Texas Law Review
See Also
Volume 94

Response

A Rose By Any Other Name: Regulating Law Enforcement Bulk Metadata Collection

Stephen E. Henderson*

In Other People's Papers, Jane Bambauer argues for careful reform of the Fourth Amendment's third party doctrine, providing an important contribution to an increasingly rich field of scholarship, judicial opinion, statute, and law reform. Bambauer is especially concerned with access to bodies of third-party data that can be filtered and mined, as they can be privacy invasive but also effective and less subject to traditional investigative prejudices and limitations. Although her article provocatively overclaims in trying to set itself apart from existing proposals, by analyzing existing constitutional and statutory law—including what I have termed a "limited" third party doctrine—and comparing and contrasting her recommendations to those of the American Bar Association Criminal Justice Standards, this article continues the project of formulating how best to regulate law enforcement access to bulk metadata, focusing on cell-site location. The Standards provide an array of access options, the application of which requires struggling with the meaning of relevance and reasonable suspicion in the world of big data and data mining. As scholars have warned and as the National Security Agency's interpretation of USA PATRIOT Act Section

* Judge Haskell A. Holloman Professor of Law, the University of Oklahoma College of Law; B.S. in Electrical Engineering, University of California at Davis; J.D., Yale Law School. I enjoyed the opportunity to serve as the assigned Commenter for Professor Bambauer's draft at the 2014 Privacy Law Scholars Conference, where we had an engaging discussion of these issues, and I appreciate this opportunity to think on them more.

215 has demonstrated, the courts and criminal justice community have work remaining in better defining the meaning of these core terms. My favored analysis suggests legislatures should consider permitting cell-tower dumps for a single point in time upon crime commission, but that for any longer durations they should require a means of selective revelation.

I. An Increasingly Common Metadata Request: Cell-Tower Dumps

On February 10, 2015, an Assistant United States attorney in Houston, Texas, filed a sealed application under § 2703(d) of the Stored Communications Act (SCA).[1] That section provides for court orders requiring electronic communications service providers—in this case seven different mobile-phone companies—to turn over customer records if the prosecutor "offers specific and articulable facts showing that there are reasonable grounds to believe that the . . . [records] are relevant and material to an ongoing criminal investigation."[2] The prosecutor wanted historic data for each company's cell tower serving a specific location for the period of one hour, as well as the subscriber data pertaining to each caller (name, address, and means of payment).[3] Such a request can obtain records pertaining to many people. A cell tower often has a coverage radius of about a mile,[4] and mobile phones are in almost constant communication with the nearest tower anytime they are powered on.[5] However, most providers currently retain this information only when the phone is actively

---

1. *In re* Application for Cell Tower Records Under 18 U.S.C. § 2703(d), 90 F. Supp. 3d 673 (S.D. Tex. 2015) [hereinafter *In re* Application Houston]; *see also* USA v. 18:2703(D) SEALED APPLICATION (No. 4:15-MJ-00136).

2. 18 U.S.C. § 2703(d) (2012).

3. *In re* Application Houston, *supra* note 1, at 674; *see also* 18 U.S.C. § 2703(c)(2) (2012) (defining subscriber information). Cell-tower records

> may include the telephone call numbers and unique identifiers for any wireless device communicating via that tower; the source and destination telephone numbers for those communications; the date, time and duration of each communication; the tower sector handling the radio signal; and the type of communication (such as phone call or text message).

In re Application Houston, *supra* note 1, at 674.

4. United States v. Davis, 785 F.3d 498, 503 (11th Cir. 2015) (en banc).

> (1) [T]he cell tower used will typically be the cell tower closest to the user, (2) the cell tower has a circular coverage radius of varying sizes, and (3) although the tower sector number indicates a general direction (North, South, etc.) of the user from the tower, the user can be anywhere in that sector.

Id. at 501–02.

5. *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. 13–14 (2010) (testimony of Professor Matt Blaze) [hereinafter *ECPA Reform*]; Thomas A. O'Malley, *Using Historical Cell Site Analysis Evidence in Criminal Trials*, U.S. ATT'YS BULL. 16, 26 (2011). Phones register with the nearest tower about every seven seconds. State v. Earls, 70 A.3d 630, 637 (N.J. 2013).

communicating, such as through a phone call.[6] Thus, the attorney was asking to learn about every person speaking on—or otherwise communicating via—a cell phone in a particular Houston location during a certain hour on a particular day.[7]

Why? Because a crime had occurred during this hour, and a private security camera had recorded the perpetrator walking to the victim's location with a mobile phone to his ear.[8] Thus, if the prosecutor could learn *everyone* speaking on a mobile phone in that part of Houston, it would include the perpetrator (assuming that the perpetrator wasn't merely enjoying some music but lacking headphones). Even so, meaning even if the requested data did include the phone number being used by the perpetrator among the many other numbers revealed, it might prove to be a dead end. It might be a list thereafter deemed too long to merit further investigation, or which therefore receives only incomplete investigation. Or, the perpetrator might have been smart enough to use a prepaid burner phone purchased without identification and without providing other leads to identity. For example, in another recent prosecution the defendant's phone was registered to "Lil Wayne," the stage name of a rapper, requiring a coconspirator to identify the phone as belonging to the defendant.[9] But many criminals are careless at best,[10] and one can certainly understand law enforcement's desire to obtain this information.

In that, however, is also the danger of providing this information. When law enforcement is provided information pertaining to multiple persons, most of whom are entirely innocent of the crime under investigation, persons come under government scrutiny and suspicion who would never otherwise.[11] In

---

6. *See In re* Application of the United States for Historical Cell Site Data, 724 F.3d 600, 602 n.1 (5th Cir. 2013) [hereinafter *In re* Application Fifth Circuit]; *ECPA Reform*, *supra* note 5, at 16, 27, 95.

7. *In re* Application Houston, *supra* note 1, at 674. The magistrate judge commented that the requested data might "retrieve several thousand phone numbers in a metropolitan area like Houston." *Id.* at 676.

8. *In re* Application Houston, *supra* note 1, at 674.

9. *See Davis*, 785 F.3d at 503. Coconspirators purchased their phones using similarly creative names. *Id.* at 503 n.6.

10. For the story of one criminal who purchased a burner phone using his real name and birth date, see Stephen E. Henderson, *Real-Time and Historic Location Surveillance After* United States v. Jones*: An Administrable, Mildly Mosaic Approach*, 103 J. CRIM. L. & CRIMINOLOGY 803, 806 (2013).

11. In the context of discussing its de-identification regime, the ABA Criminal Justice Standards explain as follows:

> On the one hand, this is perhaps a lesser intrusion. As in the nonrecord context of an automobile roadblock, each person can take solace in knowing that he or she is not individually under suspicion. On the other hand, it is a greater intrusion, in that persons whose records would never otherwise come to the attention of law enforcement are now perused.

AM. BAR ASS'N, ABA STANDARDS FOR CRIMINAL JUSTICE: LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS, Standard 25-5.6 cmt. (3d. ed 2013), http://www.americanbar.org/content/

another investigation, "[f]ederal agents combed through the records of 150,000 phones used to make calls."[12] Since two perpetrators were included within that number, 149,998 phones belonged to persons innocent of the crime under investigation.[13] In other words, 99.999% of the records pertained to innocent persons. Five nines are very good if one is talking the uptime reliability of a cell-phone provider,[14] but very bad if talking about criminal investigation. The guilty are a needle in the proverbial haystack.

Especially for those who satisfy characteristics of a "usual suspect," whether that be by a criminal record or a character trait more invidiously considered (e.g., young, black male), permitting too easy access to cell-tower dumps—meaning the log of all cell phones using a particular tower—could result in harassment and chilling effects. If every time there is a crime in Central Park the police show up on my doorstep—or, even worse, physically and verbally assault me[15]—I may rationally decide it is better to avoid the park altogether, or at least not to carry a phone, despite my having done nothing wrong. And investigating officers subject to confirmation bias may wrongly be convinced that where there is smoke there must be fire.[16]

How does and should the law respect and balance these competing considerations?

II. Existing Federal Law and Other Proposals

The Houston cell-tower request potentially implicates both the federal Fourth Amendment and the Stored Communications Act. After a brief consideration of that law, I consider Jane Bambauer's new proposal and then

---

dam/aba/publications/criminal_justice_standards/third_party_access.authcheckdam.pdf [http://perma.cc/3BWG-VLS7] [hereinafter LEATPR]. Andrew Ferguson has expressed concern with such bulk identifications. *See* Andrew Guthrie Ferguson, *Big Data Distortions: Exploring the Limits of the ABA LEATPR Standards*, 66 OKLA. L. REV. 831, 848 (2014) ("People who have no association with the crime will be tracked to a particular place at a particular time without any individualized suspicion of criminal wrongdoing.").

12. Eric Betz, *Bank 'Bandit' Pleads Guilty*, ARIZ. DAILY SUN (Nov. 8, 2011, 9:00 AM), http://azdailysun.com/news/local/crime-and-courts/bank-bandit-pleads-guilty/article_90aee950-0b4c-59da-ac56-7a5869d1cab4.html [http://perma.cc/ZFG2-5GBT].

13. *See id.*

14. Jim Waldo, *Virtual Organizations, Pervasive Computing, and an Infrastructure for Networking at the Edge*, 4 INFO. SYS. FRONTIERS 9, 13 (2002).

15. *See* Ross Tuttle & Erin Schneider, *Stopped-and-Frisked: 'For Being a F**king Mutt'*, NATION (Oct. 8, 2012), http://www.thenation.com/article/170413/stopped-and-frisked-being-fking-mutt-video [http://perma.cc/SD7L-SSG4].

16. *See generally* Barbara O'Brien, *Prime Suspect: An Examination of Factors that Aggravate and Counteract Confirmation Bias in Criminal Investigations*, 15 PSYCHOL. PUB. POL'Y & L. 315 (2009) (reporting on a case study of a mock police investigation); Kendra Cherry, *What Is a Confirmation Bias?*, ABOUT EDUCATION, http://psychology.about.com/od/cognitivepsychology/fl/What-Is-a-Confirmation-Bias.htm, [http://perma.cc/45E8-JGRL]. Of course, confirmation bias can also be a problem if police *don't* use means to learn of other possible suspects. But it explains why they might harass usual suspects, however located.

compare and contrast the framework of the American Bar Association Standards for Criminal Justice on Law Enforcement Access to Third Party Records (LEATPR Standards), for which I served as Reporter.

