Reply Memorandum of Law in Support of Request for Review 3 n.2, *CSI: Third Circuit*, 620 F.3d 304 (3d Cir. 2010) (No. 08-4227), 2009 WL 3866620 (claiming that the exemplar demonstrates that carriers do not store "call handoff" data). **R**

158. *See* Oral Argument, *supra* note 31, at 35:06–36:19 (arguing that location data in the exemplar was recorded only when calls were started or ended and points out that the exemplar did not include registration data). **R**

159. *See id.* at 35:04–35:28.

160. *See CSI: Pittsburgh*, 534 F. Supp. 2d 585, 589–90 (W.D. Pa. 2008) (noting that whenever cell phones are on, "registration" automatically "occurs approximately every seven seconds"), *aff'd*, No. 07-524M, 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008), *vacated*, 620 F.3d 304 (3d Cir. 2010); *see also supra* text accompanying note 133. **R**

161. *See supra* Part III.A.1.c.

162. Perhaps I misunderstand what the application means by "registrations" and "call handoffs"; however, it is likely a service provider receiving an associated order would assume that registration data is sought.

would have asked for registration data but never received it,[163] it does suggest that courts rely on such representations at their peril.[164]

e. Data from Other Types of Communication

Thus far, I have focused on information associated with cellular telephone calls without considering whether location data may also be recorded when targets use their cell phones, and particularly smart phones, to send and receive text messages, surf the Web, access Facebook, check the news, or conduct any number of other interactions with the Internet. Even without smart phones, nearly all traditional cell phones currently support text messaging.[165] A recent cellular industry report indicates that, while cell phone use to make telephone calls has remained relatively constant, cell phone use for texting and browsing continues to increase sharply.[166] As smart phones become more popular than traditional cell phones, these trends will only increase.[167]

Including location data for text messages and other types of communications would have a dramatic impact on the richness of such data. According to a recent survey, carriers reported handling over 1.5 trillion text messages in 2009, a rate of nearly five billion text messages per day.[168] Consider the least rich category of location information: initiation and termination data. If a target sent a text message every fifteen minutes, then associated location data would reveal cell tower information in fifteen minute intervals throughout the day. The average teenager sends text messages at a much higher rate than

163. The government also indicated at oral argument that providers do not record or collect registration data. *See* Oral Argument, *supra* note 31, at 23:00–25:00. It seems logical that the government would not request registration data unless there was some chance of receiving it. R

164. Amici alerted the Third Circuit to the discrepancies between the redacted application made available to them and the exemplar, but could not elaborate because, at the time, the application had not been made public. Civil Liberties Amici, Third Circuit Brief, *supra* note 80, at 11 & n.3; Freiwald, Third Circuit Brief, *supra* note 92, at 18 n.14. R

165. JANSEN & AYERS, *supra* note 144, at 10. R

166. *See Semi-Annual Wireless Industry Survey*, CTIA—THE WIRELESS ASS'N, http://files.ctia.org/pdf/CTIA_Survey_Midyear_2010_Graphics.pdf [hereinafter *CTIA Survey*] (on file with the Maryland Law Review) (documenting that between 2008 and 2010 cell phone minute usage remained relatively constant while text messaging increased by threefold).

167. *See* Eric Shutt, *Google Outlines Mobile Trends at Advertising Week DC's ADWKDC*, HUFFPOST TECH. (Sept. 24, 2010, 3:05 PM), http://www.huffingtonpost.com/eric-shutt/post_904_b_735621.html (according to Google Mobile Ads Senior Account Executive Elliott Nix, "By 2011, smartphone use is projected to surpass that of today's common feature phone").

168. Press Release, CTIA: The Wireless Ass'n, *CTIA—The Wireless Association Announces Semi-Annual Wireless Industry Survey Results* (Mar. 23, 2010), http://www.ctia.org/media/press/body.cfm/prid/1936.

that.[169] If location data records are generated for text messages, let alone Internet browsing sessions, such records are almost constantly refreshed, even if registration data is not recorded.

In a recent case, the government's application for location data specifically requested data associated with text messages as well as cell phone calls.[170] As with the request for registration data, the fact that a request for text messaging data has shown up in an actual application strongly suggests that the government has received such information in the past or at least believes there to be a significant chance that it will be available in the future. Indeed, industry observers have suggested that as the cost of storing data continues to decrease and as mobile applications develop quickly, companies have many incentives to retain detailed location data.[171]

Between the availability of duration and registration data and the possibility that location data will be recorded when cell phone users send text messages or browse the Internet, it seems clear that location data creates a much more detailed picture of a person's movements (or lack thereof) than has ever before been available to law enforcement.[172] To consider location data surveillance as raising the same concerns as a policeman following someone on public streets is to fundamentally misunderstand the richness of the data and the power of its use as a surveillance tool.[173]

---

169. *See* AMANDA LENHART, PEW INTERNET AND AM. LIFE PROJECT, CELL PHONES AND AMERICAN ADULTS 2 (Sept. 2, 2010), *available at* http://www.pewinternet.org/~/media//Files/Reports/2010/PIP_Adults_Cellphones_Report_2010.pdf (reporting study results that, on average, adults send ten text messages per day and teenagers send fifty per day).

170. *CSI: Brooklyn*, 736 F. Supp. 2d 578, 580 n.5 (E.D.N.Y. 2010) (describing the application as seeking location data "with respect to all calls and text messages to and from a certain mobile telephone over a period of 58 days"), *rev'd*, Order, *CSI: Brooklyn*, 736 F. Supp. 2d 578 (E.D.N.Y. Nov. 29, 2010), ECF No. 11.

171. *June Hearings*, *supra* note 14, at 27–28 (statement of Matt Blaze, Associate Professor of Computer and Information Science, University of Pennsylvania) ("Once the infrastructure to collect it is installed, the cost of collecting and storing high resolution location data about every customer is relatively small, and such information is extraordinarily valuable for network management, marketing, and developing new services."); *see also September Senate Hearings*, *supra* note 49, at 78:10–79:35 (statement of James X. Dempsey, Vice President for Public Policy, Center for Democracy & Technology) (commenting that the ability to store information is at level not contemplated in 1986). R R

172. *See* Stephanie Lockwood, Recent Development, *Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 HARV. J.L. & TECH. 307, 312 (2004) ("The reality that people carry their cell phones on their persons means that cell phone tracking technology potentially offers a detailed view of a given subscriber's movements rather than simply providing call-identifying information.").

173. See *infra* Part IV for a discussion of the problematic analogy to traditional physical surveillance.

2. Location Data Precision

The precision of location data, or how small the area that it identifies the target as within, depends on how close together the cell towers are and on whether data about the cell tower face is provided.[174] Triangulation techniques employ data about the receipt angle and strength of communications signals, often from multiple towers, and can increase location precision, as can the use of GPS data.[175]

a. Cell Tower Proximity and Cell Tower Face Data

If a cell phone communicates with cell towers that are stationed one mile apart, then, all else being equal, data indicating communication with such a cell tower will indicate the target's location with much less precision than if the towers are placed fifty feet apart.[176] As with the other factors, the precision of the location data contributes to the nature of the activities such data may disclose and therefore implicates the constitutional analysis.

The proximity of cell towers varies by provider, by location, and over time.[177] Generally, cell towers are much closer to each other in dense urban areas where they must handle a considerable volume of calls than they are in rural areas where they carry a significantly lighter load.[178] Providers vary in how much they have "built out" particular locations and, therefore, the placement and coverage their towers provide.[179] Historically, towers in cities have typically been placed within a few hundred feet of each other, while in rural areas, and particularly flat ones where the signals can travel without disruption, towers can be miles apart.[180] With providers adding towers to their networks all the time, tower proximity in any particular place should be increasing.[181] According to recent congressional testimony by an

174. *See infra* Part III.A.2.a.

175. *See infra* Part III.A.2.b–c.

176. *See June Hearings*, *supra* note 14, at 23–24 (statement of Matt Blaze, Associate Professor of Computer and Information Science, University of Pennsylvania) (explaining that the distance between cell towers determines the accuracy of the cell location data). R

177. BEDELL, *supra* note 10, at 28–31. R

178. *See, e.g.*, *June Hearings*, *supra* note 14, at 24 (statement of Matt Blaze, Associate Professor of Computer and Information Science, University of Pennsylvania) (explaining cell tower bandwidth limitations as a reason for the proliferation of cell towers in urban areas). R

179. *See id.* at 28 (describing cell phone carrier cell tower plans as utilizing various sector configurations).

180. *See* JANSEN & AYERS, *supra* note 144, at 63 (describing variations based on locale and topography and noting that some rural cell towers are about twenty-one miles apart but urban cell towers have limited coverage areas). R

181. *See CTIA Survey*, *supra* note 166 (reporting that the number of cell sites in service increased forty percent in the last five years and had almost tripled in the last ten years); R

academic and scientific expert, new base technologies permit much greater precision.[182] As he testified to Congress,

> The effect of this trend toward smaller sectors is that knowing the identity of the base station (or sector ID) that handled a call is tantamount to knowing a phone's location to within a relatively small geographic area. . . . [I]n urban areas and other environments that use microcells, this area can be quite small indeed, sometimes effectively identifying individual floors and rooms within buildings.[183]

Location data can reveal a target's location with greater precision when it includes information about the particular face (or sector) of the cell tower that communicated with the target's phone. For instance, consider the cell tower as the center of a pie, with the pie divided into three slices and with each of three sectors sending out signals into each of its corresponding pie slices.[184] If it is known which tower sector communicated with the target's phone, the target's location can be narrowed down by one-third.[185] Instead of merely knowing that the target was within 500 feet of a particular tower as defined by a concentric circle, for example, you can know that the target was more narrowly within the northern facing pie slice and not within the pie slices to the tower's southwest or southeast.[186] Government investigators quite commonly request information about cell sectors when they acquire location data, as they did in their application in *CSI: Third Circuit*.[187] Providers apparently store sector data

---

June Hearings, *supra* note 14, at 19 (statement of Matt Blaze, Associate Professor of Computer and Information Science, University of Pennsylvania) ("Wireless carriers have strained to keep up with the explosive demand for cellular service, in many areas deploying new infrastructure (most visibly cellular antenna towers) as quickly as they can find places to put it."). R

182. *June Hearings*, *supra* note 14, at 24–25 (statement of Matt Blaze, Associate Professor of Computer and Information Science, University of Pennsylvania) (observing that "the size of the 'typical' cell sector has been steadily shrinking"). R

183. *Id.* at 25; *see also id.* at 28 (noting that even without GPS or triangulation, cell sector information "in a dense urban environment with microcells . . . could identify a floor or even a room within a building").

184. *See* JANSEN & AYERS, *supra* note 144, at 8 (describing how sectors work). R

185. *See* Terrence P. O'Connor, *Provider Side Cell Phone Forensics*, SMALL SCALE DIGITAL DEVICE FORENSICS J., June 2009, at 1, 4 (concluding that use of cell tower sectors may be an accurate means of limiting a cell phone location to a 120 degree sector).

186. *Id.*

187. *CSI: Third Circuit*, 620 F.3d 304, 308 (3d Cir. 2010) (quoting the government's application, which sought "sectors when available").

every time a call is made or received and every time the caller's phone moves to a new sector to get a better signal.[188]

b. Triangulation

Cell location data can achieve much greater precision when analysts use triangulation methods to virtually pinpoint a target's location in space. Triangulation refers to a mathematical technique that involves drawing lines from multiple sources and finding the point of connection in the middle.[189] Triangulators can use information about changes in the strength of the communications signal over time and its angle from the tower to the target.[190] They can also use data from overlapping cell towers, alone or in combination with angle and signal strength data.[191] Through whatever techniques, triangulation data can reduce the area in which a target must have been from within a concentric circle or pie slice radiating out from the tower to approach the accuracy of GPS technology.[192] A senior executive of a company that uses triangulation of location information testified to Congress that triangulation techniques have been used to locate illicit cell phones in prisons and to locate missing children and wandering adults with impairments such as Alzheimer's.[193] He lauded the reliability and accuracy of triangulation information, and the fact that it operates "transparent to the device user," in that the user cannot "disable[ ]" the production of triangulation data, as he can with GPS.[194]

In several recent cases in which lower courts have granted investigators warrantless access to location data, their opinions have explicitly noted that the applications did not request multiple tower or

188. *See June Hearings*, *supra* note 14, at 27 (statement of Matt Blaze, Associate Professor of Computer and Information Science, University of Pennsylvania) (explaining the importance of accurate cell phone location data to a carrier's decisions to alter existing infrastructure); *see also id.* at 20 (describing the process by which calls are "handed off" between cell towers to maintain the best radio signal). R

189. *See, e.g.*, *id.* at 38–42 (statement of Michael Amarosa, Senior Vice President for Public Affairs, TruePosition, Inc.) (describing triangulation techniques using radio signal strengths and timing differentials); BEDELL, *supra* note 10, at 311–14 (describing how different triangulation techniques work and how they turn cell phones into tracking devices, raising fears of "Big Brother"). R

190. *See* Lockwood, *supra* note 172, at 308–09. R

191. *Id.* at 309.

