William & Mary Bill of Rights Journal

Volume *26 (2017-2018)*
Issue 2 *Symposium: Big Data, National Security, and the Fourth Amendment*

Article 11

December 2017

Carpenter v. United States and the Fourth Amendment: The Best Way Forward

Stephen E. Henderson

CARPENTER V. UNITED STATES AND THE FOURTH AMENDMENT: THE BEST WAY FORWARD

Stephen E. Henderson*

ABSTRACT

We finally have a federal 'test case.' In *Carpenter v. United States*, the Supreme Court is poised to set the direction of the Fourth Amendment in the digital age. The case squarely presents how the twentieth-century third party doctrine will fare in contemporary times, and the stakes could not be higher. This Article reviews the *Carpenter* case and how it fits within the greater discussion of the Fourth Amendment third party doctrine and location surveillance, and I express a hope that the Court will be both a bit ambitious and a good measure cautious.

As for ambition, the Court must recognize that the fundamental liberty protected by the Fourth Amendment—the right to be "secure in [our] persons, houses, papers, and effects"—is squarely at issue when the government seeks to track our longer term movements, whether historically or prospectively. It is not business records, beepers, automobiles, phones, cameras, drones, or some other coincidental medium or technology that is at issue: it is our constitutionally protected liberty. Thus, the Court should hold that law enforcement acquisition of longer term cell site location information (CSLI) constitutes a Fourth Amendment search, ending the monolithic, anachronistic third party doctrine.

As to the precise durational trigger and as to what particular law enforcement restraint would be correspondingly reasonable, the Court should be cautious, as it was in *United States v. Jones* and *Grady v. North Carolina*. It will have taken the better part of a half century to undo the Court's expansive third-party declaration in *United States v. Miller*, an unnecessary overreach best relegated to history. Thus, while the Court should not abandon Fourth Amendment development through reasonable reliance, it should remand these constitutional determinations for lower court development. Those courts should consider not only Fourth Amendment precedents, but also how state supreme courts have independently interpreted their own constitutions.

---

* Judge Haskell A. Holloman Professor of Law, The University of Oklahoma. JD Yale Law School, 1999; BS in Electrical Engineering U.C. Davis, 1995. I would like to thank Adam Gershowitz, Will Cook, and everyone who helped with and participated in the *Big Data, National Security, and the Fourth Amendment* Symposium. Everything was top notch. And I would like to thank Jordan Rubin and Matthew Tokson for helpful comments on an earlier draft.

I. THE *CARPENTER* CASE

Timothy Carpenter has ended up an ironic criminal: he organized multiple armed robberies targeting smartphones, only to have his downfall be (in part) records of his own cell phone usage.[1] As is so often the case when it comes to our Fourth Amendment rights,[2] he is hardly a good or representative spokesperson. But the courts suppress unconstitutionally obtained evidence in order to protect us all,[3] and so what is relevant is his constitutional claim, not his personal desert. Here is his story.

---

[1] United States v. Carpenter, 819 F.3d 880, 884–85 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (June 5, 2017) (No. 16-402).

[2] The Fourth Amendment provides:

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

U.S. CONST. amend. IV.

[3] Stone v. Powell, 428 U.S. 465, 490–92 (1976) ("Application of the [exclusionary] rule thus deflects the truthfinding process and often frees the guilty. . . . Evidence obtained by police officers in violation of the Fourth Amendment is excluded at trial in the hope that the frequency of future violations will decrease. Despite the absence of supportive empirical evidence, we have assumed that the immediate effect of exclusion will be to discourage law enforcement officials from violating the Fourth Amendment by removing the incentive to disregard it. More importantly, over the long term, this demonstration that our society attaches serious consequences to violation of constitutional rights is thought to encourage those who formulate law enforcement policies, and the officers who implement them, to incorporate Fourth Amendment ideals into their value system.").

A. The Investigation

Beginning in 2010 and continuing into 2012, several men robbed RadioShack and T-Mobile stores in southeastern Michigan and northwestern Ohio, netting mobile phones they would thereafter sell.[4] A larger group assisted in these robberies as lookouts and getaway drivers.[5] The organizer was typically Timothy Carpenter, who would also serve as a lookout.[6] That latter role put him near the crimes during their commission, in which he was joined by his half-brother, Timothy Sanders.[7]

Faced with a string of robberies, the government will sometimes use cell tower dumps to identify those near multiple crimes,[8] but such methods may or may not have been used in this case. What we know is that four men were arrested, and that one of them confessed.[9] He provided his cell phone number and those of co-conspirators, which naturally left investigators wanting the records of the persons with whom he communicated.[10]

Pursuant to a court order under the Stored Communications Act,[11] the FBI thus obtained 127 days of Carpenter's phone records (weighing in at 186 pages) and eighty-eight days of Sanders's.[12] These records included "cell site information . . . at call origination and at call termination for incoming and outgoing calls."[13] Using that cell-site location information (CSLI), a special agent created maps showing the proximity of both Carpenter and Sanders to the robberies during their commission.[14] These maps and related testimony helped lead to their conviction and, in Carpenter's case, to a sentence of over 100 years in prison.[15]

---

[4] *Carpenter*, 819 F.3d at 884–85.