A. The Fourth Amendment and Its Limited Third Party Doctrine

The Fourth Amendment protects the right of the people—all of us[17]—to be secure in our "persons, houses, papers, and effects, against unreasonable searches and seizures."[18] For the reasons articulated above, I believe that cell-tower dumps affect the security in my person and in what I consider to be my papers, albeit residing with a third-party provider. Further, I believe that the requested government access constitutes a "search," as "an attempt to find someone or something."[19] But, as most readers will know, in a series of cases in the 1970s and 1980s the Supreme Court decided otherwise, creating its third party doctrine.[20] In the words of the 1976 decision in *United States v. Miller*:[21]

> This Court has held repeatedly that the Fourth Amendment does not [restrict] the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[22]

One's location in the sense of being nearest to a particular cell tower is revealed to the mobile-phone provider and thus falls within this seemingly monolithic doctrine. The doctrine cannot be as encompassing as expressed in *Miller*, however, lest it conflict with other decisions by the Court protecting the contents of communications,[23] or at least with what is

---

17. At least all those who are United States citizens and others "who have otherwise developed sufficient connection with this country to be considered part of [the national] community." United States v. Verdugo-Urquidez, 494 U.S. 259, 265 (1990) (considering who is included within "the people"). For an argument that Fourth Amendment rights are by this term collective in nature, see generally David Gray, *Dangerous Dicta*, 72 WASH. & LEE L. REV. 1181 (2015).

18. U.S. CONST. amend. IV.

19. *Search*, MERRIAM-WEBSTER, http://www.merriam-webster.com/dictionary/search [http://perma.cc/EXJ7-3GLD].

20. *See* 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, 376–79 (2006) [hereinafter Henderson, *All Fifty States*] (explaining the development of the third-party doctrine); Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 MERCER L. REV. 507, 518–21 (2005) [hereinafter Henderson, *Nothing New*] (same).

21. 425 U.S. 435 (1976).

22. *Id.* at 443.

23. *See* Katz v. United States, 389 U.S. 347, 353 (1967) (declaring Fourth Amendment protection for the contents of telephone communications); Berger v. New York, 388 U.S. 41, 54–55 (1967) (same).

commonly assumed to follow from those decisions.[24] Thus, I have described the existing law as a *limited* third party doctrine that eliminates Fourth Amendment protection from information provided for a third party's *use*, thereby differentiating the protected content of a mobile-phone call from its unprotected metadata.[25] One's location at the time of a mobile call is necessarily shared with the provider in order for it to complete the desired service and therefore would be unprotected.

My limited third party doctrine is no descriptive failsafe, however, as I have demonstrated that the Supreme Court has balked at applying even this more nuanced test.[26] That longstanding reticence—which I believe to be wise—coupled with language in the GPS-tracking case of *United States v. Jones*[27] and the cell phone search case of *Riley v. California*,[28] make it likely that the Supreme Court might ultimately accept an opportunity to consider the Fourth Amendment protection of cell-site location data. What was previously fair game as a search incident to arrest under the 1973 precedent of *United States v. Robinson*[29] changed when technology altered the privacy interests in *Riley*. Similarly, what was fair game as "not a search" under the 1976 precedent of *United States v. Miller*[30] and the 1979 precedent of *Smith v. Maryland*[31] should change with technology. Thus, a panel of the Eleventh Circuit held that there is Fourth Amendment protection for cell-site data,[32]

---

24. *See* United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (interpreting these precedents to provide Fourth Amendment warrant protection when the government obtains subscriber emails from a third-party provider).

25. *See* Henderson, *Nothing New*, *supra* note 20, at 524–29 (developing and naming the limited third party doctrine); Stephen E. Henderson, *After* United States v. Jones*, After the Fourth Amendment Third Party Doctrine*, 14 N.C. J.L. & TECH. 431, 437–38 (2013) [hereinafter Henderson, *After the Third Party Doctrine*] (building upon the same).

26. *See* Henderson, *After the Third Party Doctrine*, *supra* note 25, at 438–42 (analyzing a handful of instances in which the Court fails to fairly apply its third party doctrine); Stephen E. Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 IOWA L. REV. BULL. 39, 42–43 (2011) (more quickly summarizing the same). In the words of the Second Circuit, "the Supreme Court's jurisprudence is in some turmoil." ACLU v. Clapper, 785 F.3d 787, 821 (2d Cir. 2015); *see also* Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV. 611 (2015) (arguing for further erosion of the third party doctrine).

27. 132 S. Ct. 945, 948–49 (2012) (holding that physically placing a tracking device on a vehicle to track the vehicle's movements over a twenty-eight-day period constitutes a Fourth Amendment search).

28. 134 S. Ct. 2473, 2489–95 (2014) (holding that there exists a greater expectation of privacy in mobile phones and thus that they do not fall within the traditional container doctrine for search incident to lawful arrest). *Riley* is not directly on point as it is not a third-party search, but the Court's language was unusually strong, including in expressing concern for third-party data that might be accessed by means of a phone search. *See id.* at 2491.

29. 414 U.S. 218 (1973).

30. 425 U.S. 435, 442–43 (1976).

31. 442 U.S. 735 (1979).

32. United States v. Davis, 754 F.3d 1205, 1217 (11th Cir.), *reh'g en banc granted, opinion vacated*, 573 F. App'x 925 (11th Cir. 2014), *aff'd in part*, 785 F.3d 498 (11th Cir. 2015).

and although that decision was vacated by that full court, some state high courts have held such records are protected as a matter of their respective state constitutions.[33] Most recently, a divided panel of the Fourth Circuit held there is Fourth Amendment protection, briefly creating a circuit split until the court granted rehearing en banc.[34]

Judge Rosenbaum of the Eleventh Circuit put it this way:

> In our time, unless a person is willing to live "off the grid," it is nearly impossible to avoid disclosing the most personal of information to third-party service providers on a constant basis, just to navigate daily life. And the thought that the government should be able to access such information without the basic protection that a warrant offers is nothing less than chilling. Today's world, with its total integration of third-party-provided technological services into everyday life, presents a steroidal version of the problems that Justices Marshall and Brennan envisioned when they dissented in *United States v. Miller* and its progeny.[35]

---

33. *E.g.* Commonwealth v. Estabrook, 38 N.E.3d 231, 234 (Mass. 2015) (requiring a warrant to obtain anything over six hours of historic cell site location information); Commonwealth v. Augustine, 4 N.E.3d 846, 865–66 (Mass. 2014) (same for two weeks of information); State v. Earls, 70 A.3d 630, 644 (N.J. 2013) (requiring a warrant to access cell-site location information); *see also* Tracey v. State, 152 So.3d 504, 525–26 (Fla. 2014) (requiring a warrant for real-time acquisition of cell-site location information); State v. Subdiaz-Osorio, 849 N.W.2d 748, 768 (Wis. 2014) (discussing, but not deciding, the issue). As I have explained elsewhere, I do not believe there should typically be any distinction between real-time and historic access to the same information. Henderson, *supra* note 10, at 831–32; *see also* United States v. Graham, 796 F.3d 332, 349 n.7 (4th Cir. 2015) (agreeing), *rehearing en banc granted* (4th Cir. Oct. 28, 2015). There is, however, sometimes a current statutory difference. *See, e.g.*, *In re* Application Houston, *supra* note 1, at 677–78 (contrasting the federal statutory authority for obtaining cell-site location in real time from that for historic access). Finally, some states have legislated protection for cell-site location. *E.g.,* MONT. CODE ANN. § 46-5-110 (2014) (typically requiring a warrant); 725 ILL. COMP. STAT. ANN. 168 / 10 (2014) (same for real-time acquisition); IND. CODE ANN. § 35-33-5-12 (2015) (same for real-time acquisition); *see also* Allie Bohm, *Status of Location Privacy Legislation in the States*, ACLU (Apr. 8, 2014, 12:00 AM), https://www.aclu.org/blog/status-location-privacy-legislation-states [https://perma.cc/TT7J-KJT9].

34. *See Graham*, 796 F.3d at 344–45 ("We hold that the government conducts a search under the Fourth Amendment when it obtains and inspects a cell phone user's historical CSLI for an extended period of time."); *cf. In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'ns Serv. to Disclose Records to Gov't, 620 F.3d 304, 315–19 (3d Cir. 2010) (concluding the Stored Communication Act provides magistrates an option and thus avoiding the constitutional question); *In re* Application of the United States for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013) (holding there is no Fourth Amendment protection and thus permitting cell-site location requests under the Stored Communications Act); *Davis*, 785 F.3d at 500 (same); *see also In re* Application for Tel. Info. Needed for a Criminal Investigation, No. 15-XR-90304-HRL-1(LHK), 2015 WL 4594558, at *7–20 (N.D. Cal. July 29, 2015) (holding there is Fourth Amendment protection and gathering supporting precedents and statutes).

35. *Davis*, 785 F.3d at 525 (Rosenbaum, J., concurring) (citation omitted). Rosenbaum's solution, a sort of "equilibrium adjustment," is more backward looking than my preference for focusing on the privacy implications and government need. *See id.* at 525–32. *See generally* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011).

The Onion's satirical take on a remote, enclosed Google "Opt Out Village" humorously demonstrates what it might require for anyone today to truly go off the grid.[36] In the mountain village, Google "can guarantee that there's no chance of Google reading your emails, because there are no computers. And, because they're also monitored and tracked by Google, there are no banks or hospitals."[37] Hence, "residents will be expected to know how to grow food, suture wounds, and bury corpses by hand."[38] While obviously and intentionally over-the-top, the serious question is whether the third party doctrine should change given that today people create data exhaust in almost everything they do.[39]

This potential reconfiguring of the third party doctrine is what sparks Bambauer's interest.[40] Yet for now the constitutional issue was straightforward for the Houston, Texas, magistrate to which the federal prosecutor applied—Magistrate Judge Stephen Wm. Smith[41]—because the Fifth Circuit has held there is no federal constitutional restriction on law enforcement accessing historic cell-site location records.[42] Even considering existing fractures in the third party doctrine, the Fifth Circuit holding was not terribly surprising as it largely tracks my limited test.[43] Thus, it has been

---

36. *See Google Opt Out Feature Lets Users Protect Privacy By Moving To Remote Village*, ONION (Aug. 11, 2009), http://www.theonion.com/video/google-opt-out-feature-lets-users-protect-privacy--14358 [http://perma.cc/SQS7-LRNK].