192. *See June Hearings*, *supra* note 14, at 29–30 (statement of Matt Blaze, Associate Professor of Computer and Information Science, University of Pennsylvania) ("The gap between the locational precision in today's cellular call detail records and that of a GPS tracker is closing . . . ."). R

193. *Id.* at 32 (statement of Michael Amarosa, Senior Vice President, TruePosition, Inc.).

194. *Id.* at 44.

signal strength data from which they could triangulate the targets' location.[195] Courts apparently view triangulation, unlike some of the other variables already discussed, as constitutionally significant.[196] One court specifically held that the government may not acquire data from which to triangulate on the lesser D order standard when the government in fact sought such data.[197] More recent cases may indicate a trend toward the government seeking multiple tower data.[198]

c. GPS Data

One can pinpoint a target most efficiently using GPS data, which, as one knows from Google maps and related applications, may indicate a cell phone's location down to a particular street address.[199] Increasingly, smart phones come equipped with GPS locators so they may take advantage of geo-location applications.[200] Even traditional cell phones, without Internet capabilities, now include GPS technology so that providers may comply with federal regulations requiring them to pinpoint locations during emergency calls.[201] Some reported cases reveal that government investigators have sought access to such

195. *See, e.g.*, *CSI: Houston II*, 622 F. Supp. 2d 411, 418 (S.D. Tex. 2007) (noting that the government did not indicate that it would use GPS and sought only single tower data); *CSI: SDNY*, 405 F. Supp. 2d 435, 437–38 (S.D.N.Y. 2005) (precluding the government's receipt of GPS or multitower data and noting that the government sought only single cell data).

196. *See, e.g.*, *CSI: Austin*, 727 F. Supp. 2d 571, 574 (W.D. Tex. 2010) (reporting that "there are no published decisions permitting multiple tower or GPS-based [location data] without a showing of 'probable cause'").

197. *See CSI: Houston I*, 396 F. Supp. 2d 747, 749, 765 (S.D. Tex. 2005) (rejecting the government's application for warrantless access to "information regarding the strength, angle, and timing of the caller's signal measured at two or more cell sites").

198. *See, e.g.*, *CSI: Austin*, 727 F. Supp. 2d at 579 ("[T]he application here requests far more than single tower data.").

199. *See, e.g.*, Letter from Bruce Sewell, Gen. Counsel & Senior Vice President of Legal and Gov't Affairs, Apple Inc., to Edward J. Markey and Joe Barton, U.S. House of Representatives 6–7 (July 12, 2010) [hereinafter Apple Letter] (on file with the Maryland Law Review) (describing use of GPS technology in iPhones and other devices to determine precise locations); *see also, e.g.*, *June Hearings*, *supra* note 14, at 21 (statement of Matt Blaze, Associate Professor of Computer and Information Science, University of Pennsylvania) ("GPS technology can achieve very high spatial resolution (typically within ten meters).").

200. *See, e.g.*, Adam Koppel, Note, *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, 1063–66 (2010) (describing modern uses of GPS technology); Apple Letter, *supra* note 199, at 4 ("[Location-based services] allow customers to perform a wide variety of useful tasks such as getting directions to a particular address from their current location, locating their friends or letting their friends know where they are, or identifying nearby restaurants or stores.").

201. *See* 47 C.F.R. § 20.18 (2009) (requiring increasing accuracy of location information through use of either network or handset-based technologies).

GPS data recorded by cell phone service providers.[202] Others have specifically excluded GPS data from the location data government investigators could acquire.[203] Just as with triangulation data, courts have viewed GPS data as significantly more intrusive.[204] The majority opinion in *CSI: Third Circuit* noted that the government's sample application for location data, as furnished in its Department of Justice manual, includes GPS data in the list of items the government may request.[205] Thus, the majority opinion expressed some skepticism of the government's claim that GPS data is not relevant to the analysis of location data.[206]

In one recent case, government investigators requested comprehensive location data. The district court quoted the government's application at length to highlight the extent of the government's request:

> [L]ocation-based data that will assist law enforcement in determining *the exact location of the Target Devices* (differentiated from the first or last cell-site used to make or receive a call, which simply identifies the location of the third party Provider's infrastructure)[ ] . . . includ[ing] . . . the results (through any means reasonably available) of any all [sic] available location-based services, including but not limited to real time cell-site data and those "Enhanced-911" services developed by the Providers to comply with the provisions of 47 C.F.R. § 20.18.[207]

202. *See, e.g.*, *CSI: Austin*, 727 F. Supp. 2d at 579 (W.D. Tex. 2010) (stating that the government application asked for "location-based data that will assist law enforcement in determining *the exact location of the Target Devices*").

203. *See CSI: Shreveport*, 411 F. Supp. 2d 678, 681 (W.D. La. 2006) (acknowledging that the government did not seek available GPS information from the service provider and refusing to authorize release of such information).

204. *See supra* note 196. R

205. 620 F.3d 304, 311 (3d Cir. 2010) (citing COMPUTER CRIME & INTELLECTUAL PROP. SECTION, CRIMINAL DIV., U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 222 (3d ed. 2009), *available at* http://www.cybercrime.gov/ssmanual/ssmanual2009.pdf).

206. *Compare id.* at 311 ("Nonetheless, the Government does not argue that it cannot or will not request information from a GPS device through a § 2703(d) order."), *with* Oral Argument, *supra* note 31, at 10:00–10:15 (government lawyer noting that the case had nothing to do with GPS data). R

207. *CSI: Austin*, 727 F. Supp. 2d at 579–80 (emphasis added by court); *see also id.* at 580 n.17 (explaining "Enhanced 911" requirements); *June Hearings*, *supra* note 14, at 33–37 (statement of Michael Amarosa, Senior Vice President, TruePosition, Inc.) (describing evolution of "Enhanced 911" and services to meet the requirements). R

3. Uncertain Richness and Precision of Location Data

It is impossible to know for certain what location data cell phone companies will turn over to law enforcement agents who compel its disclosure. Uncertainty about what location data would have been produced in response to the government's application apparently led the majority in *CSI: Third Circuit* to withhold judgment as a matter of law and remand for further fact finding.[208] Not surprisingly, the judges' questions during oral argument indicated their unsatisfied curiosity about the precision of the location data at issue.[209] What the judges missed, in both their questioning and the decision's reasoning, is that location data's richness makes up for any lack of precision.[210] In addition, given the ambiguity of the statute and the need for the judiciary to rein in law enforcement practices, a warrant based on probable cause should be required in all cases.[211]

The above discussion establishes that location data contains a wealth of information that, even in its most basic forms, law enforcement can use to paint a fairly complete portrait of the target's private life. The more data collected and the more precise that data, the more location information furnishes a virtual map of our movements and activities. In fact, according to an academic and scientific expert, "Some carriers also store frequently updated, highly precise, location information not just when calls are made or received, but about every device as it moves about the networks."[212] In addition to the potential of providing current or future location applications, carriers may store location information to manage their networks and to improve their

208. *CSI: Third Circuit*, 620 F.3d at 313, 319 ("We therefore cannot accept the [magistrate judge's] conclusion that [location information] by definition should be considered information from a tracking device that, for that reason, requires probable cause for its production.").

209. Oral Argument, *supra* note 31, at 26:26–27:45 (Judge Sloviter asking how close the cell towers are to the caller's cell phone); *id.* at 33:00–34:15 (Judge Tashima questioning the government lawyer about density of cell towers); *id.* at 51:40–52:00 (Judge Tashima questioning EFF lawyer, Kevin Bankston, about how closely location data can track the target); *id.* at 1:07:44–56 (Judge Tashima asking me a similar question regarding how closely location data can track the target). R

210. *See infra* Part IV (discussing reasons not to limit constitutional protection to the inside of the home).

211. *See infra* Part III.B.2 (discussing the need not to rely on law enforcement self-restraint).

212. *June Hearings*, *supra* note 14, at 27 (statement of Matt Blaze, Associate Professor of Computer and Information Science, University of Pennsylvania); *see also id.* ("[A]s even more precise location information becomes available, these records can now also include the customer's latitude and longitude along with the sector ID stored in cellular carrier databases."). R

infrastructures.[213] As the cost of storage goes down and the use of location applications continues, we should expect more storage of ever more precise data.[214]

Government litigators respond to concerns about location data by arguing that the data is too limited, and the picture it paints too vague, to implicate constitutional rights.[215] Before turning to the legal argument, I explore in the next Section three factual reasons why courts should reject the government's contentions about the limits of location data.

B. Location Data: Illegitimate Limits

Courts should reject the government's argument that location data is too limited to implicate the Fourth Amendment for three reasons. First, reviewing courts should not assume that the data providers disclose will be as limited as the data law enforcement requests, or purports to request.[216] Second, because the D order provision does not distinguish between precise and imprecise location data, if the government may use it, they may acquire, without a warrant, whatever location data is available, which is surely growing over time.[217] Because providers have no statutory obligation to filter location data, the government effectively asks the courts to trust it to self-censor and request only location data that does not implicate the Fourth Amendment.[218] Foundational constitutional principles require that the

213. *See, e.g.*, *id.* at 27–28 ("By tracking more precisely where each mobile device is located within a sector . . . a carrier can better identify where new infrastructure is required, where old infrastructure is redundant, and how and where their customers use different wireless services.").

214. *See, e.g.*, *id.* at 27 ("Maintaining such detailed records about the locations of phones as they move from place to place makes good engineering sense, and we should expect this trend to continue as part of the natural progression of technology.").

215. *See, e.g.*, *CSI: Austin*, 727 F. Supp. 2d 571, 578 (W.D. Tex. 2010) (describing the government's argument as claiming that the location information it seeks does not require probable cause "because it cannot precisely locate the phone user"); Brief for the United States, *supra* note 44, at 26–35 (arguing that subscribers have no Fourth Amendment interest in location data because the information does not reveal precise locations). R

216. *See infra* Part III.B.1.

217. *See infra* Part III.B.2; *see also, e.g.*, *CSI: Austin*, 727 F. Supp. 2d. at 579 n.15 ("And there is nothing in any of the relevant statutes that makes a distinction between 'limited' location information and fully robust, minute-by-minute location information."); *In re* Application of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d 448, 450–52 (S.D.N.Y. 2006) (describing precision of multiple tower information and observing that if the statutory provisions that do not require a warrant "authorize the disclosure of cell site information from a single antenna tower, there is no reason to believe that they would not authorize disclosure of such information from multiple antenna towers simultaneously").

218. *See infra* note 245 and accompanying text. R

courts not trust executive branch agents to police themselves; a warrant requirement is needed to ensure that zealous agents in the field do not exceed constitutional limits.[219] That is especially so when, because they have operated under a less demanding relevance standard, agents apparently have been requesting location data for a large number of targets with only a tenuous connection to crime. Finally, the intrusive nature of location data is enhanced by the government's ability to use it to draw inferences about a target's personal movements and activities.[220]

1. Applications Do Not Necessarily Dictate Results

One cannot assume that the information law enforcement requests will match the information that service providers disclose. For example, the exemplar the government provided in the *CSI: Third Circuit* litigation did not appear to be a customer bill—it had none of the trappings of a communication with a customer, such as the subscriber's name, account number, or address—but rather appeared to be a report the provider drew from a database of raw location data.[221] The exemplar was identified as the first of fifty-four pages and listed the time and date the report was created.[222] Although we cannot know how much, the underlying location data stored by the provider could actually have been much more extensive.[223] In other words, even if the exemplar suggested that the targeted provider collects the information listed there, it does not establish that the provider would provide no more. To the extent service providers retain more than the limited subset of location data the government purports to seek, there would be neither reason nor way for providers to filter the data in order to deliver only limited data.[224] As mentioned above, the profit motive should impel providers to make disclosure decisions

219. *See infra* Part III.B.2.

220. *See infra* Part III.B.3.

221. *See* Exemplar, Brief for the United States, *supra* note 44, Exhibit C, Document 11-4. R

222. *Id.*

223. *See CSI: SDNY*, 405 F. Supp. 2d 435, 438 (S.D.N.Y. 2005) (stating that the provider digitally transmitted stored cell site data to the government, which "then use[d] a software program to translate that data into a usable spreadsheet").

224. *See* 47 U.S.C. § 1002(b)(1) (2006) (clarifying that law enforcement may not compel or prohibit service providers from using any particular equipment or technology to comply with Communications Assistance for Law Enforcement Act ("CALEA")); *see also In re* Grand Jury Subpoenas to Sw. Bell Mobile Sys., Inc., 894 F. Supp. 355, 359 (W.D. Mo. 1995) (describing how in using "toll records" in the SCA, Congress intended to "make certain that the providers of electronic communication services were not required to create records not kept in the ordinary course of business").

based on the lowest cost rather than to decide based on the best interests of the target.[225]

In a related context, for example, the Communications Assistance for Law Enforcement Act requires that law enforcement agents do more than obtain a pen register order to acquire location data in real time.[226] Despite the clear prohibition against it, providers presented with only pen register orders apparently fail to filter out location data because it is just too costly to do so.[227] Instead, according to one industry lawyer, whenever providers receive a pen register order, they also provide location data: "The location information is just flowing as part of the solution."[228] Even without seeking it, then, law enforcement agents will likely receive more location data than they request. As discussed above, that information can include duration, registration, triangulation, and GPS data, all of which can provide an extremely rich and precise picture of a target's movements.[229]

Exacerbating the problem, providers do not collect and retain location data solely on their own initiative, but also in anticipation of law enforcement requests.[230] Private companies share a strong interest in cooperating with law enforcement agents in their pursuit of crime.[231] Service providers have an incentive to satisfy rather than annoy government investigators, and if they suffer no penalty for over-

225. *See CSI: Pittsburgh*, 534 F. Supp. 2d 585, 590 n.20 (W.D. Pa. 2008) (describing provider as the one making decisions about what location data to retain based on an interest in keeping costs down and complying with government demands), *aff'd*, No. 07-524M, 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008), *vacated*, 620 F.3d 304 (3d Cir. 2010); *see also* Freiwald, *Uncertain Privacy*, *supra* note 75, at 1010–13 (questioning the calculation that equates service provider interests with subscribers' privacy interests, particularly when subscribers will not find out about disclosures). R

226. 47 U.S.C. § 1002(a)(2)(B).