[5] *Id.* at 884.

[6] *Id.* Carpenter would often also supply the guns used by those who would rob the stores. *Id.*

[7] *Id.* at 884–85.

[8] *See generally* 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 (2013) [hereinafter Henderson, *Location Surveillance After* Jones] (describing and analyzing such an investigation); *Verizon's Transparency Report for the 1st Half of 2017: U.S. Report*, VERIZON, http://www.verizon.com/about/portal/transparency-report/us-report/ [https://perma.cc/W9UL-JKTM] (last visited Dec. 4, 2017) (noting that cell tower dumps are "being used much more frequently by law enforcement").

[9] *Carpenter*, 819 F.3d at 884.

[10] *Id.*

[11] 18 U.S.C. § 2703(d) (2012).

[12] *Carpenter*, 819 F.3d at 886. A much smaller amount of data was also obtained from a second provider. Petition for Writ of Certiorari, *Carpenter*, 819 F.3d 880, *cert. granted*, 137 S. Ct. 2211 (June 5, 2017) (No. 16-402).

[13] *Carpenter*, 819 F.3d at 884.

[14] *Id.* at 885.

[15] *Id.* Carpenter's sentence is so long because he was convicted of five counts of "aiding and abbetting the use or carriage of a firearm during a federal crime of violence," a crime that for any second and further conviction carries a mandatory minimum twenty-five-year

B. The CSLI

A mobile phone is in regular communication with at least one cell tower—often the nearest tower—anytime the phone is 'active,' typically meaning anytime it is turned on.[16] Were this not the case, it would be impossible to receive a call.[17] Therefore, in theory, the mobile phone provider knows—or at least its computers know—to which tower subscribers are nearest and, because those towers use different antennas for different directions, within which 'sector' or 'pie piece' the subscriber is located.[18] In other words, if a given cell tower serves a radius of two miles and uses sectors of 60 degrees, and if we imagine the coverage area as a circle in two dimensions, then the provider knows the subscriber location to within 2.1 square miles, as shown in Figure 1.[19] Why 2.1 square miles? Because a circle has an area of pi multiplied by

consecutive sentence. *Id.* at 884; *see* 18 U.S.C. § 924(c) (2012). Sanders was sentenced to just over fourteen years. *Carpenter*, 819 F.3d at 885.

[16] *Carpenter*, 819 F.3d at 885. The user can prevent such automated communication by putting her device in 'airplane,' 'flight,' or 'standalone' mode, which turns off radio service. *See, e.g.*, *Use Airplane Mode on Your iPhone, iPad, iPod Touch, and Apple Watch*, APPLE, https://support.apple.com/en-us/HT204234 [https://perma.cc/PJ8P-LMEW] (last visited Dec. 4, 2017). At least she can do so unless the CIA or someone else has hacked her device. *See* Ira "Gus" Hunt, CIA Chief Technology Officer, Address at Gigaom Structure Data Event (Mar. 20, 2013), https://www.youtube.com/watch?v=GUPd2uMiXXg (at 12:15) ("You are aware of the fact that somebody can know where you are at all times, because you carry a mobile device, even if that mobile device is turned off. You know this, I hope? Yes? No? Alright; well, you should."); *see also 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. 12–14 (2010) [hereinafter *Location Based Technologies Hearing*] (testimony of Professor Matt Blaze) (explaining the technology of mobile telephony).

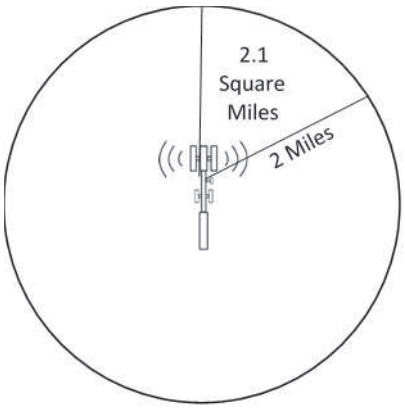
[17] *See Location Based Technologies Hearing*, *supra* note 16, at 14.

[18] *Carpenter*, 819 F.3d at 885; Stephanie K. Pell, *Location Tracking*, *in* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW 44, 47–48 (David Gray & Stephen E. Henderson eds., 2017).