37. *Id.*

38. *Id.*

39. *See* Stephen E. Henderson, *Our Records Panopticon and the American Bar Association Standards for Criminal Justice*, 66 OKLA. L. REV. 699, 700–06 (2014) (examining the incredible amounts of data that people produce and share).

40. *See* Jane Bambauer, *Other People's Papers*, 94 TEXAS L. REV. 205, 211 ("[N]one of the innovations in criminal law enforcement endorsed in this Article can justify unfettered access to all third-party records for any or no reason, which the current third-party doctrine allows. Rather than defending the third-party doctrine whole cloth, this Article will show how the doctrine should be revised to protect the subjects of criminal investigations without causing unnecessary conflicts with due process, equal protection, and First Amendment values.").

41. Magistrate Judge Smith has played a vital role in working out the rules for government access to digital data and in calling for greater transparency in the same. *See generally* Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, 6 HARV. L. & POL'Y REV. 313 (2012). The issuance of his cell-tower opinion continues in this vein.

42. *In re* Application Fifth Circuit, *supra* note 6, at 608–15. Judge Smith did not seem overly impressed with the Fifth Circuit's decision. *See In re* Application Houston, *supra* note 1, at 675–76 (pointing out a different federal statute that declares call-location records as belonging to the customer and arguing that the specific trumps the general).

43. The critical distinction for the Fifth Circuit was that the government was requesting records the business had already created for its own purposes (no search), as opposed to the government itself gathering the information (e.g., using a cell-site simulator) or requesting a third party to gather the information (e.g., asking a hotel employee or landlord to enter a guest or tenant room) (both potentially a search). *In re* Application Fifth Circuit, *supra* note 6, at 610–11. This will largely track my limited third party doctrine: "[T]hese are the providers' own records of transactions to which it is a party. . . . The provider uses this data to properly route his call." *Id.* at 612. The difference will be when information is provided for the third party's use but the party would not

followed by an en banc Eleventh Circuit opinion, an opinion which is most notable for its exhaustively tiered approach that slowly climbs to—and ultimately achieves in a final footnote—court unanimity.[44]

Perhaps, in considering the Houston request, Judge Smith could nonetheless have taken up whether the matter is different for a tower dump that accesses the records of so many different persons, a matter the Fifth Circuit expressly declined to address.[45] But there is certainly a logic in holding that obtaining unprotected information about one guy, and also unprotected information about a different gal, still remains unprotected. Zero plus zero equals zero, no matter how many addends there may be.[46]

B. The Stored Communications Act

When it comes to regulating law enforcement access to information, my preference is for "legislative differential regulation, by which I mean a hierarchy of regulation proportional to privacy, yet responsive to law enforcement needs, subject to a constitutional backstop."[47] Fortunately, we have a federal statute for cell-site location information. Unfortunately, it is quite dated.

---

typically record it. I believe my test is a more accurate description of *Smith v. Maryland*, 442 U.S. 735, 737 (1979), the seminal case in which the phone company installed a pen register *at police request*.

44. United States v. Davis, 785 F.3d 498, 518 n.21 (11th Cir. 2015) (en banc). Seven judges agreed that "[t]he longstanding third-party doctrine plainly controls the disposition of this case"; there was no Fourth Amendment search. *Id.* at 512. In order to gain two more votes, the court went on to hold the Stored Communications Act provisions reasonable *even if* the government acquisition constitutes a search. *Id.* at 518 n.21; *id.* at 521 (Jordan, J., concurring). And to gild the lily and get all eleven on board, the court held, in a single-sentence footnote, that even if the government acquisition constituted an *unreasonable* search, the officers acted in reasonable reliance upon an apparently valid statute and therefore the evidence should not be suppressed. *Id.* at 518 n.20; *id.* at 533 n.1 (Martin, J., dissenting).

45. *In re* Application Fifth Circuit, *supra* note 6, at 615.

> Recognizing that technology is changing rapidly, we decide only the narrow issue before us. Section 2703(d) orders to obtain historical cell site information for specified cell phones at the points at which the user places and terminates a call are not categorically unconstitutional. We do not address orders requesting data *from all phones that use a tower during a particular interval*, orders requesting cell site information for the recipient of a call from the cell phone specified in the order, or orders requesting location information for the duration of the calls or when the phone is idle (assuming the data are available for these periods). Nor do we address situations where the Government surreptitiously installs spyware on a target's phone or otherwise hijacks the phone's GPS, with or without the service provider's help.

Id. (emphasis added) (original emphasis omitted).

46. Judge Smith left this implicit, only commenting on the different type of customer records at issue in the two cases. *See In re* Application Houston, *supra* note 1, at 675–76.

47. Henderson, *supra* note 10, at 808.

The Stored Communications Act came into being via Title II of the 1986 Electronic Communications Privacy Act.[48] Despite some amendments, the law often requires trying to squeeze contemporary technology—playing the part of the proverbial square peg—into a round hole.[49] This is not surprising when one considers that the aim of the 1986 law was "to update and clarify Federal privacy protections . . . in light of dramatic changes in new computer and telecommunications technologies."[50] That dramatic change has only hastened since 1986, the Bulletin Board Systems of the 1980s being at best crude precursors to the World Wide Web and cloud computing, and only the seed of today's pervasive access via the mobile phone.[51] But it is the existing law, and for government access it relies upon a content/noncontent distinction (and, within content, a now-anachronistic 180-day limitation).[52]

A prosecutor wanting to obtain "contents"—defined to include "any information concerning the substance, purport, or meaning of [a] communication"[53]—must sometimes proceed by obtaining a search warrant.[54] But a prosecutor wanting to obtain noncontent information can instead choose the § 2703(d) "specific and articulable facts" court order.[55] There are circumstances in which it is not at all clear whether location information is content.[56] But for cell-site location accompanying a mobile-

48. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1860 (1986) (codified as amended at 18 U.S.C. §§ 2701–11 (2012)).

49. *See* Susan Freiwald, *Light in the Darkness: How the LEATPR Standards Guide Legislators in Regulating Law Enforcement Access to Cell Site Location Records*, 66 OKLA. L. REV. 875, 877 (2014).

50. S. REP. NO. 99-541, at 1 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555. The immediate referent for these remarks is change to the wiretap provisions, adding protection for electronic communications. *Id.* at 2. However, the full context and further comments make clear the same goal for the new Stored Communications Act. *See id.* at 3.

51. *See* Stephen E. Henderson, *Expectations of Privacy in Social Media*, 31 MISS. COLL. L. REV. 227, 227–29 (2012) (describing some of this evolution in online technology); *id.* at 244 (briefly explaining the statutory architecture).

52. For a thorough explanation of the statute and how it should be modified, see generally Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004); Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373 (2014); .

53. 18 U.S.C. §§ 2510(8), 2711(1) (2012).

54. *Id.* § 2703(a).

55. *Id.* § 2703(d); *see* Freiwald, *supra* note 49, at 880–81. The Third Circuit has held, not very persuasively, that the Stored Communications Act permits a magistrate to choose to require a probable cause warrant rather than provide a § 2703(d) order. *See* Application of the U.S. for an Order Directing a Provider of Elec. Commc'ns Serv. to Disclose Records to Gov't, 620 F.3d 304, 315–19 (3d Cir. 2010); *cf. In re* Application Fifth Circuit, *supra* note 6, at 606–08 (disagreeing). *But see id.* at 615–22, 630–32 (Dennis, J., dissenting) (more persuasively building off the Third Circuit's opinion to argue for application of the canon of constitutional avoidance).

56. *See* Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975, 1019–24 (2007) (arguing that a content/noncontent distinction relies upon the particular architecture of traditional

phone call, location does not concern the substance of the communication and therefore is squarely on the "noncontent" side of the fence.[57] Hence, in the Houston investigation, as noted above, the federal prosecutor sought a § 2703(d) order.[58]

In order to obtain such an order, the prosecutor must offer "specific and articulable facts showing that there are reasonable grounds to believe that the . . . [records] are relevant and material to an ongoing criminal investigation."[59] This language derives from the Supreme Court's opinion in *Terry v. Ohio*[60] and its progeny governing temporary investigative seizures of the person.[61] Thus, despite that different context, courts and commentators have assumed the standard for a § 2703(d) order is the familiar reasonable suspicion.[62]

Despite an otherwise thoughtful opinion, Magistrate Judge Smith seemed to think it a given that reasonable suspicion was satisfied, or at least he did not articulate any analysis in this regard. Thus, he issued the order, though narrowing the time period from the requested hour to just ten minutes.[63] But reasonable suspicion is actually not clear, and indeed I think the standard *not* satisfied as the term is ordinarily understood.

Remarkably, there exists a rather poor understanding of the critical measures of Fourth Amendment suspicion.[64] Some think probable cause

---

telephony); Steven Bellovin et al., *It's Too Complicated: The Technological Implications of IP-Based Communications on Content/Non-Content Distinctions and the Third Party Doctrine* (draft on file with author); *see also* United States v. Davis, 785 F.3d 498, 537 (11th Cir. 2015) (Martin, J., dissenting) (arguing against a content/noncontent distinction).

57. *See Davis*, 785 F.3d at 502 (using § 2703(d) for cell site location); *In re* Application Fifth Circuit, *supra* note 6, at 615 (same).

58. *In re* Application Houston, *supra* note 1, at 674.

59. 18 U.S.C. § 2703(d) (2012).

60. 392 U.S. 1 (1968).

61. *See id.* at 21 ("And in justifying the particular intrusion the police officer must be able to point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion.").

62. *See* Heien v. North Carolina, 135 S. Ct. 530, 536 (2014) ("[O]fficers need only 'reasonable suspicion'—that is, 'a particularized and objective basis for suspecting the particular person stopped' of breaking the law.") (citation omitted); *In re* United States for an Order Pursuant to 18 U.S.C. Section 2703(d), 707 F.3d 283, 287 (4th Cir. 2013) ("[Section 2703(d)] is essentially a reasonable suspicion standard."); United States v. Graham, 796 F.3d 332, 344 (4th Cir. 2015) (quoting the earlier panel opinion and reiterating the same), *rehearing en banc granted* (4th Cir. Oct. 28, 2015). Stephanie Pell and Christopher Soghoian have also argued for a reasonable suspicion standard for location data. *See* Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data that Congress Could Enact*, 27 BERKELEY TECH. L.J. 117, 180 (2012).

63. *In re* Application Houston, *supra* note 1, at 677. The relevant private video surveillance had a duration of six minutes. *Id.* at 674.