227. *See* Albert Gidari, Jr., Keynote Address, *Companies Caught in the Middle*, 41 U.S.F. L. REV. 535, 549–50 (2007).

228. *See id.* at 550 ("[Service providers] are paying a fortune for the CALEA hardware and software, and they are not paying to filter it further.").

229. *See supra* Part III.A.1–2.

230. Magistrate Judge Lenihan pointed out that companies retain data for law enforcement's benefit in her decision. *CSI: Pittsburgh*, 534 F. Supp. 2d at 615 ("Nor does a [provider's] retention of [location data] generally serve any business purpose for the customer or for the provider in serving the customer; rather, such information is retained principally, if not exclusively, in response to Government directive."); *see also June Hearings*, *supra* note 14, at 86–87 (statement of Stephen Wm. Smith, U.S. Mag. J.) ("[W]hat about historical [location data] that is captured only at the instigation of law enforcement, and for which the provider has no legitimate business reason to generate or maintain on its own."). R

231. *See, e.g.*, *ECPA Reform and the Revolution in Cloud Computing: Hearing Before the H. Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 28–29 (2010) (statement of Michael Hintze, Associate General Counsel, Microsoft Corporation) (describing Microsoft's extensive efforts to cooperate with law enforcement).

disclosing, they will disclose what is most convenient and likely to comply rather than withholding data on principle.[232] Although the ex parte and usually sealed nature of government applications makes them exceedingly difficult to research,[233] requests for location data have apparently been quite extensive.[234] In one recent case, which the district court took the unusual step of unsealing, the court noted a discrepancy between the extremely precise location data that the government's application sought, and the "boilerplate" footnote on its application that suggested it was seeking much more limited data.[235]

In general, there are thousands of wireless service providers who undoubtedly collect and retain different amounts and types of location data.[236] Efforts to have the major service providers disclose their collection and retention policies have proved fruitless in the past, as companies may consider such information to be trade secrets.[237] A recent congressional hearing on the need to update the electronic surveillance laws that focused on location data, however, has brought more information to light than was previously available. In particular, testimony revealed that the precision of location data has increased dramatically, even without the use of either triangulation or GPS technologies. Both of those technologies, of course, are becoming in-

232. *See* 18 U.S.C. § 2707(e) (2006) (providing broad service provider immunity for cooperation with law enforcement when they submit documentation in support of their requests); *see also id.* § 2712(c) (providing only for administrative discipline for law enforcement agents who violate SCA provisions).

233. *See* Bankston, *supra* note 72, at 605–06 (discussing the secrecy involved in ex parte cases); Crump & Calabrese, *supra* note 8, at 3, 4–5 (describing the need to issue Freedom of Information Act requests to obtain information about location data cases, because they were filed under seal "'until further order of the Court'" and conducted ex parte (quoting *In re* Sealing & Non-Disclosure of Pen/Trap/2703(D) Orders, 562 F. Supp. 2d 876, 878 (S.D. Tex. 2008))); *see also* Crump & Calabrese, *supra* note 8, at 4 (noting that the lawyers were able to obtain information from only the few federal districts with which they engaged in Freedom of Information Act litigation). R R R

234. *See June Hearings*, *supra* note 14, at 80 (statement of Stephen Wm. Smith, U.S. Mag. J.) (estimating that the total number of electronic surveillance orders issued at the federal level exceeds 10,000 per year); *May Hearings*, *supra* note 14, at 23 (statement of Albert Gidari Jr., Partner, Perkins Coie LLP) ("The number of user records requested on a daily basis is astronomical."); Gidari, *supra* note 227, at 554 (discussing the magnitude of government requests for information). R R R

235. *CSI: Austin*, 727 F. Supp. 2d 571, 579 (W.D. Tex. 2010). See *supra* text accompanying note 207 for the text of the government's request. R

236. *See June Hearings*, *supra* note 14, at 27 (statement of Matt Blaze, Associate Professor of Computer and Information Science, University of Pennsylvania) (explaining that "each carrier has its own data collection and retention practices"); Gidari, *supra* note 227, at 550 (reporting that in 2007 there were "at least 3500 registered carriers in this country" and "another 1300 wireless companies"). R R

237. Thanks to John Shafer, USF Research Librarian, for help pursuing this information.

creasingly common with the advent of smart phones. As each individual data point is more and more informative, private companies collect more and more data, and both trends should only continue. As a result, whether it was true in years past that the location information itself was not informative or that the informative data would not show up in provider records, neither fact appears to be true any longer.[238]

2. Law Enforcement Self-Restraint

Whatever location data may be available, in *CSI: Third Circuit* the government urged the court to consider only the circumscribed set of location data it purportedly requested in its application.[239] When the government argues that the limited nature of its location data requests insulates those requests from Fourth Amendment scrutiny, it essentially asks courts to rely on agents' own self-restraint to protect Fourth Amendment rights.[240] But law enforcement agents may not avoid the application of the Fourth Amendment by asserting that they themselves will limit their review of location data and that they may do so without meaningful judicial oversight.[241] The applicable statutory provision places no limits on the information available with a D order if the Fourth Amendment does not apply.[242] As the majority recognized in *CSI: Third Circuit*, when considering law enforcement surveillance methods, courts must take the inevitable growth of the technology into account.[243] Just ten years ago, the Supreme Court rejected the idea that the constitutionality of surveillance should be

238. *See, e.g.*, *June Hearings*, *supra* note 14, at 27 (statement of Matt Blaze, Associate Professor of Computer and Information Science, University of Pennsylvania) (describing how providers are recording more location data, and that information is more intrusive now). *But see June Hearings*, *supra* note 14, at 63–64 (statement of Richard Littlehale, Assistant Special Agent in Charge, Technical Services Unit, Tennessee Bureau of Investigation) (complaining that new technologies are making it harder to get access to information and presaging government demands for greater access). R R

239. *See, e.g.*, Brief for the United States, *supra* note 44, at 7, 9 (focusing on the records "requested"); Oral Argument, *supra* note 31, at 30:25–30:34 (the government lawyer arguing that Fourth Amendment determinations must be made on the facts before the court); Oral Argument, *supra* note 32, at 50:20–50:31, 50:56–51:16 (Judge Tashima expressing resistance to issuing an "advisory opinion" based on facts not before the court). R R R

240. Freiwald, Third Circuit Brief, *supra* note 92, at 22–23, 25. R

241. Oversight under 18 U.S.C. § 2703(d) includes neither probable cause justification, meaningful remedies for misuse, nor judicial oversight of the monitoring, once begun.

242. *See* Brief for the United States, *supra* note 44, at 11–12 (recognizing that the language in 18 U.S.C. § 2703(c)(1) is a "catch-all category" designed to include any information that a service provider stores that is "'pertaining to'" a subscriber of an electronic communication service). R

243. 620 F.3d 304, 318 (3d Cir. 2010) (citing Kyllo v. United States, 533 U.S. 27, 36 (2001)); *see also Kyllo*, 533 U.S. at 36 ("While the technology used in the present case was

judged on the basis of what occurred in the case at bar and instead required courts to "take the long view" and give "clear specification of those methods of surveillance that require a warrant."[244]

Moreover, if courts were to rely on the government's representation that executive branch agents will not seek data that implicates the Fourth Amendment, they would permit those agents to take on for themselves the oversight role the Constitution entrusts solely to the members of the judiciary.[245] The Supreme Court soundly rejected a similar request more than forty years ago in the famous *Katz*[246] decision in which it first determined that the Fourth Amendment regulates wiretapping:

> The Government urges that, because its agents . . . did no more here than they might properly have done with prior judicial sanction, we should retroactively validate their conduct. That we cannot do. It is apparent that the agents in this case acted with restraint. Yet the inescapable fact is that this restraint was imposed by the agents themselves, not by a judicial officer. They were not required, before commencing the search, to present their estimate of probable cause for detached scrutiny by a neutral magistrate. They were not compelled, during the conduct of the search itself, to observe precise limits established in advance by a specific court order. Nor were they directed, after the search had been completed, to notify the authorizing magistrate in detail of all that had been seized.[247]

Trusting the government to curb its own appetite for increasingly intrusive location data would run counter not only to constitutional principles but also to experience. For example, as pen registers evolved from devices that recorded telephone numbers into devices capable of recording ever richer data, law enforcement agents demanded the ability to use them without satisfying more than the mini-

---

relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development.").

244. *Kyllo*, 533 U.S. at 40.

245. According to one court, agents limit their requests specifically to avoid constitutional confrontations. *See In re* Application of the U.S. for an Order Authorizing Installation & Use of Pen Register, 415 F. Supp. 2d 211, 218 n.5 (W.D.N.Y. 2006) (outlining a conversation between the court and the government lawyer during oral argument in which the latter described how agents refrain from asking for all possible data so as not to alarm magistrate judges).

246. Katz v. United States, 389 U.S. 347 (1967).

247. *Id.* at 356.

mally demanding requirements Congress established in 1986.[248] In the latest installment of this story, law enforcement agents advocated the right to obtain post-cut-through dialed-digits with a pen register order, despite the fact that those digits often contain content, on the ground that service providers are unable to filter out the non-contents data.[249] "Post-cut-through dialed digits" generally refer to digits dialed after the first ten (phone number digits) and may include bank account numbers, social security numbers, and prescription numbers.[250] Courts have quite properly refused to allow law enforcement agents to segregate the data themselves.[251]

With regard to location data, law enforcement agents have shown that they will not limit themselves. ACLU lawyers obtained information pursuant to Freedom of Information Act requests that suggests that agents in the field regularly violate Department of Justice guidelines and request the most precise location data without first obtaining a warrant.[252] The Associate Director of the Office of Enforcement Operations wrote several memos explaining to agents that they should establish probable cause when seeking prospective records that would divulge location data indicating a target's latitude and longitude (using either GPS or "similarly precise" data).[253] Nonetheless, the ACLU discovered that in one U.S. Attorney's Office, nineteen applications in which agents requested "GPS or similarly precise location data without a judicial determination of probable cause"

248. *See* Freiwald, *Uncertain Privacy*, *supra* note 75, at 982–89 (discussing the evolution of "pen register," which has led to "government lawyers press[ing] for an open-ended and functional definition" that includes "computer system[s]"). R

249. *In re* U.S. for Orders (1) Authorizing the Use of Pen Registers & Trap & Trace Devices, 515 F. Supp. 2d 325, 332 & n.5 (E.D.N.Y. 2007) [hereinafter *PCTDD: EDNY*].

250. *Id.* at 328.

251. *See, e.g.*, *In re* Application of the U.S. for an Order Authorizing the Use of a Pen Register & a Trap & Trace Device on Wireless Tel., No. 08 MC 0595(JO), 2008 WL 5255815, at *3 (E.D.N.Y. Dec. 16, 2008) (denying application if government would segregate the data itself, as violative of the statute); *PCTDD: EDNY*, 515 F. Supp. 2d at 339 (finding government segregation of data to violate Fourth Amendment); *In re* Application of the U.S. for an Order Authorizing (1) Installation & Use of a Pen Register & Trap & Trace Device or Process, (2) Access to Customer Records, & (3) Cell Phone Tracking, 441 F. Supp. 2d 816, 827 (S.D. Tex. 2006).

252. *See* Crump & Calabrese, *supra* note 8, at 4. R

253. *See, e.g.*, E-mail from Mark Eckenwiler, Assoc. Dir., Office of Enforcement Operations, Criminal Div., to CHIPs (Nov. 16, 2007, 3:19 PM), *available at* http://www.aclu.org/pdfs/freespeech/18cellfoia_release_CRM-200800622F_06012009.pdf (page 80); E-mail from Mark Eckenwiler, Assoc. Dir., Office of Enforcement Operations, Criminal Div., to All USAEO Criminal Chiefs (Sept. 12, 2008, 2:38 PM) (on file with author). Note that the government does not concede that probable cause is required. *See supra* note 114. R

were granted in about a one year period.[254] In another office, judges granted six such applications.[255] There is no way to know what goes on at other offices that did not provide information, but these applications indicate that officials can neither control nor speak for the actions of their agents in the field.[256] Accordingly, representations based on "official policy" cannot be relied upon as what is happening in reality.