[19] The provider can make a better estimate of location based on signal strength, which can be correlated with distance from the tower, and can do even better if the signal can be triangulated using several towers. *See* Phil Locke, *Cell Tower Triangulation—How It Works*, WRONGFUL CONVICTIONS BLOG (June 1, 2012), https://wrongfulconvictionsblog.org/2012/06/01/cell-tower-triangulation-how-it-works/ [https://perma.cc/5MNB-YTMA] (describing triangulation for a group of three-sector towers). But such a precise location will typically not be calculated, let alone recorded in records later received by law enforcement, at least not based upon current business practices. *See* Tom Jackman, *Experts Say Law Enforcement's Use of Cellphone Records Can Be Inaccurate*, WASH. POST (June 27, 2014), https://www.washingtonpost.com/local/experts-say-law-enforcements-use-of-cellphone-records-can-be-inaccurate/2014/06/27/028be93c-faf3-11e3-932c-0a55b81f48ce_story.html [https://perma.cc/PTL3-HN3T] [hereinafter Jackman, *Experts Say*]. Such precision was not at issue in *Carpenter*. Thus, I will disregard such details. As will become clear shortly, all of this is merely a back-of-the-envelope approximation, which—like any scientific model—is perfectly adequate for some purposes but totally unacceptable for others.

the radius squared, but given the 60-degree sector, this is only one-sixth of a circle.[20] If the subscriber moves out of that sector, her phone will begin communicating with a different sector or tower, or lose signal, as the case may be.[21]

Figure 1
A Single Cell Tower (Circular Model)



This model will work for our purposes, but it is at best imprecise. After all, while electromagnetic waves do distribute spherically—making for a circle in two dimensions—if this accurately represented cellular coverage, we would be very unhappy. Just look at Figure 2, in which many a phone user would be without coverage. So, cell sites are sometimes represented by interlocking hexagons, but that too is not a physically accurate representation.[22] Cell sites need to substantially overlap in order to seamlessly hand off calls from one site to the other, and every site is irregular because of obstructions (such as trees and buildings) and signal reflections.[23] Moreover, the goal of the provider's switching equipment is not to

---

[20] A bit more detail: The area of a circle is computed by multiplying π by the square of the radius (πr^2), meaning that in this case the tower has a coverage area of 4π square miles, which is approximately 12.6 square miles. That coverage area is segmented into 60 degree sectors, of which there are six (the 360 degrees of a circle divided into six equal sectors). So, 4π square miles divided by six ($\pi r^2/6$), which is approximately 2.1 square miles.

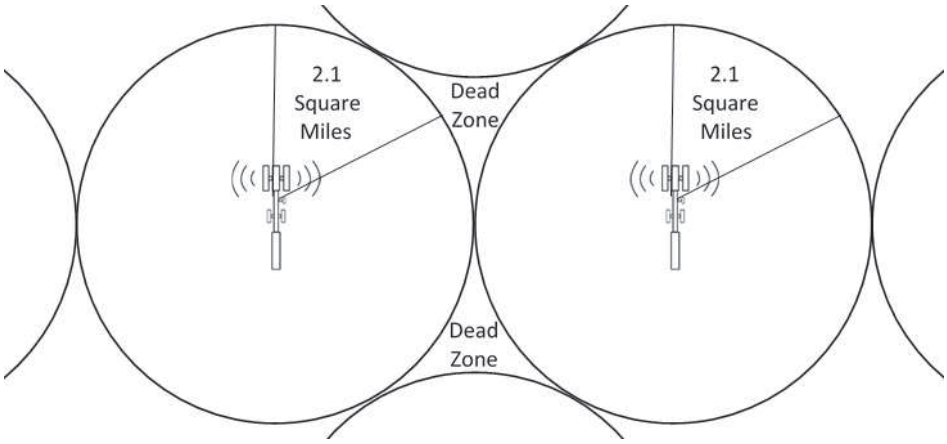
[21] *See Location Based Technologies Hearing*, *supra* note 16, at 13–14.

[22] *See* James Donovan, *Cells, Sectors and Antenna Beamforming*, COMMSCOPE (May 28, 2014), http://www.commscope.com/Blog/Cells--Sectors-and-Antenna-Beamforming/ [https://perma.cc/9CNP-76ZE].