64. *See generally* Andrew E. Taslitz, *Cybersurveillance Without Restraint? The Meaning and Social Value of the Probable Cause and Reasonable Suspicion Standards in Governmental Access to Third-Party Electronic Records*, 103 J. CRIM. L. & CRIMINOLOGY 839 (2013) (trying to make sense of the uncertainty).

requires a preponderance of the evidence,[65] whereas I think it a slightly less, albeit inarticulable, measure. For its part, the Supreme Court has declared the standard "incapable of precise definition or quantification into percentages,"[66] but has also declared that "[f]inely tuned standards such as proof beyond a reasonable doubt or by a preponderance of the evidence . . . have no place in the probable-cause decision."[67] Thus, probable cause "does not demand any showing that . . . a belief be correct or more likely true than false."[68] What it does require is a "fair probability" or "substantial chance."[69] Reasonable suspicion, requiring a "moderate chance,"[70] is "obviously less demanding"[71] than probable cause, and "considerably less [demanding]"[72] than a preponderance. But what *is* it?

I can readily understand the Court's refusal to articulate percentage, because historically investigatory methods have rarely been capable of being expressed in precise probabilistic terms (though this might cause confusion when more modern methods *can* be so quantified).[73] But I see the standards as differing in confidence level, such that if probable cause is something akin to being 40% confident that evidence of crime will be found in a particular location, reasonable suspicion is something akin to being 30% confident.[74]

Using anything like this model, how could there be reasonable suspicion in the case of the desired Houston cell-tower dump? Only, it would seem, if very few people were talking on their cell phones. Think of it this way: if police were physically present after the commission of the crime, could they temporarily detain—and thereby constitutionally seize—everyone standing within the relevant cell-site sector? If there are many people present, of course not. In other words, reasonable suspicion requires a respectable hit to no-hit ratio. It can be constitutionally permissible to temporarily detain—though not, I think, to arrest—two persons when only one can have

65. *See id.* at 883.

66. Maryland v. Pringle, 540 U.S. 366, 371 (2003).

67. Florida v. Harris, 133 S. Ct. 1050, 1055 (2013) (quoting Illinois v. Gates, 462 U.S. 213, 235 (1983)).

68. Texas v. Brown, 460 U.S. 730, 742 (1983).

69. Safford Unified Sch. Dist. #1 v. Redding, 557 U.S. 364, 371 (2009) (citations omitted).

70. *Id.*

71. United States v. Sokolow, 490 U.S. 1, 7 (1989).

72. *Id.*

73. *See generally* Erica Goldberg, *Getting Beyond Intuition in the Probable Cause Inquiry*, 17 LEWIS & CLARK L. REV. 789 (2013).

74. *Cf. id.* at 834 ("[A] significant number of courts and scholars assume that probable cause is within the 40% to 51% range.").

committed the crime. But, as that number of potential suspects increases, at some point—and rather quickly, I think—reasonable suspicion dissipates.[75]

What would reasonable suspicion look like in this context? Again, it helps to think of the more familiar Terry stop. Just as police can constitutionally detain a person near the scene of a recent crime if his appearance is sufficiently consistent with an eyewitness description, they could obtain cell-phone records if, say, the perpetrator had been seen talking on a particular model phone and the phone company was able to narrow its records accordingly.

Thus, despite Judge Smith granting the requested order, I do not think reasonable suspicion was satisfied, and therefore I do not think law enforcement should have obtained the Houston tower dump according to the requirements of the Stored Communications Act. This means an obviously useful tool is much less often available to police investigating crime, a result that Bambauer finds unacceptable. Therefore, I next turn to her arguments, but first quickly explain one last reasonable suspicion wrinkle.

1. Christopher Slobogin's Different Formulation.—Like Andrew Taslitz, Christopher Slobogin believes that probable cause requires a preponderance.[76] But Slobogin goes one further, also requiring a preponderance for reasonable suspicion but a differently characterized one: whereas probable cause requires it be more likely than not that evidence of crime will be located within the information immediately obtained, reasonable suspicion requires it be more likely than not that the information *will lead to* evidence of crime.[77] At first blush, this alternative conception of reasonable suspicion would seem to be satisfied in the case of the Houston cell-tower dump. If the officer can determine everyone who was speaking on a mobile phone, that will include the perpetrator, and so methodically working that list, no matter how long, will ultimately lead to the desired evidence of crime.

Indeed, the text of § 2703(d) can be read in this manner. It requires "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."[78] Given the private surveillance video showing the perpetrator speaking on a mobile phone

---

75. Jane Bambauer agrees there will not typically be reasonable suspicion in the context of a cell-tower dump. Bambauer, *supra* note 40, at 235; *see also id.* at 236 (suggesting a necessary hit rate of one in three or one in four to satisfy reasonable suspicion).

76. Christopher Slobogin, *Making the Most of* United States v. Jones *in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST. L. & PUB. POL'Y (SPECIAL ISSUE) 1, 20–21 (2012).

77. *Id.* at 22–23. Andrew Ferguson has argued for this same distinction between different "levels" of probable cause. *See* Ferguson, *supra* note 11, at 865.

78. 18 U.S.C. § 2703(d) (2012).

(specific and articulable facts), the prosecutor has reasonable grounds to believe that the cell-tower records are relevant and material.

But this sort of reading, meaning one that ignores the hit to no-hit ratio required above, poses a major problem. It would mean that a larger database is always to be preferred, because by definition there will be evidence of crime in that larger set. In other words, a police officer might posit the following: "If I can stop everyone within five feet of the robbery victim because the crime just occurred, I can also stop everyone within fifty feet—or indeed within five thousand feet. I'm even more confident the perpetrator is still within that group!" This would mean that a prosecutor confident that *a* bank customer is committing tax fraud could access the combined records of *all* customers of that bank because, somewhere in there, she is very sure is evidence of crime. Indeed, just to be safe she should probably access all the world's bank-customer records, because the bad guy is *definitely* within that set.

Slobogin of course does not advocate such an absurd reading. Instead, I believe he would require that with respect to each person's obtained records, meaning here each phone number contained within the dump, it be more likely than not that the number will lead to evidence of crime. If many persons were talking on their cell phones within this tower sector, this alternative criterion—like that of traditional reasonable suspicion—would not be satisfied.

C. Jane Bambauer's Other People's Papers

In *Other People's Papers*, Jane Bambauer agrees with my (and many others') claim that the third party doctrine should be reformed,[79] and on many other things besides. Bambauer agrees that ideally computer-automated searches could separate the wheat from the chaff, locating the incriminating information without exposing the innocent[80] (although of course this has proved very difficult in practice such as in the forensic examination of a computer hard drive).[81] She agrees that law enforcement access to third-party information invades the information privacy interest in

---

79. *See* Bambauer, *supra* note 40, at 209; *supra* subpart II(A). I was pleased to serve as the assigned Commenter for Bambauer's draft article at the 2014 Privacy Law Scholars Conference.

80. *See id*. at 217.

81. *See* Stephen E. Henderson, *What Alex Kozinski and the Investigation of Earl Bradley Teach About Searching and Seizing Computers and the Dangers of Inevitable Discovery*, 19 WIDENER L. REV. 115, 129–36 (2013) (describing courts' struggles over how the Fourth Amendment regulates searches of computer hard drives). *See generally* Paul Ohm, *Response: Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 VA. L. REV. IN BRIEF 1 (2011) (arguing that magistrates can and should regulate such searches); Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 VA. L. REV. 1241 (2010) (arguing to the contrary).

controlling what information is given to others and for what purposes[82] and recognizes further harms in that information's misuse.[83] She agrees that many concerns diminish—or even disappear—if laws are evenly enforced including throughout the "elite and politically powerful."[84] She agrees that broad subpoena authority is necessary for investigations of white collar crime.[85]

This is not to say there are not points of disagreement. Bambauer follows Christopher Slobogin in broadly desiring different rules for "target-driven" and "event-driven" investigations,[86] which she relabels as "suspect-in" and "crime-out."[87] As will be described below, the ABA Criminal Justice Standards do sometimes permit the type of data access Bambauer would like to see in event-driven investigations.[88] But as a more general matter, at the urging of law enforcement and prosecutors who considered it unworkable in practice, the ABA Task Force decided against a target-driven and event-driven distinction.[89] Investigations waffle between having an individual suspect, a limited group of suspects, and more disparate suspicions, and it was difficult for law enforcement to comprehend why they could more easily obtain *everyone's* record 'x' than merely 'x' for six identified persons, or even for only one.

For example, homicide is often not a stranger crime,[90] and thus for most any homicide police may immediately intuit a suspect (e.g., an estranged spouse), a handful of suspects (e.g., family more generally), or a class of suspects (e.g., rival gang members). Is police access to information in each

---

82. *See* Bambauer, *supra* note 40, at 217–18 (recognizing limited harms involved in collection); Henderson, *supra* note 51, at 229–33.

83. *See* Bambauer, *supra* note 40, at 222–23; LEATPR, *supra* note 11, 123–30 ("Part VI: Retention, Maintenance, and Disclosure of Records.").

84. *See* Bambauer, *supra* note 40, at 226, 242; Henderson, *Nothing New*, *supra* note 20, at 554–59. *See generally* Christopher Slobogin, *Panvasive Surveillance, Political Process Theory, and the Nondelegation Doctrine*, 102 GEO. L.J. 1721 (2014) (developing richly a related argument).

85. *See* LEATPR, *supra* note 11, Standard 25-2.1(c) (expansive grand jury carve-out); Bambauer, *supra* note 40, at 249–50; Andrew E. Taslitz & Stephen E. Henderson, *Reforming the Grand Jury to Protect Privacy in Third Party Records*, 64 AM. U. L. REV. 195, 211 (2014) (arguing against the total LEATPR carve-out but recognizing that standards might differ for some white-collar investigations).

86. *See* CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 191–96 (2007) (developing this framework); Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 336–41 (2008) (same).

87. Bambauer, *supra* note 40, at 233–34.

88. *See infra* subpart II(E).

89. I served as the Reporter for the drafting of this set of Standards, and thus the assertions regarding Task Force meetings are based upon my personal recollections as memorialized in internal Task Force communications and memoranda.

90. SPECIAL REPORT: VIOLENT VICTIMIZATION COMMITTED BY STRANGERS, 1993–2010, BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE 1 (2012), http://www.bjs.gov/content/pub/pdf/vvcs9310.pdf [http://perma.cc/Z7PK-JQCL].

instance target-driven or event-driven? One could argue that the search remains event-driven so long as police do not have *a* singular suspect, but then the rule would be perverse. Not only will police often have multiple suspects at various stages of an investigation, but it would mean that so long as there remain two suspects, all searches would be event-driven merely because the privacy of two persons rather than of one were being infringed.