As discussed, a mere relevance and materiality standard permits law enforcement agents to obtain location data and make inferences from it about those who have only tenuous connections to crimes. The government apparently seeks location information about ostensibly innocent parties regularly. According to an industry lawyer, "With respect to location information of specific users, many orders now require disclosure of the location of all of the associates who called or made calls to a target."[257] Agents apparently request information on all calls handled by a particular cell tower.[258] At oral argument, a member of the *CSI: Third Circuit* panel expressed concern about the government's attempt to determine the identity of callers using cell location data.[259] If law enforcement agents could acquire location data, without a warrant, about people so tenuously connected to crimes, then more than two hundred and ninety million Americans

254. Letter from William G. Stewart II, Assistant Dir., FOIA/Privacy Unit, to Catherine Crump, Request No. 07-4132 (Dec. 31, 2008), *available at* http://www.aclu.org/pdfs/freespeech/cellfoia_released_074132_12312008.pdf.

255. Letter from William G. Stewart II, Assistant Dir., FOIA/Privacy Unit to Catherine Crump, Request No. 07-4135 (Dec. 31, 2008), *available at* http://www.aclu.org/pdfs/freespeech/cellfoia_released_074135_12312008.pdf.

256. *See* Crump & Calabrese, *supra* note 8, at 4 ("Because the FOIA focused on only a small number of U.S. Attorney's Offices around the country, it may well be that many other offices also do not follow DOJ's recommendation."). R

257. *See* Gidari, *supra* note 227, at 557. R

258. *See May Hearings*, *supra* note 14, at 29–30 (statement of Albert Gidari, Partner, Perkins Coie LLP) (describing a common practice of government agents seeking the "location [information] of the community of interest—that is, the location of persons with whom the target communicates"); JANSEN & AYERS, *supra* note 144, at 63 (describing as a possible search criterion "all calls handled by a base station responsible for a particular cell"); Crump & Calabrese, *supra* note 8, at 7 ("[I]t appears that the government took the dragnet approach of getting location information for a large number of innocent people to try to figure out who was involved in the crime."). R R R

259. *See* Oral Argument, *supra* note 31, at 13:45–14:15 (Judge Sloviter questioning the government lawyer about what the government is "trying to get at" with "its interpretation of the statute" and specifically inquired about identity information); *see also id.* at 28:00–29:50 (Judge Sloviter expressing concern about government interest in attendance at political meetings or protests and acquisition of location data without a warrant to determine who attended). R

who use cell phones are at risk of location data surveillance.[260] That risk justifies the judicial oversight that a warrant requirement guarantees.

3. Inferences

In its arguments before the Third Circuit, the government repeatedly implied that the Fourth Amendment is implicated only when acquisition of location data pinpoints a target's physical location in a space that exactly matches an area previously identified as his home or other constitutionally protected space. For example, the government argued that the location data in the case was "much too imprecise to tell whether calls have been made or received from a constitutionally protected space, let alone to reveal facts about the interiors of private homes or other protected spaces."[261] The next Part addresses the government's unduly narrow view of the spaces the Constitution protects, which the Third Circuit unfortunately seemed to adopt. But here I discuss how location data can intrude on privacy by facilitating inferences, in addition to directly providing pinpoint data.

The majority in *CSI: Third Circuit* properly recognized the possibility of inferring "private" facts about the target through his location data.[262] As the majority also recognized, information gained from inference can be just as intrusive as information gained directly.[263] In *Kyllo v. United States*,[264] the Supreme Court rejected the "dissent's extraordinary assertion that anything learned through 'an inference' cannot be a search."[265]

Even when they do not know the target's home address, agents can likely figure out when a target was home using his location data and simple inferences.[266] For example, the target will likely use his cell phone regularly from his home in the morning, evening, and weekend hours.[267] Law enforcement agents should be able to infer,

260. *See CTIA Survey*, *supra* note 166 (reporting an estimated 292,847,098 cellular subscriber accounts in the United States at the end of June 2010). R

261. Brief for the United States, *supra* note 44, at 35. R

262. *CSI: Third Circuit*, 620 F.3d 304, 311–13 (3d Cir. 2010).

263. *Id.* at 312.

264. 553 U.S. 27 (2001).

265. *Id.* at 36.

266. *CSI: Third Circuit*, 620 F.3d at 311–12.

267. In fact, many users have replaced their landline phones with cell phones, which they use to make and receive all calls. *See* DAVID KRANE & KERRI MILLER, HARRIS INTERACTIVE, THE HARRIS POLL #36: CELL PHONE USAGE CONTINUES TO INCREASE (Apr. 4, 2008), *available at* http://www.harrisinteractive.com/vault/Harris-Interactive-Poll-Research-Cell-Phone-Usage-Continues-to-Increase-2008-04.pdf (finding that thirty-two percent of Americans ages 18 to 29 and fourteen percent of all adults exclusively used cell phones).

from data covering a fairly short time frame, when the target was making and receiving calls from home. Agents can then identify which cell tower and sector is closest to the target's home.[268] Once they identify that cell tower and sector,[269] the agents can determine whenever the target was likely in his home.[270] In addition, law enforcement agents might use the incoming and outgoing telephone numbers, along with the duration of those calls, to identify the target's presence at other places of interest and to infer information about his activities while there.[271]

Besides, under law clearly established by the SCA, law enforcement agents can acquire "subscriber information" about a target without obtaining a warrant, by procuring only a D order from a judge that meets the "relevant and material" standard.[272] That information may yield the target's home address, credit card information, Internet account information, telephone number, and the numbers dialed by his telephone.[273] Consequently, without a warrant, agents may find out where a target lives and his telephone number even before they obtain his location data. Equipped with that knowledge, location data that shows the target's cell phone communicated with the cell tower closest to his home indicates that the target was likely at home and on the telephone during that time.[274]

Location data has furnished law enforcement with investigatory and prosecutorial value in the past several years. Prosecutors have used the data, even when fairly "imprecise," to connect targets to

---

268. In addition to divulging information about actual calls, if location data was recorded whenever the telephone was powered on, then the information would quickly divulge when a target was home because it would show the telephone on in the same place for long periods (for example, sleeping hours) that would correspond to the time the target was home.

269. Presumably, one could figure this out using merely a tower without associated sector information.

270. *See* JANSEN & AYERS, *supra* note 144, at 63 ("Identifying the geographical coverage of specific cells can provide valuable information when combined with call detail records, geographically establishing plausible locations with some degree of certainty for the times involved."). R

271. *See, e.g.*, *id.* at 63–64 (explaining how to analyze "the patterns and content of communications" to determine ownership of prepaid phones despite a target's attempts to evade discovery).

272. 18 U.S.C. § 2703(d) (2006).

273. *See* JANSEN & AYERS, *supra* note 144, at 62 (providing a complete listing of subscribing information typically available from service providers). R

274. *See June Hearings*, *supra* note 14 at 86, (statement of Stephen Wm. Smith, U.S. Mag. J.) ("For instance, when law enforcement already knows the business and residential addresses of the target (or the target's family, friends, and associates), a single phone call signal captured from a single tower may be all that's needed to reliably pinpoint a target's exact location at a given time."). R

crime scenes and to disprove alibis.[275] In making their cases, prosecutors have used inferences to enhance the value of location data that is otherwise not very precise.[276]

The richness and precision of the data, the reasons to believe providers will disclose more than what they are asked for, and the likelihood that government agents will be unable to restrain themselves from over-collecting, mandate the protections of the warrant requirement. Individuals particularly need the protections of the warrant requirement because of the inferences that location data permits one to draw about their movements and activities, the possibility of which the majority in *CSI: Third Circuit* recognized.[277] Nonetheless, the majority remanded the case to the magistrate judge to determine whether a warrant was in fact required, leaving open the distinct possibility that the government could compel disclosure of the wealth of location data on the minimal protections of the D order.[278] The explanation lies in part on the majority's narrow interpretation of the protection offered by the bumper-beeper cases, to which I next turn.

IV. LOCATION DATA AND THE HOME

A. *The Bumper-Beeper Cases:* Knotts *and* Karo

In cases like *CSI: Third Circuit*, the government has contended that courts must read two bumper-beeper precedents from the 1980s to deny Fourth Amendment protection to location data derived from cell phone providers.[279] In particular, the government has asserted that *United States v. Knotts*[280] establishes that "there is no reasonable expectation of privacy in cell-site information."[281] The government maintains that because cell tower "records provide only a very general indication of a user's whereabouts at certain times in the past, the

275. *See, e.g.*, People v. Pese, No. A100933, 2004 WL 899768, at *2–3 (Cal. Ct. App. Apr. 28, 2004) (involving location data that connected defendant to the place where the victim's body was found); O'Connor, *supra* note 185, at 4 (describing use of location data to disprove alibi in a criminal investigation); Lockwood, *supra* note 172, at 310–11 (furnishing more examples of law enforcement use of cell phone location data). R R

276. *See* Civil Liberties Amici, Third Circuit Brief, *supra* note 80, at 14–19; *see also id.* at exhibit A (providing expert testimony from a case where location data was used to infer when the target was at home and at the home of another person). R

277. 620 F.3d 304, 312–13 (3d Cir. 2010).

278. *Id.* at 319.

279. *See, e.g.*, *id.* at 312–13 (finding that the bumper-beeper precedents "make clear that the privacy interests at issue are confined to the interior of the home"); United States v. Suarez-Blanca, No. 1:07-CR-0023-MHS/AJB, 2008 WL 4200156, at *9–11 (N.D. Ga. Apr. 21, 2008) (using the bumper-beeper precedents to deny a Fourth Amendment challenge).

280. 460 U.S. 276 (1983).

281. Brief for the United States, *supra* note 44, at 28–29 (citing *Knotts*, 460 U.S. at 282). R

requested [location] records do not implicate a Fourth Amendment privacy interest."[282]

Knotts, decided in 1983, had nothing to do with location data gleaned from use of cell phones. It addressed the government's monitoring of a radio beeper attached to a large container of chemicals stored in an automobile that government agents followed "on public streets and highways."[283] Several meaningful differences between location data and the data divulged by the beeper in *Knotts* undermine the case's relevance for location data.[284]

First, agents affixed the beeper in *Knotts* to a five-gallon drum of chloroform and monitored the drum rather than the individual suspects.[285] If those surveillance targets had been separated from the drum for any reason, the monitoring would have ceased to be effective. Unlike five-gallon drums of chloroform, cell phones generally travel with the user and are often on the user's person. Indeed, modern cell phones include many features that tempt users to have them at hand all the time.[286] Thus, the beeper monitoring the Supreme Court considered in *Knotts* was considerably less intrusive, by virtue of being considerably less reliable, than that afforded by acquisition of location data.[287] According to one recent decision, "The level of information obtained from [traditional] tracking devices was thus akin to (and indeed, less precise than) what law enforcement agents today can know about a modern cell phone user's location from information from a single cell tower," even without triangulation or GPS information.[288]

Second, agents often obtained a warrant before installing the type of beeper used in the mid-1980s; that initial hurdle limited the use, and therefore possible abuse, of beepers.[289] Thus, the Supreme Court had to consider whether beeper monitoring, which was a real-

282. *Id.* at 7.

283. *Knotts*, 460 U.S. at 277, 281.

284. The Civil Liberties Amici did an excellent job distinguishing the *Knotts* case. *See* Civil Liberties Amici, Third Circuit Brief, *supra* note 80, at 14–19. R

285. *Knotts*, 460 U.S. at 277.

286. *See* United States v. Park, No. CR 05-375 SI, 2007 WL 1521573, at *8 (N.D. Cal. May 23, 2007) (listing the features of "modern cell phones," including "address books, calendars, voice and text messages, email, video and pictures").

287. *See, e.g.*, *CSI: Austin*, 727 F. Supp. 2d 571, 578–79 & n.14 (W.D. Tex. 2010) (describing how beepers used in traditional cases were significantly less sophisticated than cell phones today and provided "only general information regarding the location of the tracked object or person").

288. *Id.* at 579.

289. *See* United States v. Karo, 468 U.S. 705, 713 n.3 (1984) (discussing advisability of getting a warrant before installing a beeper).

time tracking of radio signals to determine how close the car with the beeper was to the radio monitor, constituted a search.[290] Compelling a cell phone service provider to disclose detailed records from whatever period they are stored to indicate the movements and travels of an individual can hardly be considered a similar investigative technique, merely because both types of data reveal information about the target's place in space.[291]

Third, because government agents in *Knotts* exclusively monitored a car, the Court relied on the "diminished expectation of privacy in an automobile."[292] Location data, in contrast, reveals the movements and activities of cell phone users in many places besides their cars; modern cell phones accompany their users on walks, into buildings, and into their homes.[293] Because the *Knotts* Court focused on the lack of privacy in cars on public roads, its reasoning does not apply to location data, which can reveal a user's location anywhere.

Just because a subset of location data may reveal what a bumper-beeper could reveal—or even what naked-eye surveillance could reveal—does not mean that the technique of acquiring location data must be constitutionally unregulated. In *Kyllo*, the Court rejected the notion that use of the thermal imaging device was not a search because, had snow been present on the roof, its melting patterns could have revealed (without technology) the same information about heat in the house.[294] As the Court stated, "The fact that equivalent information could sometimes be obtained by other means does not make lawful the use of means that violate the Fourth Amendment."[295] Ultimately, the Court had to consider "what limits there are upon this power of technology to shrink the realm of guaranteed privacy."[296]

---

290. *Id.* at 707 & n.1.