But if this means such searches are instead target-driven, as Slobogin would argue, then police suspecting only two (or six) persons would make it *more* difficult to access given information than if police were clueless and therefore "suspected" everyone within the town. Can it be that police can more readily obtain records if they pretend not to have—or actually do not have—any suspicions? It seems odd to in effect penalize police for narrowing the field of suspects, and moreover it is unclear whether a hunch or something much more (and then precisely what?) suffices to tip the balance and thus change the rules. In short, something about such a two-tiered system seemed wrong—or at least not fully formulated—and so as a Task Force decision it was not generally adopted.

Bambauer and I also differ on what to make of due process. We are both proponents of the due process obligation to turn over known material, exculpatory information,[91] and more importantly would generally favor a meaningful open-file policy.[92] Unlike Bambauer, however, I do not believe there should be a due process obligation to "perform additional investigation in search of evidence that might prove the defendant's innocence and someone else's guilt."[93] Not only does she provide no standard to know *when* this obligation would be satisfied (*how much* searching of other people's records is enough?),[94] but the law traditionally considers the due process burden of proving guilt beyond a reasonable doubt a sufficient safeguard. It is hard to imagine how it is fundamentally unfair that police wrap up their investigation upon obtaining that quantum of evidence, and a

---

91. *See* Brady v. Maryland, 373 U.S. 83, 87 (1963).

92. *See* Bambauer, *supra* note 40, at 239; Taslitz & Henderson, *supra* note 85, at 217 (expressing skepticism for broad claims limiting discovery). Bambauer builds from Joshua A. T. Fairfield & Erik Luna, *Digital Innocence*, 99 CORNELL L. REV. 981 (2014). *See generally* Jane Bambauer, *Collection Anxiety*, 99 CORNELL L. REV. ONLINE 195 (2014) (commenting on the Fairfield and Luna article and prefacing the arguments of *Other People's Papers*).

93. Bambauer, *supra* note 40, at 238.

94. According to Bambauer,

> [S]uppose the criminal investigation has centered on a particular suspect and a search or arrest warrant can be justified on probable cause. Before the police take any of those formal steps, they should be able to use a crime-out subpoena to access data that might lead the police to more witnesses or other suspects.

Id. at 240. There seems to be no limiting principle to such an expansive notion of "search everyone," since any record could theoretically hold the key.

contrary rule could have seriously implications given very limited police resources.

But despite these two differences, given the broad agreement, it is surprising that Bambauer declares such a break from the past. She alleges that all previous reform efforts use "a cramped analytical model" that will "distort criminal justice."[95] The rest of us have all "looked backward for solutions, embracing rules that simulate the slow and costly process of investigating crime with old tools."[96] We thereby "unwittingly promote an outdated criminal investigation system riddled with inequities and error."[97] This would be damning indeed, were it an accurate representation. Fortunately, it is nothing of the sort.

The ABA LEATPR Standards have the most generous regime of accessing large bodies of de-identified records of which I am aware.[98] Bambauer alleges that "[s]o far, critics of the third-party doctrine have called for a warrant requirement to protect personal information contained in third party records."[99] Such a monolithic requirement would be problematic, as the Eleventh Circuit recently expressed en banc: permitting certain access upon lesser standards, "like other forms of compulsory process not subject to the search warrant procedure—help to build probable cause against the guilty, deflect suspicion from the innocent, aid in the search for truth, and judiciously allocate scarce investigative resources."[100] But before I began writing about any of this, Christopher Slobogin argued against a "warrant or nothing" model;[101] I have never advocated such an approach myself,[102] and the LEATPR Standards instead provide for a hierarchy of protections and only require a warrant for those that are ultimately considered highly protected.[103]

---

95. *Id.* at 205.

96. *Id.* at 209.

97. *Id.* at 210.

98. *See* LEATPR, *supra* note 11, Standard 25-5.6.

99. Bambauer, *supra* note 40, at 261.

100. United States v. Davis, 785 F.3d 498, 518 (11th Cir. 2015) (en banc).

101. *See* Christopher Slobogin, *Let's Not Bury* Terry*: A Call For Rejuvenation of the Proportionality Principle*, 72 ST. JOHN'S L. REV. 1053, 1081–85 (1998), which builds upon his earlier work, Christopher Slobogin, *The World Without a Fourth Amendment*, 39 UCLA L. REV. 1, 68–75 (1991); *see also* SLOBOGIN, *supra* note 86, at 21–47.

102. *See, e.g.*, Henderson, *All Fifty States*, *supra* note 20, at 417–25 (arguing for scalar protections); Henderson, *supra* note 56, at 1019 (disagreeing with a monolithic warrant proposal).

103. LEATPR, *supra* note 11, Standard 25-5.3. The Standards Commentary explains as follows:

> [I]n the Fourth Amendment context of the home, the Supreme Court in *Kyllo v. United States* refused to develop 'a jurisprudence specifying which home activities are "intimate" and which are not.' But the Court was able to decline such a jurisprudence only because it could hold that the use of sense-enhancing technology to determine *any* information regarding the interior of the home constitutes a search typically requiring a warrant supported by probable cause. In other words, *all* home activities are intimate

Indeed, the LEATPR Standards incorporate in some form all three of Bambauer's ultimate recommendations. First, she asserts that "[f]or crime-out investigations, police should be able to access third party records without probable cause or reasonable suspicion."[104] As just noted and as will be described in more detail below, although the Standards decided against a general adoption of Slobogin's target-driven versus event-drive framework, they not only include a generous selective revelation regime working with large bodies of de-identified records, but they more generally do not necessarily require probable cause or reasonable suspicion justifications before permitting access. Second, Bambauer asserts that "[f]or pattern-driven data mining programs, courts should permit law enforcement agencies to collect and analyze bulk records as long as there are means to test whether the programs are effective and evenhanded."[105] Again, the Standards include such a provision.[106]

Finally, Bambauer asserts that "unless a confidentiality statute is in place, individuals and businesses should be free to voluntarily share records in their control with the government out of deference to their First Amendment rights."[107] The Standards carve from their scope several scenarios. The first is anytime a third party is not acting as an institutional third party.[108] Such a person has an autonomy interest in choosing to share information that strikes me as more expansive than the corporate First Amendment interest Bambauer appropriately notes following *Citizens United*.[109] Second, the Standards exempt when an institutional third party

---

> so far as the Fourth Amendment is concerned. Because it would unduly cripple law enforcement to apply that same rule to all third-party records, it is impossible to avoid making distinctions based on the personal nature of information.

Id. Standard 25-4.1(b) cmt. (citations omitted).

104. Bambauer, *supra* note 40, at 262.

105. *Id.*

106. *See infra* subsection II(E)(3)(a).

107. Bambauer, *supra* note 40, at 263.

108. LEATPR, *supra* note 11, Standard 25-2.1(d).

109. Citizens United v. Fed. Election Comm'n, 558 U.S. 310 (2010). *See* LEATPR*, supra* note 11, Standard 25-2.1(d); Bambauer, *supra* note 40, at 259–61. For example, corporations lack Fifth Amendment privilege against self-incrimination rights. Bellis v. United States, 417 U.S. 85, 87 (1974). In the words of the Standards Commentary,

> [A]n individual has an autonomy and free speech interest in choosing to share information that will often trump any privacy interest. That is, the right of the purveyor of information to control its dissemination and use . . . is in significant tension with the freedom of the individual who receives the information to speak his or her mind. Institutional third parties may also have some First Amendment rights [citing to *Citizens United*], but these Standards assume that the balance in cases involving institutional record-holders is different than when the autonomy and freedom of expression of an individual not acting as a business entity are at stake.

LEATPR, *supra* note 11, Standard 25-2.1(d) cmt.

that is a crime victim discloses information.[110] And third, the Standards exempt anytime an institutional third party decides "of its own initiative and volition to provide information,"[111] a provision carefully designed to account for the "behind-the-scenes pressure" that Bambauer rightly acknowledges.[112]

Hence, while there do remain some disagreements, overall Bambauer and I, and Bambauer and the ABA LEATPR Standards, are very much working the same lines. In order to make this more clear and concrete, I next turn to considering how Bambauer's arguments would approach the Houston, Texas, cell-tower dump, and then how the Standards would do the same.

D. Applying Jane Bambauer's Other People's Papers

Bambauer argues that the law should permit a cell-tower dump "in order to identify who was near" the scene of a crime,[113] and thus she would permit the request made by the federal prosecutor in Houston: "This sort of information could give police an initial suspect pool that could then be winnowed further with the usual detective work."[114]

So far so good, in the sense of promoting police investigation. Only Bambauer provides no standard for determining *when* such a request is to be permitted. Is it permissible if it would identify fifteen phones? One hundred and fifty? One and half million? In her desire to "give wide latitude" to these investigations,[115] she offers only hints that the number cannot be too large. She is in favor of "small . . . dragnets,"[116] but what constitutes a big one? She would limit requests to "a designated temporal and geographic range,"[117] but of course a particularized designation can have any scope. The only hint of a standard comes in a footnote, explaining that "[a]n *inappropriately* tailored request will result in the return of data that is too numerous to be usefully followed-up by the investigation team."[118] So, apparently a very large police force can access very large data sets, whereas a

---

110. *Id.* Standard 25-2.1(f)(i).

111. *Id.* Standard 25-2.1(f)(ii).

112. Bambauer, *supra* note 40, at 260.

113. *Id.* at 234.

114. *Id.* One reason Bambauer favors these searches is because they entail less police discretion than others: "In other words, crime-out investigating imposes constraints on police discretion." *Id.* at 236. She notes two other scholars who have recently recognized the importance of limiting discretion, *see id.* at 236 n.152, and others could be added to that list. *See* Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. (forthcoming 2016) ("From general warrants to mass surveillance to high-tech snooping, courts and commentators have been clear that protection from generalized, arbitrary searches runs to the core of the Fourth Amendment."); Gray, *supra* note 17, at 1184 ("Rather, the point is that the Fourth Amendment targets government practices, which, if left to the unfettered discretion of government agents, would leave all of us and each of us insecure in our persons, houses, papers, and effects.").

115. Bambauer, *supra* note 40, at 238.

116. *Id.* at 236.

117. *Id.*

118. *Id.* at 237 n.154.

very small office can obtain next to nothing. Since this has no correlation to the privacy and liberty interests at stake, it strikes me as a less than ideal standard.

Moreover, her desired wide latitude is not limited to telephone records; police should "be able to access records about telephone calls, Internet searches, [and] credit card transactions."[119] Indeed records should generally be accessible, "whatever the data type."[120] Once again, there is no access standard based upon the privacy of those records because Bambauer is confident that, "[u]nlike the current, unbounded third party doctrine, this system cannot expand to cover the universe of records."[121] I am not so sure. Automatic-teller-machine records—and for that matter other banking records, sales records, and other business records more generally—would also indicate who was within a particular area at a particular time. If, as she posits, Internet searches are to be fair game, does that mean police are able to learn the identity of everyone having searched for information about a location in which crime happens to occur? Everyone who has searched for information about a manner of crime commission that happens to occur? Within what time period? Without articulated standards both for what types of records are permissible to access and in what quantity, it seems police are given carte blanche access to obtain incredibly diverse, private records about very large numbers of people, all on account of a crime having been committed. By contrast are the requirements of the LEATPR Standards.

E. Applying the ABA LEATPR Standards

The LEATPR Standards do not provide an answer to the question, "Should the federal prosecutor in Houston be able to access the requested cell-site location records?" Instead, the Standards provide a framework or algorithm through which the appropriate decision makers—such as the federal and state legislatures—can answer the question. That this structure is the most appropriate is well demonstrated in this instance, a situation in which everyone from courts to scholars are unsure and in disagreement. Over time, as typically happens in areas of criminal justice as divergent as the Fourth Amendment's exclusionary rule[122] to what constitutes cruel and unusual punishment,[123] consensus points will begin to emerge, and the Standards can be updated to provide more absolute guidance.

---

119. *Id.* at 237.

120. *Id.* at 236.

121. *Id.*

122. *See, e.g.*, Mapp v. Ohio, 367 U.S. 643, 651–53 (1961) (looking to developments in the states in reversing course regarding the exclusionary rule).

123. *See, e.g.*, Roper v. Simmons, 543 U.S. 551, 564–67 (2005) (looking to developments in the states in reversing course regarding the death penalty for juvenile offenders).

The LEATPR Standards first step is for a decision maker—say a legislature—to decide how private is the type of information, here cell-site location.[124] The Standards recognize four levels of privacy: large (highly private), medium (moderately private), small (minimally private), and not at all (not private).[125] The Standards provide four nonexclusive factors to consider in this determination, which ask the following: Why is the information in the hands of the third party? Is that transfer necessary to meaningfully participate in society, or one that we otherwise need to be wary of chilling?[126] How personal is the information? Will its access tend to embarrass or stigmatize, or, by contrast, is it information that we typically indiscriminately share?[127] Is the information in fact being accessed by others outside the third party?[128] Does existing law speak to access or restriction thereon?[129]

These are not always—perhaps not even often—easy questions. But when it comes to location data, it seems evident that privacy critically depends upon duration.[130] A single datum *could* place one in a strip club or church, assuming it is sufficiently geographically precise, but we constantly reveal current location to everyone around us. And it is recorded in everything from time-stamped image capture to a credit card or other identified store receipt.[131] So, it would not seem there is a high degree of privacy in a single datum. On the other hand, I agree with the five Justices in *United States v. Jones* who recognized that location information over an extended period of time (there twenty-eight days) can reveal a great deal, and is not generally known to others.[132] Therefore, at some duration, location information strikes me as highly private.

---

124. LEATPR, *supra* note 11, Standard 25-4.1. For a more detailed explanation of the Standards' methodology and reasoning, see the Standards Commentary or Henderson, *supra* note 10, at 811–15.

125. LEATPR, *supra* note 11, Standard 25-4.1.

126. *Id.* Standard 25-4.1(a).

127. *Id.* Standard 25-4.1(b).

128. *Id.* Standard 25-4.1(c).

129. *Id.* Standard 25-4.1(d).

130. *But see* Matthew B. Kugler & Lior Jacob Strahilevitz, *Surveillance Duration Doesn't Affect Privacy Expectations: An Empirical Test of the Mosaic Theory*, 2015 SUPREME CT. REV. (forthcoming 2016) (reporting on empirical study finding a longer duration of surveillance is considered more intrusive, but the magnitude of this difference is small).

131. *See* LEATPR, *supra* note 11, Standard 25-4.1. Law enforcement has thus used credit-card receipts to demonstrate location. *See* United States v. Kragness, 830 F.2d 842, 848 (8th Cir. 1987) ("[T]he government introduced a substantial volume of telephone and credit-card records, tracing the movement of and communication between participants in these drug activities.").

132. United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring) ("[T]he use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy"); *id.* at 955 (Sotomayor, J., concurring) (agreeing). None of the Justices disagreed with this proposition; four merely did not reach it. *Id.* at 954 (majority opinion) ("It may be that achieving the same result through electronic means, without an accompanying trespass, is an

There is likely to be disagreement as to where to draw the precise line. Perhaps one legislature will think over a week of location is highly private, while another will draw that line at anything over twenty-four hours.[133] But presumably none will consider the actual Houston request, namely for an hour of cell-site location, to be highly private. It might be moderately or minimally private, hopefully decided not only according to the direction provided in the Standards Commentary[134] but, more importantly, consistently with how that jurisdiction has decided to regulate other types of information. Finally, location for a single point in time might be considered not private.

Equipped with that privacy determination, the legislature would decide how much protection to provide such records outside of emergency and consent. If there were an emergency, for example if a kidnapper were believed to be carrying a mobile phone, then appropriate records could be obtained via officer request.[135] In the case of a cell-tower dump there is unlikely to be genuine interested-party consent, which would require that each phone subscriber agree to this very transfer of cell-site information.[136] And I will assume that all customers did not provide meaningful generalized permission for such access when they subscribed, meaning they were not provided this choice, or if they were, they did not opt in.[137] Under these

---

unconstitutional invasion of privacy, but the present case does not require us to answer that question."). In the words of the Standards Commentary:

> [L]imited location information may tell very little, but location over a significant period 'reveals an intimate picture of the subject's life that he expects no one to have—short perhaps of his spouse.' The potential of . . . location records to provide such a biography makes them more personal, and a legislature or other decision maker might therefore differentiate access regulation according to [duration].

LEATPR, *supra* note 11, Standard 25-4.1(b) cmt.

133. As for cell site location information, the Massachusetts Supreme Judicial Court recently drew the line as a matter of state constitutional law at six hours. Com. v. Estabrook, 38 N.E.3d 231, 231 (Mass. 2015). And the California legislature recently enacted a warrant requirement irrespective of duration. S.B. 178, 2015-2016 Reg. Sess. (Cal. 2015). I previously posited the twenty-four hour criterion:

> Given (1) that location information must necessarily be provided in order to use a mobile phone, (2) that mobile phones are becoming increasingly pervasive in the discourses of society, (3) that individually location information is often shared but collectively location information is highly personal and almost never shared outside of the necessary transfer to the provider, (4) that such information is not accessed by others, and (5) that—while far too confusing—existing legal protections are significant, I could imagine a decisionmaker deciding the following: Location at a single point in time is not private, a relatively short period of location information (say up to twenty-four hours) is moderately private, and anything longer is highly private. This is of course not the only solution, but it strikes me as a reasonable one.

Henderson, *supra* note 10, at 819. I proposed a similar criterion for stakeouts. *See id.* at 832–33.

134. *See* LEATPR, *supra* note 11, Standard 25-4.1 cmt; Henderson, *supra* note 10, at 815–20.

135. LEATPR, *supra* note 11, Standard 25-5.4.

136. *Id.* Standard 25-5.1(a).

137. *Id.* Standard 25-5.1(b).

circumstances, highly private records default to being highly protected (and thus requiring a warrant supported by probable cause),[138] moderately private records default to being moderately protected (and thus require one of three different court orders),[139] minimally private records default to being minimally protected (and thus require a prosecutorial or agency subpoena),[140] and not private records are unprotected and therefore may be obtained upon officer request for any legitimate law enforcement purpose.[141]

1. Case One: Law Enforcement Seeks a Single Point in Time, Unprotected.—Imagine that the legislature has deemed location information (including cell-site data) for a single point in time to be not private and therefore unprotected. And imagine further that law enforcement were satisfied with knowing everyone using the cell tower servicing that particular Houston location at the precise time that the surveillance camera captured the perpetrator with a cell phone to his ear, say 12:43 PM.[142] Then, as described above in considering the current Fourth Amendment rules,[143] from each customer's data being unprotected it seems to follow that a record including many such customers' data is unprotected.[144] To use an analogy, that law enforcement is free to read one newspaper article online means it is also free to read many such articles. Therefore, this limited cell-tower dump would be permissible upon officer request, because seeking the perpetrator of the crime is certainly a legitimate law enforcement purpose.[145] I am cautiously in favor of this result, because it seems to appropriately balance the law enforcement and privacy interests. If one believes it misguided, then either this information should not be unprotected or the Standards should separately regulate access to large bodies of unprotected information.

Would permitting this limited tower dump mean that a crafty police officer can make one such request every day for two months in order to obtain an hour's worth of data? Or even one such request every minute? I have previously argued that courts, ideally at legislative behest, should

---

138. *Id.* Standards 25-4.2(a), 25-5.3(a)(i).

139. *Id.* Standards 25-4.2(a), 25-5.3(a)(ii).

140. *Id.* Standards 25-4.2(a), 25-5.3(a)(iii).

141. *Id.* Standards 25-4.2(a), 25-5.3(d).

142. Providing this data might require the service provider to manipulate its stored records. For example, if those records show only that a call was placed within this tower location at 12:35 pm that lasted for twenty minutes, that phone number would need to be included within the request. If the service provider is not willing to do this and doing so is not required by law, then law enforcement would need to make a different request.

143. *See supra* subpart II(A).

144. The LEATPR Standards at several points contemplate that a provider will combine records of different types and/or pertaining to different persons. *See, e.g.*, LEATPR, *supra* note 11, Standard 25-1.1(c) (defining the focus of a record); *id.* Standard 25-4.2 ("If a record contains different types of information, it should be afforded the level of protection appropriate for the most private type it contains."); *id.* Standard 25-5.5 (providing for third-party redactions).