291. *PCTDD: EDNY*, 515 F. Supp. 2d 325, 338 (E.D.N.Y. 2007) (finding use of pen registers to divulge content to violate the Fourth Amendment and observing that "[t]he evolution of technology and the potential degree of intrusion changes the analysis").

292. United States v. Knotts, 460 U.S. 276, 281 (1983); *see also* United States v. Forest, 355 F.3d 942, 951–52 (6th Cir. 2004) (explaining that because the location data in the case divulged only the movements of a car along public highways, on facts "nearly identical to the facts in *Knotts*," its acquisition did not implicate the Fourth Amendment).

293. *See* James X. Dempsey, *Digital Search & Seizure: Updating Privacy Protections to Keep Pace with Technology*, *in* NINTH ANNUAL INSTITUTE ON PRIVACY AND SECURITY LAW 2008, at 543, 572 (PLI Patents, Copyrights, Trademarks, & Literary Property Course Handbook Series No. 14648, 2008) ("A cell phone clearly goes places where an individual has a reasonable expectation of privacy.").

294. United States v. Kyllo, 533 U.S. 27, 35 n.2 (2001).

295. *Id.*

296. *Id.* at 34.

The monitoring the police conducted in *United States v. Karo,*[297] which the Supreme Court found to implicate the Fourth Amendment, comes closer to the acquisition of location data. In *Karo*, the constitutional question turned on whether agents monitored the beeper "in a private residence, a location not open to visual surveillance."[298] The Court elaborated that agents determined that "the beeper was inside the house," which was "a fact that could not have been visually verified."[299] The Court imposed Fourth Amendment constraints on the government's use of the beeper "to determine . . . whether a particular article—or a person, for that matter—is in an individual's home at a particular time."[300] While it is not necessary for an investigative technique to penetrate the home to intrude upon a reasonable expectation of privacy, it is extremely likely that location data will reveal at least as much information about the inside of a home as the beeper revealed in *Karo*. As discussed above, with inferences, law enforcement should be able to determine, from location data, when a target was home, awake, and on the phone.[301] That would suffice to implicate the Fourth Amendment under *Karo* and necessitate a probable cause warrant.[302]

The government implies that it need not obtain a warrant before acquiring location data because agents will not be able to tell in advance whether the target has used the cell phone in his home. But that putative lack of knowledge is the reason to get a warrant rather than to be excused from getting one.[303] Just as the Supreme Court did in *Karo*, when it recognized that "[r]equiring a warrant will have the salutary effect of ensuring that use of beepers is not abused[ ] by imposing upon agents the requirement that they demonstrate in ad-

297. 468 U.S. 705 (1984).

298. *Id.* at 714.

299. *Id.* at 715. In *CSI: Third Circuit*, the government apparently sought location data only after physical surveillance had "proven difficult." Brief for the United States, *supra* note 44, at 5. **R**

300. *Karo*, 468 U.S. at 716.

301. *See supra* Part III.B.3; *see also* Civil Liberties Amici, Third Circuit Brief, *supra* note 80, at 14–19 (providing a hypothetical and actual example to illustrate the power of location data). **R**

302. *See Karo*, 468 U.S. at 708–14.

303. *See CSI: Pittsburgh*, 534 F. Supp. 2d 585, 613 n.75 (W.D. Pa. 2008) (noting that "'[t]he argument that a warrant requirement would oblige the Government to obtain warrants in a large number of cases is hardly a compelling argument against the requirement'" (alteration in original) (quoting *Karo*, 468 U.S. at 718)), *aff'd*, No. 07-524M, 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008), *vacated*, 620 F. 3d 304 (3d Cir. 2010); *CSI: Houston I*, 396 F. Supp. 2d 747, 757 (S.D. Tex. 2005) (arguing that uncertainty about the need for a warrant in advance counsels in favor of getting a warrant in all cases).

vance their justification for the desired search,"[304] modern courts should impose a warrant requirement on government acquisition of location data.

Even if agents could somehow know that a given set of location data would not reveal activities within the home, which they could not, government acquisition of location data still intrudes upon a reasonable expectation of privacy.[305] Because cell phones typically travel in a user's pocket or purse they are "withdrawn from public view" under the Court's reasoning in *Karo*.[306] As the Court explained in that case, agents need to "obtain warrants prior to monitoring a beeper when it has been withdrawn from public view."[307] Agents similarly need to obtain a warrant before acquiring location data. As Justice Stevens explained in *Karo*,

> The concealment of such [electronic devices] on personal property significantly compromises the owner's interest in privacy, by making it impossible to conceal that item's possession and location from the Government, despite the fact that the Fourth Amendment protects the privacy interest in the location of personal property not exposed to public view.[308]

Cell phones travel in users' purses or pockets and stay with them throughout the day and night. An attempt to minimize the privacy intrusion that location data monitoring[309] presents by analogizing it to bumper-beeper monitoring or even visual surveillance by police ignores fundamental differences. The bumper-beepers the Supreme Court considered in the 1980s were tied to cars and gave only a rough indication of how close the device was.[310] Meanwhile, police departments do not have many spare police officers available for twenty-four

304. *Karo*, 468 U.S. at 717.

305. *See, e.g.*, *CSI: Brooklyn*, 736 F. Supp. 2d 578, 582 (E.D.N.Y. 2010) ("[T]echnology has progressed to the point where a person who wishes to partake in the social, cultural, and political affairs of our society has no realistic choice but to expose to others . . . a broad range of conduct and communications that would previously have been deemed unquestionably private."), *rev'd*, Order, *CSI: Brooklyn*, 736 F. Supp. 2d 578 (E.D.N.Y. Nov. 29, 2010), ECF No. 11; *CSI: Austin*, 727 F. Supp. 2d 571, 576, 583 (W.D. Tex. 2010) (citing with approval cases finding a reasonable expectation of privacy in location data); *CSI: Houston I*, 396 F. Supp. 2d at 756–57 (finding support for a reasonable expectation of privacy in location data).

306. *Karo*, 468 U.S. at 716.

307. *Id.* at 718.

308. *Id.* at 735 (Stevens, J., concurring in part and dissenting in part).

309. By monitoring I mean either in real time or through analysis of records of location data.

310. *See* Oral Argument, *supra* note 31, at 53:30–54:00 (EFF lawyer Kevin Bankston describing how the beepers used by the government in *Karo* worked). R

hour physical surveillance, and those officers who do conduct visual surveillance cannot travel in people's pockets or purses.

In *United States v. Maynard*, issued the month prior to *CSI: Third Circuit*, the D.C. Circuit explained how modern tracking technologies implicate the Fourth Amendment in ways that the simple bumper-beepers the Supreme Court considered in the 1980s did not.[311] The D.C. Circuit considered the government's continuous tracking, over four weeks, of a GPS device installed on the defendant's car.[312] The court found the monitoring to constitute a search, notwithstanding a lack of evidence that the monitoring revealed activities inside a home. According to the *Maynard* court, the Supreme Court left open the question of "twenty-four hour surveillance" in *Knotts* when it found that the defendant in that case had "no reasonable expectation of privacy in his movements from one place to another" on public thoroughfares.[313] As for Maynard, he retained a reasonable expectation of privacy in "the totality and pattern of his movements from place to place to place," which is what the police obtained through their continuous GPS surveillance.[314] The *Maynard* court explained that "[a] reasonable person does not expect anyone to monitor and retain a record of every time he drives his car, including his origin, route, destination, and each place he stops and how long he stays there; rather, he expects each of these movements to remain 'disconnected and anonymous.'"[315] Notwithstanding the lack of information about the inside of the home, the *Maynard* court reasoned that society viewed the defendant's expectation of privacy as reasonable because "prolonged GPS monitoring reveals an intimate picture of the subject's life that he expects no one to have—short perhaps of his spouse. The intrusion such monitoring makes into the subject's private affairs stands in stark contrast to the relatively brief intrusion in *Knotts*."[316]

The D.C. Circuit's reasoning that the Supreme Court's bumper-beeper precedents do not cover the use of prolonged GPS tracking applies even more clearly to the use of location data monitoring. As lower courts have begun to realize, location data monitoring through acquisition of location records creates an even more intimate view of

311. 615 F.3d 544, 555–66 (D.C. Cir. 2010). The EFF and ACLU of the National Capital Area submitted an amicus brief in the case. *See id.* at 548.

312. *Id.* at 555–56.

313. *Id.* at 556–57 (quoting United States v. Knotts, 460 U.S. 276, 281, 283 (1983)) (internal quotation marks omitted).

314. *Id.* at 558.

315. *Id.* at 563 (quoting Nader v. Gen. Motors Corp., 255 N.E.2d 765, 772 (N.Y. 1970) (Breitel, J., concurring)).

316. *Id.*

one's personal activities than the GPS monitoring in *Maynard*.[317] In short, location data provides a continuous, pervasive, comprehensive, and almost universally available view into the lives of ordinary people.

V. REASONABLE EXPECTATIONS OF PRIVACY UNDER *SMITH*, *MILLER*, *KATZ*, AND THE FOUR FACTOR TEST

A. Miller *and* Smith *Do Not Apply*

As discussed, the majority in *CSI: Third Circuit* rejected the government's suggestion that it decide the case by making analogies to *Miller v. United States*[318] and *Smith v. Maryland*.[319] In particular, the government claimed that because targets voluntarily disclose location data to their service providers, who retain such information in ordinary business records, the targets forfeit any reasonable expectations of privacy in the data under *Miller*.[320] As for *Smith*, the government asserted that the case establishes a rule under which *non-contents* data receive none of the Fourth Amendment protection accorded to the *contents* of communications.[321] The Third Circuit majority properly rejected both of the government's arguments, but I elaborate on its reasons for doing so because the government has made similar arguments for many years, and those arguments have been crucial in undermining privacy rights in online communications.[322]

Several key distinctions between location data and the data sought in *Miller* and *Smith* render those decisions inapplicable to location data.[323] Unlike the records of deposits and checks the government subpoenaed from Miller's bank, location data records are not actively and voluntarily created by cell phone users, who likely lack any knowledge of what location data their service providers record.[324]

---

317. *See* cases cited *supra* note 27. R

318. 425 U.S. 435 (1976).

319. 442 U.S. 735 (1979).

320. Brief for the United States, *supra* note 44, at 26–28. R

321. *See* Government Reply Brief at 3, *CSI: Third Circuit*, 620 F.3d 304 (3d Cir. 2010) (No. 08-4227) (drawing a distinction between the protection given to contents and non-contents data).

322. *See generally* Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373 (2006) (describing the application of the third-party rule in federal and state cases).

323. My thinking about these questions has benefitted tremendously from discussions with Kevin Bankston and Jennifer Granick of EFF. The Civil Liberties Amici did an excellent job distinguishing the *Smith* and *Miller* cases in their brief in the *CSI: Third Circuit* litigation. *See* Civil Liberties Amici, Third Circuit Brief, *supra* note 80, at 19–22 (distinguishing location data from dialed telephone numbers and bank records). R

324. *Id.*

As the Third Circuit majority recognized, "A cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way," because users are unlikely to know that providers collect and store the information.[325] Similarly, the historical nature of the location data does not detract from users' reasonable expectations of privacy in it. Finally, far from establishing a broad "non-contents" rule, *Smith* covered only the telephone numbers the target dialed and limited its reasoning to that data.[326]

1. Miller *and the "Third Party" Rule*

Location data is not an unprotected third-party record—to the extent that such a thing exists.[327] In *Miller*, the Supreme Court rejected the defendant's claim of a reasonable expectation of privacy in the bank's records of his financial transactions.[328] As a result, Miller could not complain when government agents did not first obtain a warrant based on probable cause before they compelled the bank to turn over records of Miller's banking transactions.[329] While the Supreme Court did permit warrantless access to Miller's bank records stored by his bank, it did not mandate a broad "third party" rule under which users forfeit constitutional protection in things they voluntarily share with third parties.[330] Instead, it engaged in an assumption of risk analysis which, when properly considered in the location data context, does not yield the same result.

a. Location Data Is Not Stored in "Ordinary Business Records"

The *Miller* Court held that customers assumed the risk that their banks would disclose records of their deposits and copies of their statements because banks retained those records in the ordinary course of their business.[331] Despite the government's repeated attempts to characterize the location data in the case as contained in "routine business records,"[332] it failed to produce such a business re-

325. *CSI: Third Circuit*, 620 F.3d 304, 317 (3d Cir. 2010).

326. Admittedly, the decision, like *Miller*, does have broader dicta. *See Smith*, 442 U.S. 735, 743–44 (1979) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." (citing United States v. Miller, 425 U.S. 435, 442–44 (1976))).

327. *See* Brief for the United States, *supra* note 44, at 26–28 (arguing that location data is a third-party business record for which there is no reasonable expectation of privacy). R

328. *Miller*, 425 U.S. at 442–43.

329. *Id.* at 444–46.

330. *Id.* at 445. *But see* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009) (quoting language from *Miller* to support a broader third-party doctrine).