145. *See id.* Standard 25-5.3(d) cmt.

address such abuse of a lesser process, but that the law should not abandon the underlying rules on account of its potential.[146]

2. Case Two: Law Enforcement Seeks a Single Point in Time, Minimally Protected.—What if a legislature is swayed by that strip club or church example, and therefore considers even a single datum of location information to be minimally private and therefore minimally protected? This might be hard to imagine for the currently imprecise cell-site location, but the precision of that information will continue to increase.[147] Moreover, the same issue will arise if the police request a longer period of data that is considered minimally protected, such as ten minutes or a half hour.

According to the LEATPR Standards, minimally protected information should be accessible via an administrative or prosecutorial subpoena based upon relevance, and of course a legislature desiring this method of access would provide that requisite subpoena authority.[148] So, is the information contained within the cell-tower dump—all phones using the tower servicing a particular location at or within a particular time—relevant?

If the debates concerning USA PATRIOT Act Section 215[149] have taught us anything, it is that the term "relevant" is not as clear as we should

---

146. *See* Henderson, *supra* note 10 at 823–25. *See generally* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012) (articulating the potential issues when protections depend upon duration). As for legislatures taking the initial stab, "there is a 'strong presumption of constitutionality due to an Act of Congress, especially when it turns on what is "reasonable"'" United States v. Watson, 423 U.S. 411, 416 (1976) (quoting United States v. Di Re, 332 U.S. 581, 585 (1948)) (holding constitutional a warrantless probable-cause arrest in public). And a legislature can provide for creative procedures such as a citizen suit to have an officer fired over an egregious violation. *See, e.g.*, 18 PA. CONS. STAT. § 5726 (2015) ("Any aggrieved person shall have the right to bring an action in Commonwealth Court against any investigative or law enforcement officer . . . seeking the officer's . . . removal from . . . office or employment on the grounds that the officer . . . has intentionally violated the [wiretap] provisions of this chapter. If the court shall conclude that such officer . . . has in fact intentionally violated the provisions of this chapter, the court *shall order* the dismissal . . . of said officer . . . .") (emphasis added).

147. *See ECPA Reform*, *supra* note 5, at 15, 20, 26–27, 30, 95 (testimony of Professor Matt Blaze).

148. LEATPR, *supra* note 11, Standard 25-5.2(b) cmt.; *id.* Standard 25-5.3(a) cmt.

149. United and Strengthening America By Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, § 215, 115 Stat. 272, 287–88; (codified as amended at 50 U.S.C. § 1861 (2012)). For a comprehensive overview of "everything 215," see PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT, (2014), http://fas.org/irp/offdocs/pclob-215.pdf [http://perma.cc/V53L-NYDH] [hereinafter PCLOB REPORT]. Congress allowed § 215 to sunset and then replaced it in the Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act (USA FREEDOM Act) of 2015, Pub. L. No. 114-23, §§ 101–110, 129 Stat. 268, 269–277 (to be codified as amended at 18 U.S.C. § 1861). It is not clear that those in Congress read bills, but if warring acronyms become important, they have us covered. *See* Philip Bump, *364 Bills That Have Been Introduced in Congress, Ranked by Acronym Quality*, WASH. POST (Aug 3, 2015), http://www.washingtonpost.com/news/the-

wish it. Both the National Security Agency (NSA) and the secret Foreign Intelligence Surveillance Court (FISC) thought relevance permitted storing *all* phone metadata—though in this case it did not store cell-site location—because national security investigators might later wish to query that data based upon particularized suspicion.[150] If the data no longer exists, or is not structured in a format suitable to search, then perhaps this later desired access is impossible.[151]

The term "relevance" is perhaps used too cavalierly in too many different contexts. For example, it plays a central role in civil discovery,[152] administrative subpoenas,[153] grand jury investigation,[154] and trial evidence.[155] Andrew Ferguson has argued that big data makes it more difficult for such

---

fix/wp/2015/08/03/364-bills-that-have-been-introduced-in-congress-ranked-by-acronym-quality/ [http://perma.cc/5H8B-KM8M].

150. *See* Amended Memorandum Opinion, *In re* Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things, No. BR 13-109 (FISA Ct. Aug. 29, 2013), https://www.aclu.org/files/assets/br13-09-primary-order.pdf [http://perma.cc/A6P2-LJSB]; Order, *In re* Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things, No. BR 06-05 (FISA Ct. May 24, 2006), https://www.aclu.org/files/assets/pub_May%2024%202006%20Order%20from%20FISC.pdf [http://perma.cc/4A9K-UXTA]; PCLOB REPORT, *supra* note 149, at 21–25. The NSA was gathering the length of calls, the originating and destination phone numbers, and general information about caller location via trunk identification. ACLU v. Clapper, 785 F.3d 787, 793–97 (2d Cir. 2015). "A 'trunk identifier' provides information regarding how a call is routed through the telephone network, revealing general information about the parties' locations." *Id.* at 797 n.3.

151. For an analysis of this and other "Fourth Amendment time machines," see generally Stephen E. Henderson, *Fourth Amendment Time Machines (and What They Might Say About Police Body Cameras)*, 18 PENN. J. CONST. L. (forthcoming 2016).

152. *See* FED. R. CIV. P. 26(b)(1) ("Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense . . . . "); PCLOB REPORT, *supra* note 149, at 66–71.

153. *See, e.g.*, 21 U.S.C. § 876(a) (2012) ("In any investigation relating to his functions under this subchapter with respect to controlled substances . . . the Attorney General may subpoena witnesses, compel the attendance and testimony of witnesses, and require the production of any records (including books, papers, documents, and other tangible things which constitute or contain evidence) which the Attorney General finds relevant or material to the investigation."); PCLOB REPORT, *supra* note 149, at 74–78. For years, the DEA collected massive amounts of telephone metadata for *international* calls under its administrative subpoena authority, an apparent precursor to the NSA bulk collection. *See* Brad Heath, *U.S. Secretly Tracked Billions of Calls for Decades*, USA TODAY (Apr. 8, 2015, 10:36 AM), http://www.usatoday.com/story/news/2015/04/07/dea-bulk-telephone-surveillance-operation/70808616/ [http://perma.cc/46UK-UN2Z]. On federal administrative subpoenas, see generally U.S. DEP'T OF JUSTICE OFFICE OF LEGAL POLICY, REPORT TO CONGRESS ON THE USE OF ADMINISTRATIVE SUBPOENA AUTHORITIES BY EXECUTIVE BRANCH AGENCIES AND ENTITIES (2002), http://www.justice.gov/archive/olp/rpt_to_congress.htm [http://perma.cc/JR3N-BHJ6].

154. *See* United States v. R. Enters., Inc., 498 U.S. 292, 301 (1991) (interpreting Federal Rule of Civil Procedure 17(c) to render a subpoena unacceptable only when "there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury's investigation"); PCLOB REPORT, *supra* note 149, at 71–74 (analyzing NSA bulk telephone metadata surveillance under this standard); Taslitz & Henderson, *supra* note 85, at 204–06 (trying to make sense of this as a constitutional matter).

155. *See* FED. R. EVID. 401 ("Evidence is relevant if . . . it has any tendency to make a fact more or less probable than it would be without the evidence . . . .").

terms to provide meaningful restraint,[156] and has thus criticized the LEATPR Standards for incorporating the relevance standard.[157] But, looking to that grand jury practice, I agree with the Privacy and Civil Liberties Oversight Board[158] and the Second Circuit[159] that the NSA-FISC interpretation is not a conception the term can bear. If an entity were to gather all of the world's information, that data could later usefully be queried based upon particularized suspicion. Whereas if the information were not gathered, the later query might prove impossible. But relevance has never been equated to preemptive omniscience, no matter how much the J. Edgar Hoovers of the world might like it to be.[160]

Of course, the federal prosecutor did not request all of Houston's, let alone all the country's, cell-tower data because that data might later prove useful. Instead, on our current hypothetical, he requests only that from a single tower at a single point in time, or for a very brief duration on the order of ten minutes. It seems akin to a grand jury investigation of a bank in which the subpoena request is for a record of all deposits made in a particular branch at a particular time. Courts have certainly authorized more encompassing demands,[161] and thus it seems the cell-tower dump can satisfy the relevance standard and thus be permissible under the minimally protected framework.

It is interesting to ask whether the request would remain relevant if there was no surveillance video showing the perpetrator seemingly engaged in a phone call, since companies currently store location data only when the phone is being used. If the perpetrator's data is almost certainly *not* included, can the data be considered relevant? It would seem not. So, if the surveillance video showed no mobile phone, and one could be sure this was

---

156. *See generally* Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327 (2015).

157. *See* Ferguson, *supra* note 11, at 845–49, 865–68.

158. PCLOB REPORT, *supra* note 149, at 57 ("[B]ecause the records are collected in bulk—potentially encompassing all telephone calling records across the nation—they cannot be regarded as 'relevant' to any FBI investigation without redefining that word in a manner that is circular, unlimited in scope, and out of step with precedent from analogous legal contexts involving the production of records.").

159. ACLU v. Clapper, 785 F.3d 787, 818 (2d Cir. 2015) ("We conclude that to allow the government to collect phone records because they may become relevant to a possible authorized investigation in the future fails even the permissive 'relevance' test.").

160. Though this historic truth may not be reason enough to reject such omniscience as it becomes increasingly available. *See* Henderson, *supra* note 151.

161. *See In re* Grand Jury Proceedings: Subpoenas Duces Tecum, 827 F.2d 301, 302, 306 (8th Cir. 1987) (permitting grand jury request to a single Western Union office for all wire transfers over $1,000 during a period of two years and a summary of all wire transfers made during a single year). The PCLOB Report notes, however, that this Eight Circuit holding was "[t]he broadest grand jury subpoena that the government cites" in defense of the NSA bulk telephone metadata surveillance. PCLOB REPORT, *supra* note 149, at 73; *see also ACLU*, 785 F.3d at 813–15 (analyzing subpoena cases including this Eighth Circuit precedent).

the "complete picture," demonstrating relevance is at the very least a much more difficult issue. But what of when there is no surveillance video, or of when the perpetrator might have placed a phone in his pocket right before coming onscreen? Generally, I am not very confident in our understanding of relevance, and as data mining progresses to present us with statistical possibilities, I submit that we need to better develop the criterion.[162]

3. Case Three: Law Enforcement Seeks an Hour, Moderately Protected.—In the actual investigation, prosecutors sought an hour of tower data from each of the seven providers.[163] If an hour's worth of location data were considered minimally protected, this would be equivalent to Case Two. But what if a legislature considers an hour of data to be moderately private and thus moderately protected?