331. *Id.* at 442–43.

332. Brief for the United States, *supra* note 44, at 2, 4, 26, 27, 35. R

cord in the *CSI: Third Circuit* litigation. The government's "exemplar" that it identified as resembling a location data record looked much more like a customized report drawn from a service provider database than a bill that a customer would actually see.[333] In another location case, the provider apparently furnished raw data to the government rather than ordinary business records.[334] In *Miller*, the Supreme Court found a waiver of privacy in the fact that the customer knew the bank would retain his records and the bank employees would encounter those records in the ordinary course of their business.[335] Because the same cannot be said for location data, a *Miller*-based "business records" argument fails.[336]

In addition, it was not the bank's mere ability to produce the records that precluded Miller's Fourth Amendment claim, but rather the nature of the records themselves and Miller's relationship to them that defeated his privacy expectations.[337] The *Miller* Court explained that it had to "examine the nature of the particular documents sought to be protected in order to determine whether there is a legitimate 'expectation of privacy' concerning their contents."[338] Much more so than the records of a few checks and deposit slips at issue in *Miller*,[339] location data provides detailed information about people's communications as well as their movements and activities.[340] Because location data will often disclose extensive personal information about where users go and how long they spend there, it much more closely resem-

333. *See supra* text accompanying notes 221–22. R

334. *CSI: SDNY*, 405 F. Supp. 2d 435, 437–38 (S.D.N.Y. 2005).

335. *See Miller*, 425 U.S. at 442 ("All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.").

336. *See* United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) ("*Miller* involved simple business records, as opposed to the potentially unlimited variety of 'confidential communications' at issue [in a stored email case]."); *see also PCTDD: EDNY*, 515 F. Supp. 2d 325, 337 (E.D.N.Y. 2007) (rejecting an extension of the *Miller* "logic" because the information sought was not kept by service providers in the ordinary course of their businesses).

337. *See PCTDD: EDNY*, 515 F. Supp. 2d at 337–38 (noting that a test based solely on a third party's ability to access a given piece of data would lead to unacceptable consequences (citing Warshak v. United States, 490 F.3d 455, 470 (6th Cir. 2007), *vacated en banc*, 532 F.3d 521 (6th Cir. 2008))).

338. *Miller*, 425 U.S. at 442.

339. Congress disagreed with the Supreme Court that bank records should not be private when it passed the Right to Financial Privacy Act of 1978 two years after the *Miller* decision and guaranteed notice to targets of bank subpoenas and an opportunity to be heard on the privacy of the records sought. *See* Pub. L. No. 95-630, §§ 1100–22, 92 Stat. 3697, 3697–3710 (codified at 12 U.S.C. §§ 3401–22 (2006))).

340. *See supra* Part III.A. Although he might have, Miller raised no First Amendment claim in his case. *See Miller*, 425 U.S. at 444 n.6; *see also infra* note 396 (discussing First Amendment interests in location data). R

bles the private communications the *Miller* Court found subject to a reasonable expectation of privacy than the banking records it did not.[341]

b. Customers Do Not Actively and Knowingly Convey Location Data

In addition to the almost public nature of the bank records, the Supreme Court found that Miller had "voluntarily conveyed" his financial information to the bank and thereby waived his reasonable expectation of privacy in it.[342] Under the Court's logic, Miller assumed the risk that the bank would disclose its records of his transactions because he voluntarily and affirmatively made the bank a party to those transactions.[343] That reasoning seems questionable because one has little choice but to use a bank if one wants to engage in modern business.[344] Nonetheless, it is true that when Miller took the affirmative step of writing a check, he must have known that it was an instruction to the bank's employees to pay money to the check's payee. So while the Court's analogy of banking to confiding in one's friends seemed a bit stretched in *Miller*, it does not entirely lack justification.[345]

Stretching the Supreme Court's analogy to the location data context, however, would be going too far. In the two cases upon which *Miller* relied, *United States v. White*[346] and *Hoffa v. United States*,[347] parties to communications, which the defendants had affirmatively and voluntarily made to them, disclosed those communications to law en-

341. *See Miller*, 425 U.S. at 442 ("The checks are not confidential communications but negotiable instruments to be used in commercial transactions.").

342. *Id.*

343. *Id.* at 443 ("The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."). In *California Bankers Ass'n v. Shultz*, decided two years before *Miller*, the Supreme Court held that banks are parties to customer's financial transactions. 416 U.S. 21, 48 (1974).

344. *Miller*, 425 U.S. at 451 (Brennan, J., dissenting) ("For all practical purposes, the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account.").

345. I have criticized that reasoning and argued that its strained logic counsels in favor of limiting *Miller* to its facts. *See* Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-mail*, 2008 U. CHI. LEGAL F. 121, 145–56 (arguing against extending *Miller* to support a broad third-party doctrine); *see also* Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1397–1412 (2004) (criticizing the reasoning in *Miller* based on an understanding of its precedents and advocating for a limited understanding of *Miller*'s holding).

346. 401 U.S. 745 (1971).

347. 385 U.S. 293 (1966).

forcement agents.[348] In both cases, the Supreme Court found that the defendants had assumed the risk of disclosure and had no Fourth Amendment interest in preventing it.[349] Cell phone service providers are third parties to their users' calls, not second parties with whom the users are communicating.[350] Because *White* and *Hoffa* addressed disclosures by a party to the communication, or second party disclosures, as did *Miller*, none of these cases establishes a broad third-party rule under which a person waives a privacy interest in any information that a third party holds.[351]

To find *White*, *Hoffa*, and *Miller* controlling in the location data context, one would need to find that cell phone users assume the risk that their providers will be compelled to disclose their location data in the same way that the defendants in the three precedent cases assumed the risk of disclosure by the parties to their communications.[352] But, cell phone users do not voluntarily, actively, and knowingly convey location data to providers.[353] Instead, cell phone systems generate location data automatically, without any input by the user.[354] That is clearly true for registration and duration information, which is generated without any action by the cell phone user, but even initiation and termination information is generated by the provider's system to route the call. Consequently, location data differs from the information on a check or deposit slip that a bank customer handwrites as an instruction to the bank and the telephone numbers that a

348. *White*, 401 U.S. at 746–47; *Hoffa*, 385 U.S. at 295.

349. *White*, 401 U.S. at 752 (explaining that "the law permits . . . authorities to use the testimony of those associates who for one reason or another have determined to turn to the police" and permits those associates to record or transmit their conversations with the wrongdoer); *Hoffa*, 385 U.S. at 302 (finding no Fourth Amendment interest in incriminating statements voluntarily revealed to a confidant).

350. *See* Bellia & Freiwald, *supra* note 345, at 164 (distinguishing between "cases in which the ISP" is a "recipient of an intended communication," and therefore a second party, and those in which the ISP is a "third party to a communication *between two others*" (emphasis added)); *see also* United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (referring to the Bellia and Freiwald article and rejecting applicability of *Miller* to stored e-mail because the service provider "was an *intermediary*, not the intended recipient of the emails" (citing Bellia & Freiwald, *supra* note 345, at 165)). R

351. *See* Bellia & Freiwald, *supra* note 345, at 164–67. R

352. *See id.* at 141–47 (discussing the difference between voluntary disclosures and compelled disclosures).

353. *See CSI: Houston III*, Nos. H-10-998M et al., 2010 WL 4286365, at *13 (S.D. Tex. Oct. 29, 2010) ("In sum, *Miller* and *Smith* do not permit warrantless law enforcement access to all historical cell site data, because the user has not 'knowingly exposed' or 'voluntarily conveyed' that information to the provider, as those phrases are ordinarily understood.").

354. *CSI: Houston I*, 396 F. Supp. 2d 747, 756–57 (S.D. Tex. 2005) (explaining that users do not voluntarily convey information data, which is "transmitted automatically during the registration process, entirely independent of the user's input, control, or knowledge").

telephone user actively dials into the telephone.[355] Some courts have limited the location data available only to that recorded when targets initiate calls.[356] Cell phone users, however, do not voluntarily convey location data to providers, or tell their providers to record it.[357] Quite unlike bank statements, which are designed for customer review,[358] customers can hardly know what location data their providers store when the picture remains so opaque.[359] At the same time, customers have no reason to know when, how, or why employees would access their location data, whether in the ordinary course of business or not.[360]

Because cell phone users do not affirmatively and knowingly convey location data to service providers, the mere production of location data does not defeat customers' reasonable expectations of privacy in that data. The majority in *CSI: Third Circuit* properly recognized this point.[361] Other cases have affirmed that mere access, which is what providers have regarding cell phone location data, does not defeat a user's expectations of privacy in that data.[362]

For example, the Sixth Circuit reasoned in *Warshak* that a user's consent to service provider access does not forfeit a reasonable expec-

355. Smith v. Maryland, 442 U.S. 735, 742 (1979) ("All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed."). The *Smith* Court discussed how, not long before its decision, users had to actually convey phone numbers verbally to live operators, and noted that the automation of the process should not make a difference in the assumption of risk analysis. *Id.* at 744–45.

356. *See supra* note 135 and accompanying text. R

357. Perhaps we can draw an exception for some location applications in which the user's location is the content of the communication. *See supra* note 117 (discussing Gidari testimony). R

358. The *Smith* court emphasized the customer's knowledge that the phone company could collect and record telephone numbers and did so in the ordinary course of its business. *See Smith*, 442 U.S. at 742–43 (discussing the presence of dialed numbers on customer bills and the information in telephone directories indicating a phone company's ability to record dialed numbers to prevent harassment and for other purposes).

359. *See supra* Part III.B.1 (discussing the lack of information about location data collection practices); *see also CSI: Third Circuit*, 620 F.3d 304, 317–18 (3d Cir. 2010) (discussing cell phone customers' lack of knowledge of provider collection and storage practices).

360. *CSI: Third Circuit*, 620 F.3d at 317–18.

361. *Id.* (rejecting applicability of the *Smith* and *Miller* cases to location data).

362. *See, e.g.*, Quon v. Arch Wireless Operating Co., 529 F.3d 892, 905–06 (9th Cir. 2008) (stating that it was "irrelevant" that the cellular provider could access the contents of text messages because "[a]ppellants did not expect that Arch Wireless would monitor their text messages, much less turn over the messages to third parties without Appellants' consent"), *rev'd and remanded sub nom.* City of Ontario v. Quon, 130 S. Ct. 2619 (2010); *see also* United States v. Long, 64 M.J. 57, 63 (C.A.A.F. 2006) (reasoning that consent to monitoring did not imply consent to "engage in law enforcement intrusions . . . in a manner unrelated to maintenance of the e-mail system").

tation vis-à-vis law enforcement access. Service provider access is sufficiently extensive "to snuff out a reasonable expectation of privacy" only in limited situations, such as when the provider "expresses an intention to 'audit, inspect, and monitor' its subscriber's emails."[363] Notably, the Sixth Circuit rejected a monolithic expectation of privacy that is defeated whenever the information at issue is seen by anyone. Instead, and appropriately, the court recognized that we may permit a service provider to run its business without relinquishing the protections of the warrant requirement—the interposition of a neutral magistrate to review the propriety and need for the government to pry into our personal communications.

c. The Historical Nature of Location Data Does Not Change the Analysis

Some lower court cases have recognized that acquisition of forward-looking, real-time location data requires law enforcement to obtain a warrant but acquisition of backward-looking, historical data does not.[364] In distinguishing between historical and real-time location data, courts have generally based their reasoning on *Miller* and *Smith*, without offering any additional analysis of why to treat historical data differently.[365] As is true with non-content data, the ECPA treats stored (and therefore historical) data as easier to acquire, but that statutory distinction does not determine the constitutional analysis. Given that Congress can hardly have considered storage of location data in 1986 when it passed the ECPA, its decision to make it easier for agents to acquire stored records generally should carry little or no weight on the issue of location data.[366]

---

363. United States v. Warshak, 631 F.3d 266, 287 (6th Cir. 2010) (quoting Warshak v. United States, 490 F.3d 455, 472 (6th Cir. 2007), *vacated en banc*, 532 F.3d 521 (6th Cir. 2008)).

364. *See CSI: Pittsburgh*, 534 F. Supp. 2d 585, 600 n.42 (W.D. Pa. 2008) (collecting cases that distinguish forward-looking and backward-looking data), *aff'd*, No. 07-524M, 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008), *vacated*, 620 F.3d 304 (3d Cir. 2010).

365. *See, e.g.*, United States v. Benford, No. 2:09 CR 86, 2010 WL 1266507, at *2–3 (N.D. Ind. Mar. 26, 2010) ("Having no Seventh Circuit precedent on the issue, this court is persuaded by the well-reasoned decision of the *Suarez-Blanca* court that the logic of the Supreme Court in *Smith* and *Miller* should be extended to cell-site data."); United States v. Suarez-Blanca, No. 1:07-CR-0023-MHS/AJB, 2008 WL 4200156, at *8 (N.D. Ga. Apr. 21, 2008) (relying on *Smith* and *Miller* in determining that "historical cell site information is akin to other business records maintained in the course of business"); *see also CSI: Houston II*, 622 F. Supp. 2d 411, 418 n.8 (S.D. Tex. 2007) ("This court concludes that a request for *historical* cell-site data when the phone is idle does not raise the same concerns as might a request for real-time cell-site data when the phone is idle . . . .").

366. Indeed, a group of major technology companies, nonprofit organizations, civil liberties groups, and academics have formed the Digital Due Process coalition and recom-

From the perspective of the Fourth Amendment, law enforcement acquisition of historical location data can intrude into personal privacy even more than acquisition of real-time or prospective location data.[367] A law enforcement agent seeking prospective location data could get an order on August 1st to track the target's movements for three months, but then would have to wait until October 31st to have three months of location data to review. Alternatively, the agent could ask the provider for historical location data and immediately obtain a year's worth or more of the target's location data.[368] The length of time a target's cell phone generates records and the service provider stores them set the only limit on the scope of the historical records the law enforcement agent may acquire.

In addition, historical location data may be at least as informative to law enforcement agents as prospective location data. Historical data may indicate with whom, where, and for how long targets have met. It may put a target at the scene of a crime at the time the crime was committed and thereby refute the target's alibi.[369] Magistrate Judge Lenihan appropriately found that "the privacy and associational interests implicated [by acquisition of location data] are not meaningfully diminished by a delay in disclosure."[370] Other courts have also recognized that law enforcement acquisition of records of historical location data, by virtue of creating a target's complete digital profile,

---

mended that Congress amend the ECPA to remove distinctions between the treatment of historical and forward-looking data. *See* DIGITAL DUE PROCESS, http://www.digitaldueprocess.org (last visited Mar. 21, 2011).

367. *See* Freiwald, *First Principles*, *supra* note 5, ¶¶ 61–76 (arguing that stored data implicates reasonable expectations of privacy as much as forward-looking data unless it is isolated to a single point in time). The Digital Due Process coalition recommends that Congress protect historical location and electronic communications data just the same as it protects prospective data. *See Background*, DIGITAL DUE PROCESS, http://www.digitaldueprocess.org/index.cfm?objectid=C00D74C0-3C03-11DF-84C7000C296BA163 (last visited Mar. 21, 2011) ("The government should obtain a search warrant based on probable cause before it can track, prospectively or retrospectively, the location of a cell phone or other mobile communications device."). R

368. Historical location data could contain data of quite recent vintage. *See June Hearings*, *supra* note 14, at 8 (statement of Stephen Wm. Smith, U.S. Mag. J.) ("How is 'historical' to be defined—one second after transmission? One hour? One day? One month?" (citing Gidari, *supra* note 227, at 544)); *see also id.* (noting ambiguity whereby "prospective [location data] may be understood as referring to that generated anytime after the court issues its order"). R R

369. *See supra* Part III.B.3. (illustrating the inferences that can be drawn from historical location data).

370. *CSI: Pittsburgh*, 534 F. Supp. 2d 585, 612 (W.D. Pa. 2008), *aff'd*, No. 07-524M, 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008), *vacated*, 620 F.3d 304 (3d Cir. 2010).

should receive the same Fourth Amendment protection as acquisition of location data in real-time or prospectively.[371]

2. Smith *Does Not Establish a "Non-Contents" Rule*

Besides citing *Smith* as further support for its third party rule argument, the government has urged courts that the "non-contents" nature of location data renders it unprotected by the Fourth Amendment under *Smith*.[372] As with the historical/forward-looking distinction, the content/non-content distinction has its origin in the SCA, which Congress passed in 1986,[373] well before the explosion of new communications technologies and associated non-contents attributes. Again, the statutory distinction does not determine the constitutional analysis.

Two recent cases illustrate how courts shortcut the analysis when they rely on a supposed non-contents rule. In *United States v. Suarez-Blanca*[374] and *United States v. Benford*,[375] two federal district courts granted government applications to compel the disclosure of location data on facts apparently similar to those in *CSI: Third Circuit*. In *Suarez-Blanca*, the government sought initiation, termination, and duration data but apparently not registration or GPS data.[376] In *Benford*, the court vaguely described the information sought as data "identifying which cell tower communicated with the cell phone while it was turned on,"[377] which suggests that the location data included registration data, as well. Each court found the acquisition proposed would not implicate the Fourth Amendment,[378] and the *Benford* court explicitly adopted the reasoning of the *Suarez-Blanca* decision.[379] Neither

371. *See, e.g.*, *In re* Applications of the U.S. for Orders Pursuant to Title 18, United States Code, Section 2703(d) to Disclose Subscriber Info. & Historical Cell Site Info. for Mobile Phone Identification Nos: (XXX) XXX-AAAA, (XXX) XXX-BBBB, & (XXX) XXX-CCCC, 509 F. Supp. 2d 64, 76 (D. Mass.) (finding no "material difference" between "real time," prospective, and historical tracking), *rev'd*, 509 F. Supp. 2d 76 (D. Mass. 2007).

372. *See* Government Reply Brief, *supra* note 321, at 3. R

373. Act of Oct. 21, 1986, Pub. L. 99-508, sec. 201, 100 Stat. 1848, 1860–68 (codified as amended at 18 U.S.C. §§ 2701–10 (2006)).

374. No. 1:07-CR-0023-MHS/AJB, 2008 WL 4200156 (N.D. Ga. Apr. 21, 2008).

375. No. 2:09 CR 86, 2010 WL 1266507 (N.D. Ind. Mar. 26, 2010).

376. *Suarez-Blanca*, 2008 WL 4200156, at *2. It is unclear from the decision whether the government acquired triangulation data or not. *See id.* at *11 ("The Court recognizes that the government sought information about three towers that were used in making calls, but there has not been any showing that the use of the three towers allows the government to triangulate the exact location of a particular defendant."). If the "three towers" were for each call, then that information would certainly permit triangulation.

377. *Benford*, 2008 WL 1266507, at *1.

378. *Id.* at *3; *Suarez-Blanca*, 2008 WL 4200156, at *11.

379. *Benford*, 2008 WL 1266507, at *3.

court, however, engaged in a full consideration of reasonable expectations of privacy. In a cursory discussion that ignored both the differences in the nature of location information and the way it is created, the *Suarez-Blanca* court analogized location data to the telephone numbers dialed in *Smith v. Maryland*.[380] The *Suarez-Blanca* court also adopted the government's broad reading of the third-party rule and cited *Smith* and *Miller* for the proposition that the records' status in the storage facilities of the service provider deprived the defendant of a reasonable expectation of privacy.[381] The *Benford* court did not discuss how rich the location data might be if it were recorded at regular and frequent intervals throughout the day, but instead agreed, without further discussion, that "individuals do not have a legitimate expectation of privacy in the information showing which cell phone tower communicated with her or her cell phone at a particular moment in the past."[382]

Indeed, the information that a pen register revealed at the time of *Smith* was much more limited and therefore less revealing than location data.[383] It neither indicated "the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed."[384] Location data, by contrast, provides revealing information about the whereabouts of a user that directly implicates his right to privacy.

Magistrate Judge Smith in the Southern District of Texas recently issued a decision that recognized the inapplicability of *Smith* to location data.[385] Judge Smith distinguished *Smith* by noting that "[u]nlike

380. *See Suarez-Blanca*, 2008 WL 4200156, at *8 ("[A] cell phone user voluntarily dials a number and as a result voluntarily uses the cell phone provider's towers to complete the number. The cell phone provider retains records of which towers were used in dialing a call. By voluntarily using the equipment, the cell phone user runs the risk that the records concerning the cell phone call will be disclosed to police.").

381. *Id.* The court also explained that the bumper-beeper precedents did not apply because there was no evidence that the tracking divulged information inside a home. *Id.* at *9–10.

382. *Benford*, 2010 WL 1266507, at *2.

383. In addition, the telephone numbers at issue in *Smith* vary considerably from location data, as do the risks users voluntarily assume about each. *See* Civil Liberties Amici, Third Circuit Brief, *supra* note 80, at 19–22. R

384. United States v. N.Y. Tel. Co., 434 U.S. 159, 167 (1977). It obviously did not reveal the caller's physical location, except to the extent it could be determined from his telephone number.

385. *See CSI: Houston III*, Nos. H-10-998M et al., 2010 WL 4286365, at *7–14 (S.D. Tex. Oct. 29, 2010). The government challenged Judge Smith's decision, and I submitted an Amicus Brief to the district court supporting Judge Smith's denial of the government's applications, as did the EFF and ACLU. Brief of Amicus Curiae Susan Freiwald in Opposition to the Government's Request for Review, *CSI: Houston III*, 2010 WL 4286365 (Nos. H-10-998M et al.).

a wireline phone in a fixed location such as a residence, a cell phone accompanies its user throughout the day, revealing when the user leaves the house and when he returns."[386] More colorfully, Judge Smith described how "[t]wo months' worth of hourly tracking data will inevitably reveal a rich slice of a user's life, activities, and associations . . . . If the telephone numbers dialed in *Smith v. Maryland* were notes on a musical scale, the location data sought here is a grand opera."[387]

Beyond its "limited capabilities," the pen register at issue in *Smith* could acquire information only after the government installed it—prospectively or in real-time.[388] As mentioned, historical location data includes comprehensive information about past travels and activities for whatever period of time the provider retains the data. Only the particularity and probable cause requirements of the Fourth Amendment can prevent the government from fishing through potentially vast amounts of location data in violation of Fourth Amendment principles.

To determine whether subscribers have a reasonable expectation of privacy in their location data, courts must engage in the two-part analysis outlined in *Katz*, rather than simply characterize the information as a third party record and consider the inquiry finished.[389] Similarly, the mere categorization of location data as either non-contents or historical does not end the analysis. In fact, courts have sometimes called data "content" after determining that its acquisition implicates a reasonable expectation of privacy, rather than determining expectations of privacy based on the characterization of the data in the first place.[390] Under a reasonable expectation of privacy analysis, location data implicates the Fourth Amendment, and its acquisition by law en-

386. *CSI: Houston III*, 2010 WL 4286365, at *7 n.67. Judge Smith also discussed at some length why *United States v. Miller* did not govern location data. *See id.* at *12–13; *supra* note 353. R

387. *CSI: Houston III*, 2010 WL 4286365, at *14.

388. *See* Smith v. Maryland, 442 U.S. 735, 742 (1979) (describing the "search" question as "rest[ing] upon a claim" of "a 'legitimate expectation of privacy' regarding the numbers he dialed on his phone").

389. *See* Freiwald, *First Principles*, *supra* note 5, ¶¶ 36–49 (criticizing the tendency of courts to rely on analytic shortcuts like a "third-party" rule and a "content/non-contents" distinction rather than analyzing reasonable expectations of privacy). R

390. *See, e.g.*, United States v. Forrester, 512 F.3d 500, 510–11 & n.6 (9th Cir. 2008) (holding that IP address collection by law enforcement does not implicate the Fourth Amendment, but finding that URL collection "might be more constitutionally problematic" because the latter "reveals much more information," such as what articles we read, and thus must be treated as content).

forcement should proceed only after agents obtain a warrant based on probable cause. I turn to that analysis now.

B. Reasonable Expectations of Privacy in Location Data

When the "government violates a subjective expectation of privacy that society recognizes as reasonable," it conducts a Fourth Amendment search.[391] The Supreme Court has used that formulation repeatedly since Justice Harlan first used it in his concurring opinion in *Katz v. United States* in 1967.[392] In *Katz*, the Supreme Court found for the first time that the Fourth Amendment protects telephone calls from warrantless government acquisition.[393] Because government agents also intrude upon a cell phone user's reasonable expectation of privacy when they acquire his location data, they must either obtain a warrant based on probable cause or establish an exception to the warrant requirement.[394] Common uses of cell phone technology support a subjective expectation of privacy in location data, and applicable precedents support an objective expectation.

1. Subjective Expectations of Privacy in Location Data

Most cell phone users would be unpleasantly surprised, if not outraged, to learn that a law enforcement agent could gain access to their location information without first obtaining a warrant based on a showing of probable cause. Location data may reveal to law enforcement agents that a cell phone user has attended an Alcoholics Anonymous meeting, sought AIDS treatment, or visited an abortion clinic.[395] It may also divulge when and where a user gave confession, viewed an X-rated movie, or protested at a political rally. Knowledge that the government could keep track of such information could easily inhibit valuable and constitutionally protected activities.[396] As I discussed

391. Kyllo v. United States, 533 U.S. 27, 33 (2001).

392. 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

393. *Id.* at 356–58 (majority opinion).

394. *See id.* at 359 ("Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures."); *CSI: Pittsburgh*, 534 F. Supp. 2d 585, 610–11 (W.D. Pa. 2008) ("For reading the statutes in the manner advocated by the Government would, as to at least a substantial portion of the information at issue, violate Americans' reasonable expectation of privacy in any cell-phone-derived information/records as to their physical movements/locations by authorizing *ex parte* disclosure of that information with no judicial review of the probable cause."), *aff'd*, No. 07-524M, 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008), *vacated*, 620 F.3d 304 (3d Cir. 2010).

395. *See id.* at 586 n.6.