The LEATPR Standards provide a court order menu for law enforcement to access moderately protected information, any one of which could be selected by the legislature: a judicial determination of reasonable suspicion, a judicial determination of relevance, or a prosecutorial certification of relevance.

a. Judicial Determination of Reasonable Suspicion.—Reasonable suspicion is of course the statutory standard of the Stored Communications Act, or at least its typical interpretation.[164] As explained above in considering that statute, there does not seem to be reasonable suspicion in the Houston case, and therefore access would not be permitted.

There are, however, two important caveats. First, if the cell-tower data could be correlated with other information in a de-identified manner, including other tower data, then that correlation might itself provide reasonable suspicion. Bambauer posits the following hypothetical: "Suppose the Miami police department had requested all cell phone service providers to query their geolocation logs to identify any customers who were at three . . . robbery locations within an hour of the respective robberies."[165] But this is no mere hypothetical, as I have previously analyzed precisely such an investigation.

Ronald Capito and Joel Glore, the "High Country Bandits," robbed sixteen banks in four states, and were caught when police correlated the cell-tower records nearest several victim bank locations.[166] As I describe in detail

---

162. I have previously posited that relevance would not be satisfied as to the acquisition of records pertaining to 150,000 different phones where there was no indication of phone usage by the perpetrator. Henderson, *supra* note 10, at 826.

163. *In re* Application Houston, *supra* note 1, at 674.

164. *See supra* subpart II(B).

165. Bambauer, *supra* note 40, at 207–08.

166. Henderson, *supra* note 10, at 804–05.

in another article,[167] the LEATPR Standards permit any politically accountable law enforcement official to access an appropriately inclusive body of de-identified records through a writing that certifies "that there is a reasonable possibility that the record is relevant to initiating or pursuing an investigation."[168] And if correlation of those records demonstrates the requisite level of suspicion ordinarily necessary to access the type of data at issue—here reasonable suspicion—then law enforcement may re-identify that data.[169] In the investigation of the High Country Bandits precisely this would have occurred, as the data included only two phones at or near all of the relevant robberies; police ultimately learned that one belonged to robber Capito and the other to robber Glore.[170]

So far as I know, the LEATPR Standards' de-identification provisions are the first concrete proposal of their kind, and it certainly makes it difficult to see them as looking "backward for solutions, embracing rules that simulate the slow and costly process of investigating crime with old tools,"[171] thereby "unwittingly promot[ing] an outdated criminal investigation system."[172] Which is a good thing, because this type of correlation is increasingly common. It is what led to the identification of Paula Broadwell as the source of threatening communications,[173] which ultimately unraveled into the resignation and criminal prosecution of General and CIA Director David Petraeus.[174] The messages had been sent anonymously from hotel networks, but investigators were able to correlate the guest lists for those various hotels on the relevant dates.[175] Investigators have similarly identified those trading in child pornography.[176]

---

167. *Id.* at 826–31.

168. LEATPR, *supra* note 11, Standard 25-5.2(c); *id.* Standard 25-5.6(a).

169. *Id.* Standard 25-5.6(b); *see also id.* Standard 25-5.3.

170. Betz, *supra* note 12.

171. Bambauer, *supra* note 40, at 209.

172. *Id.* at 210.

173. *See* Michael Isikoff & Bob Sullivan, *Emails on 'Coming and Goings' of Petraeus, Other Military Officials Escalated FBI Concerns*, NBC NEWS (Nov. 12, 2012, 5:30 PM), http://openchannel.nbcnews.com/_news/2012/11/12/15119872-emails-on-coming-and-goings-of-petraeus-other-military-officials-escalated-fbi-concerns [http://perma.cc/U5JT-YVA5].

174. Adam Goldman, *Petraeus Pleads Guilty to Mishandling Classified Material, Will Face Probation*, WASH. POST (Apr. 23, 2015), https://www.washingtonpost.com/world/national-security/petraeus-set-to-plead-guilty-to-mishandling-classified-materials/2015/04/22/3e6dbf20-e8f5-11e4-aae1-d642717d8afa_story.html [https://perma.cc/2DTG-MZVG].

175. Isikoff & Sullivan, *supra* note 173.

176. *See In re* Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335, 1339 (11th Cir. 2012). The technique could also be useful in national security investigations, correlating those who repeatedly appear near the same location as a person of interest or correlating persons who mutually turn off mobile phones at similar times. BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 39 (2015).

So, while the government has not released sufficient facts about the Houston investigation—the order remains under seal—correlation will sometimes provide the requisite reasonable suspicion. And this can occur even if there is only a single crime under investigation. For example, if an eyewitness recalled a partial license plate, a correlation of license-plate data with the cell-tower data might provide reasonable suspicion. Or, if one perpetrator in a joint crime were recognized or discovered, correlating his phone records with those of a tower dump might provide reasonable suspicion. Or, if an eyewitness description or security-camera footage was sufficiently clear, a computer running facial-recognition technology might correlate the database of driver's license records with the cell-tower records, and if there are only one or a few hits, that would provide the requisite reasonable suspicion. One can see, then, that the difference between Bambauer's proposal and that of the Standards is *not* that one will permit access and the other will not, but rather that the Standards articulate legal standards that must be satisfied, thus providing a means of differentiating lawful from unlawful access.

The second caveat permitting access despite an initial lack of reasonable suspicion, the LEATPR Standards safety valve, is considered below.

b. LEATPR Safety Valve.—The Standards have even more flexibility. Even if (1) law enforcement wants an hour of cell-site location data, (2) the legislature considers such data to be moderately private, and (3) the legislature decides the reasonable suspicion court order is typically the appropriate means of access, the legislature can deviate downward from the default level of protection if that limitation "would render law enforcement unable to solve or prevent an unacceptable amount of otherwise solvable or preventable crime, such that the benefits of respecting privacy are outweighed by this social cost."[177] Unsurprisingly, not everyone working on the Standards was in favor of this provision, as it could be used to gut them. But most felt that in the hands of a legislature it was a proper tool, and the Commentary provides the example of hospital admission records evidencing a violent wound.[178] Most jurisdictions affirmatively require disclosure of such records, which seems the correct result but otherwise inconsistent with the privacy that should be afforded medical files.[179] Thus, a legislature believing the requested cell-tower data moderately private could nonetheless, consistent with the Standards, provide it only minimal (or even no) protection when requested in the form of a cell-tower dump in the context of seeking leads based upon a single, isolated crime.

177. LEATPR, *supra* note 11, Standard 25-4.2(b); *see also id.* Standard 25-4.2(b) cmt.
178. *Id.* Standard 25-4.2(b) cmt.
179. *Id.*

c. Judicial or Prosecutorial Determination of Relevance.—For moderately protected information the Standards provide a court order menu.[180] Above I have already considered a judicial determination of reasonable suspicion;[181] the other two options are a judicial determination of relevance or even a mere prosecutorial certification of relevance like that of the federal Pen Trap Act.[182] Relevance too has already been considered above, in the context of asking whether it is satisfied as to a single point in time at which the security camera captured the perpetrator apparently speaking on the phone, or to a very short duration around that point (e.g., ten minutes).[183] It seems likely an hour's worth of data would also be considered relevant. As with reasonable suspicion, relevance should require some hit to no-hit ratio,[184] but of course a lesser ratio would be required for the lesser relevance standard. Thus, if a legislature selected either of these options, law enforcement would likely be permitted the hour of cell-tower data.

III. Conclusion

I am glad that I have not yet discovered what I consider a major flaw in the ABA LEATPR Standards, but they are of course imperfect.[185] It was for this purpose that I convened a symposium on the Standards a couple of years ago: to discover flaws and continue moving the ball forward.[186] I am thus excited that Jane Bambauer's encompassing article leads her to conclusions largely consistent with the Standards, and I am glad to take this opportunity to work out the Standards' application in yet another context.

Table One summarizes the likely outcomes for a cell-tower dump following a crime at a particular location where tower data is requested as to a single point in time. Table Two summarizes the likely outcomes in which an hour of data is requested. Although some of the moderately protected options have the same substantive standard as minimal protection, they have the added procedural protection of court involvement.

---

180. *Id.* Standard 25-5.2(a); *id.* Standard 25-5.3(a)(ii).

181. *See supra* subsection II(E)(3)(a).

182. 18 U.S.C. § 3122(b)(2) (2012) (requiring "a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation").

183. *See supra* section II(E)(2).

184. *See supra* subpart II(B).

185. *See, e.g.*, Henderson, *supra* note 39, at 716–19 (criticizing formulation of grand jury carve out and court constitutional carve out).

186. *See, e.g.*, Marc Jonathan Blitz, *Third Party Records Protection on the Model of Heightened Scrutiny*, 66 OKLA. L. REV. 747 (2014); Thomas P. Crocker, *Ubiquitous Privacy*, 66 OKLA. L. REV. 791 (2014); David Gray, *The ABA Standards for Criminal Justice: Law Enforcement Access to Third Party Records: Critical Perspectives from a Technology-Centered Approach to Quantitative Privacy*, 66 OKLA. L. REV. 919 (2014).

Table 1: Law Enforcement Requests Cell-Tower Data for a Single Point in Time

	Legislative Determination	Dump Permissible?
1.	Unprotected	**Yes** (regardless of quantity of mobile numbers thereby disclosed)
2.	Minimally Protected	**Yes . . .** so long as the quantity of numbers disclosed is not so large as to exceed the relevance threshold; perhaps dependent upon reason to believe the perpetrator was using a phone

Table 2. Law Enforcement Requests Cell-Tower Data for an Hour

	Legislative Determination	Dump Permissible?
3.	Minimally Protected	Same as Number 2
4.	Moderately Protected, Reasonable Suspicion Court Order	**No . . .** unless (1) can correlate with other de-identified data or (2) legislature invokes the safety valve for this circumstance
5.	Moderately Protected, Relevance Court Order	Same as Number 2
6.	Moderately Protected, Certification Court Order	Same as Number 2

It would be ideal to have a single, precise answer, and at this point my preferences are options One and Four. But that level of precision would be unacceptable in criminal justice standards before widespread norms begin to emerge, and that may explain why Bambauer does not articulate a limiting standard despite her thoughtful normative analysis. Regardless of result, I am a firm believer that there is value in working through the same algorithm for every type of data under consideration, as opposed to the ad hoc nature of historic legislation. This is the key contribution of the ABA LEATPR Standards. And to the extent this analysis, like other contemporary issues of policing and national security surveillance, exposes uncertainty in the criminal justice standards of investigation (relevance, reasonable suspicion,

and probable cause), this is something on which scholars, courts, and legislatures should focus greater attention.