396. In addition to implicating Fourth Amendment interests, location data disclosure may implicate First Amendment rights of expression and association. *See generally* Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 165–76 (2007)

above regarding the inferences one can draw from location data, as well as the precision that location data has the potential to yield, fears that location data will provide an intrusive eye onto a target's private activities are not overblown.[397]

Not surprisingly, cell phone users regard access to their location data as yielding private data about their locations. A research report found that seventy-three percent of cell phone users surveyed favored "a law that required the police to convince a judge that a crime has been committed before obtaining [historical] location information from the cell phone company."[398] Seventy-two percent also supported a law requiring the police to give notice to the user before the police may obtain historical records of location data.[399] Both findings demonstrate that most users view their location data as private information and expect it to remain private absent a compelling need for access.[400]

People surely entertain a subjective expectation of privacy in their location data and would not expect police to have access to it without first demonstrating a compelling justification to a reviewing court. As Justice Stevens wrote, perhaps coincidentally in 1984, "As a general matter, the private citizen is entitled to assume, and in fact does assume, that his possessions are not infected with concealed electronic devices."[401] For the same reasons that people expect a law enforcement agent to obtain a warrant from a neutral magistrate before he may bug their conversations, monitor their phone calls, or subject them to silent video surveillance, people would surely expect judicial

---

(identifying implications of electronic surveillance for First Amendment interests); *see also* Mulligan, *supra* note 113, at 1587 (finding that the Supreme Court "calls for exacting scrutiny under the Fourth Amendment when First Amendment interests are implicated"); *see also* Lockwood, *supra* note 172, at 316 ("[T]he door is open for an Orwellian scenario whereby law enforcement agents could monitor not just criminals, but anyone with a cell phone."). R R

397. *See supra* Part III.

398. Jennifer King & Chris Jay Hoofnagle, Research Report: A Supermajority of Californians Supports Limits on Law Enforcement Access to Cell Phone Location Information 8–9 (unpublished manuscript) (Apr. 18, 2008), *available at* http://ssrn.com/abstract=1137988.

399. *Id.* at 8.

400. Eighty-three percent of respondents agreed that police should be able to track them in an emergency, *id.* at 7, a view which statutes reflect, *see, e.g.*, 18 U.S.C. § 2518(7) (2006) (providing a forty-eight hour period during which agents may wiretap without a warrant in an emergency); *see also* Lockwood, *supra* note 172, at 316 ("[P]eople are likely to reject the prospect of turning every cell phone into a tracking device.").

401. United States v. Karo, 468 U.S. 705, 735 (1984) (Stevens, J., concurring in part and dissenting in part).

oversight of an agent's use of their cell phones to track their movements and activities.

2. Objective Expectations of Privacy in Location Data

The objective prong of the reasonable expectation of privacy test ultimately requires a court to make a normative finding about whether users should be entitled to view the object of the search as private. As Justice Harlan explained in a case decided a few years after *Katz*, "The critical question, therefore, is whether under our system of government, as reflected in the Constitution, we should impose on our citizens the risks of the electronic listener or observer without at least the protection of a warrant requirement."[402] The critical question in the location data cases is whether, in our society, law enforcement agents may use cell phone technology as a window for constant surveillance of our citizens without the procedural limits imposed by the Fourth Amendment. The answer must be "no."

By analogy, the expectation of privacy users have in their location data should be objectively reasonable. Just as the Supreme Court recognized in *Katz* that warrantless government eavesdropping violated the privacy on which the target "justifiably relied while using the telephone booth," so too does warrantless access to location data violate the privacy on which cell phone users justifiably rely while using their cell phones.[403] When describing government acquisition of telephone conversations as a search under the Fourth Amendment, the Supreme Court in *Katz* reasoned that "[t]o read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication."[404] To deny Fourth Amendment protection to location data would similarly ignore the vital role that mobile telephony has come to play in the lives of the over 290 million subscribers in the United States.[405]

In the *Warshak* case, the Sixth Circuit recognized the need for a normative approach to determining reasonable expectations of privacy in new communications media. In general, the court recognized that "[a]s some forms of communication begin to diminish, the Fourth Amendment must recognize and protect nascent ones that

402. United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting).

403. Katz v. United States, 389 U.S. 347, 353 (1967); *see* Quon v. Arch Wireless Operating Co., 529 F.3d 892, 904–06 (9th Cir. 2008), *rev'd and remanded sub nom.* City of Ontario v. Quon, 130 S. Ct. 2619 (2010) (finding text message users to be entitled to privacy in their messages just as telephone callers are entitled to the privacy of their telephone calls).

404. *Katz*, 389 U.S. at 352.

405. *See supra* note 260 and accompanying text. R

arise."[406] Regarding e-mail in particular, the court found that it "plays an indispensable part in the Information Age" and "requires strong protection under the Fourth Amendment; otherwise, the Fourth Amendment would prove an ineffective guardian of private communication, an essential purpose it has long been recognized to serve."[407]

The *Warshak* court's recognition that "the Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish,"[408] supports a finding of an objective expectation of privacy in location data.

C. Electronic Surveillance Under the Four Factor Test

Location data shares those features of other types of electronic surveillance that the Supreme Court and lower courts have found to require high procedural hurdles and extensive judicial oversight. In *Berger v. New York*,[409] the Supreme Court explained that electronic eavesdropping techniques presented "inherent dangers" and therefore required more "judicial supervision" and "protective procedures" than even "conventional" searches.[410] When they determined that the Fourth Amendment required the same procedural hurdles for use of silent video surveillance, several federal courts of appeals elaborated on which features necessitated heightened judicial oversight. Judge Posner, in a widely followed Seventh Circuit decision, explained that the *hidden*, *continuous*, *indiscriminate*, and *intrusive* nature of electronic surveillance raises the likelihood and ramifications of law enforcement abuse.[411]

When agents compel the disclosure of location data, they use a technique that is similarly hidden, continuous, indiscriminate, and intrusive.[412] Unlike the search of a home, which is usually subject to view either by the occupant of the home or his neighbors, government acquisition of location data is *hidden*. Just as a telephone user

406. United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010).

407. *Id.*

408. *Id.* at 285 (citing Kyllo v. United States, 533 U.S. 27, 34 (2001)).

409. 388 U.S. 41 (1967).

410. *Id.* at 60; *see also id.* at 64 (noting that a New York statute permitting eavesdropping with insufficient judicial oversight constituted a "general warrant" in violation of the Fourth Amendment).

411. United States v. Torres, 751 F.2d 875, 882–85 (7th Cir. 1984); *see also id.* at 882 (finding it "unarguable that television surveillance is exceedingly intrusive . . . and inherently indiscriminate, and that it could be grossly abused—to eliminate personal privacy as understood in modern Western nations"); Freiwald, *Online Surveillance*, *supra* note 3, at 79–80. R

412. In fact, law enforcement agents seeking location data should perhaps satisfy the heightened procedural requirements imposed on government wiretappers.

does not know when a law enforcement agent has wiretapped his call, a cell phone user does not know when a law enforcement agent has acquired his location data. That significantly raises the risk that agents will exceed the scope of a proper investigation with impunity.[413] In addition, acquisition of location data is *continuous*, like the acquisition of telephone conversations and video surveillance footage. The longer the period an investigation spans, the greater the likelihood that the government will conduct surveillance without sufficient justification.

Besides being hidden and continuous, acquisition of location data is inherently *indiscriminate* in that much of such data will not be incriminating but will rather reveal activities that are entirely unrelated to criminal actions. For example, and as mentioned, the government's application in *CSI: Third Circuit* sought location data pertaining to a user upon whom apparently no individualized suspicion had fallen.[414] As discussed previously, the government has engaged in expansive acquisitions of location data.[415] The risk of acquiring location information about non-incriminating activities counsels in favor of substantial judicial oversight to reduce unwarranted invasions of privacy and to ensure that searches do not become government fishing expeditions. Although it is possible that a request could be so circumscribed in time and place that the data could turn out to be unrevealing, agents cannot know that when they request the data initially.[416] In addition, government agents are unlikely to seek such unrevealing information in the first place.

One could go so far as to argue that agents should obtain a Title III (Wiretap Act) court order before they may compel service providers to disclose location data.[417] When the federal appellate courts considered the proper procedural hurdle for law enforcement use of silent video surveillance in locations in which the subjects held reasonable expectations of privacy, they imposed the substantive requirements of the Wiretap Act as a matter of Fourth Amendment law

413. *See CSI: Pittsburgh*, 534 F. Supp. 2d 585, 586 & n.7 (W.D. Pa. 2008) (noting that the ex parte nature of location data applications makes them "particularly vulnerable to abuse"), *aff'd*, No. 07-524M, 2008 WL4191511 (W.D. Pa. Sept. 10, 2008), *vacated*, 620 F.3d 304 (3d Cir. 2010).

414. *See supra* text accompanying notes 99–100. R

415. *See supra* text accompanying notes 257–60. R

416. *See CSI: Houston I*, 396 F. Supp. 2d 747, 757 (S.D. Tex. 2005) (concluding that a "prudent prosecutor" would seek a search warrant before requesting location data, because "it is impossible to know in advance whether the requested phone monitoring will invade the target's Fourth Amendment rights").

417. 18 U.S.C. § 2518 (2006).

because the statute did not apply.[418] Because of the analogy to silent video surveillance and wiretapping, the minimization, last resort, and other substantive requirements of Title III orders may be appropriate for location data orders, as well. Language in the magistrate judges' decision[419] and in a few location data cases involving real-time access suggests that courts are not entirely averse to that approach.[420] Given the difficulty establishing a warrant requirement, however, it seems unrealistic to imagine that courts will go further and impose the super-warrant requirement for location data acquisition.[421] But should a warrant requirement be imposed, as I believe it should, courts will need to recognize that associated procedural protections, such as notice and redress, will also be necessary.[422]

VI. CONCLUSION

Because government compulsion of disclosure of location data constitutes a search under the Fourth Amendment, the judicial oversight inherent in the probable cause warrant requirement is required. The power and intrusiveness of the method, and its susceptibility to

418. *See* Freiwald, *First Principles*, *supra* note 5, ¶¶ 53–56 ("Because the four factors identified made video surveillance, like wiretapping, particularly susceptible to abuse, the Courts of Appeals imposed those provisions of the Wiretap Act that they viewed as incorporating the Fourth Amendment particularity requirement."); Freiwald, *Online Surveillance*, *supra* note 3, at 79–80 (same). R R

419. *See CSI: Pittsburgh*, 534 F. Supp. 2d 585, 611 & n.63 (W.D. Pa. 2008) (citing to other courts that have suggested that location data searches should potentially be subject to the Wiretap Act requirements), *aff'd*, No. 07-524M, 2008 WL4191511 (W.D. Pa. Sept. 10, 2008), *vacated*, 620 F. 3d 304 (3d Cir. 2010).

420. *See In re* Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. and/or Cell Site Info., 396 F. Supp. 2d 294, 322–25 (E.D.N.Y. 2005) (refusing to address or rule out whether a "*more* exacting showing" under the Wiretap Act may be required for real-time access to location data).

421. Note that in the video surveillance cases, however, the federal courts of appeals imposed those requirements on government investigators who believed that they could use silent video surveillance cases without any statutory limits. *See, e.g.*, United States v. Koyomejian, 946 F.2d 1450, 1453 (9th Cir. 1991) (stating that the government argued that video surveillance is entirely "unregulated"), *vacated and remanded en banc*, 970 F.2d 536 (9th Cir.), *cert. denied*, 506 U.S. 1005 (1992).

422. *See, e.g.*, Warshak v. United States, 490 F.3d 455, 476 & n.8 (6th Cir. 2007) (noting the need for government searches of stored e-mails to comply with the particularity requirement of the Fourth Amendment), *vacated en banc*, 532 F.3d 521 (6th Cir. 2008); *CSI: Austin*, 727 F. Supp. 2d 571, 577–78 (W.D. Tex. 2010) (describing how notice and return of warrants are required in location data cases due to operation of Rule 41); *CSI: Austin*, 727 F. Supp. 2d at 582–83 (suggesting that the Fourth Amendment particularity requirement ought to apply and imposing a time limit on prospective orders); *June Hearings*, *supra* note 14, at 90–91 (statement of Stephen Wm. Smith, U.S. Mag. J.) (suggesting legislative reforms of location data orders, including notice to targets, public reporting, duration limits, exclusionary remedies, and civil remedies and penalties for violations). R

abuse, mean that anything less would violate Fourth Amendment rights. While the probable cause standard will not necessarily be that much more demanding than the showing needed for a D order,[423] the need to provide notice to the target, after the fact judicial review, and meaningful remedies should make a significant difference.[424] A warrant must be required for location data acquisition as a matter of law, and no Supreme Court precedents pertaining to bumper-beepers, bank records, or telephone numbers counsel a different result.

423. At oral argument in *CSI: Third Circuit*, Chief Judge Sloviter chided the government for resisting a warrant requirement, observing that in her thirty years on the bench, magistrate judges had not been "very grudging" in granting warrants. *See* Oral Argument, *supra* note 31, at 37:12–37:44. *But see supra* text accompanying notes 96–104 (discussing possible practical differences in D order standard versus the probable cause standard). R

424. *See CSI: Pittsburgh*, 534 F. Supp. 2d. at 585, 592 (noting that Rule 41 provides for notice within ten days from the end of the warrant period and suppression of information wrongfully obtained).