[23] *See What Is a Cell Tower's Range*?, WASH. POST. (June 27, 2014), https://www.washingtonpost.com/local/what-is-a-cell-towers-range/2014/06/27/a41152ce-fe3b-11e3-b1f4-8e77c632c07b_graphic.html?utm_term=.96df0b5a6635 [https://perma.cc/6PPU-UP79].

discern customer location, but to provide excellent service, which might mean using a farther tower—assuming adequate signal—in order to better balance the load.[24] In short, to quote George Box, "all models are wrong, but some are useful,"[25] and since our only interest will be in ballpark estimates that give a rough sense of CSLI location precision, we can use circles to keep the math easy. But in a courtroom, lawyers should exercise significant care.[26]

Figure 2
Multiple Cell Towers (Circular Model)



Figures 1 and 2 make obvious that the precision of CSLI location information increases as the number of towers within an area increases, resulting in a corresponding decrease in the coverage area of each tower sector. For example, if the tower serves a radius of one mile rather than two, the precision of the cell-site location—using our circular model—increases by a factor of four, placing the subscriber within a half square mile.[27] If the tower serves a radius of one-half mile, then the subscriber is located within one-tenth (0.1) of a square mile, and so on, and sometimes specialized towers serve quite small areas.[28]

---

[24] *See id.*; Jackman, *Experts Say*, *supra* note 19.

[25] GEORGE E. P. BOX & NORMAN R. DRAPER, EMPIRICAL MODEL-BUILDING AND RESPONSE SURFACES 424 (1987).

[26] Readers may be familiar with the cell-site location dispute relating to the conviction of Adnan Syed, the central character in the podcast *Serial*. *See* Jessica Anderson, *Appeal to Be Heard in 'Serial' Case Thursday: Court to Rule on Request for New Trial for Adnan Syed, Convicted in 2000 Killing*, BALT. SUN, June 7, 2017, at 2.

[27] The decrease is a factor of four, rather than two, because the area of a circle is proportional to the *square* of the radius.

[28] *See* United States v. Graham, 824 F.3d 421, 448 (4th Cir. 2016) (en banc) (Wynn, J., dissenting in part) (explaining increasing precision using smaller cells); Pell, *supra* note 18, at

In Carpenter's case, the relevant cell towers had coverage radii of between one-half mile and two miles,[29] meaning that location precision on our circular, 60-degree sector model ranges between 0.1 square miles to 2.1 square miles. The Sixth Circuit reported these figures in square feet, making the numbers much larger[30]: such sectors would range from an area of 3.6 million square feet to 58 million square feet (there of course being 5,280 feet in a mile).[31] If a tower had a larger, 120-degree sector—which some of them did—that upper range doubles to 117 million square feet, or 4.2 square miles.[32]

So, federal agents obtained 127 days of cell-site information, each datum of which under our circular model placed Carpenter within an area ranging from 0.1 square miles to 4.2 square miles. In terms that might be somewhat more familiar, that is a range of 84 acres to 2,700 acres.[33] In the college town of Norman, Oklahoma, where I live and where college football is king, the more precise area would not place someone at Gaylord Memorial Stadium (were the geographic area a circle of 0.1 square miles centered there), but she would have to be nearby on campus; she could certainly not be at the law school.[34] The larger area, by contrast, would mean she could not only be most anywhere on campus, but could also be in any of the private businesses on our 'campus corner,' in many residential neighborhoods, or in our downtown area north of campus.[35] In Washington, D.C., where the

---

48–49 (same); *Location Based Technologies Hearing*, *supra* note 16, at 15, 20, 26–27, 30, 95 (same).

[29] United States v. Carpenter, 819 F.3d 880, 889 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (June 5, 2017) (No. 16-402).

[30] *Id.*

[31] In calculating the sector areas, I have used the original radius of one-half mile and two miles, respectively, *not* the rounded square mile values.

[32] *Carpenter*, 819 F.3d at 889. The Sixth Circuit cites a "3.5 million square-foot to 100 million square-foot area." *Id.* The expert on which the court relied obviously either did not use a circular model, or imprecision arose from a less precise approximation of π, a more precise radius, different rounding to significant digits, or other such reasons. The extent of the deviation is rather meaningless, since surely only the order of magnitude is meaningful when it comes to millions of square feet. Thus, I have not bothered being consistent in terms of my own rounding, merely reporting numbers in a precision that seems most approachable.

[33] I have once again used the original radii for the calculations, not merely area unit conversion, and have rounded the result rather cavalierly.

[34] *See* Gaylord Family Oklahoma Memorial Stadium, GOOGLE MAPS, https://www.google.com/maps/place/The+Gaylord+Family+Oklahoma+Memorial+Stadium/@35.205503,-97.4448048,1571m/data=!3m1!1e3!4m5!3m4!1s0x0:0x1abd3cf33ea1be12!8m2!3d35.2058537!4d-97.4423145. Of course, all of this depends upon the particular location of the cell towers, and the cell site area in our model is a circle *sector* as opposed to a full circle; these illustrations are merely intended to give a sense of the size of these areas. In other words, a 0.1 square mile area corresponds to a circle with a radius of about 1,000 feet, and so to give a sense of how big an area that is, I have centered such a circle on the stadium.

[35] *See* Gaylord Family Oklahoma Memorial Stadium, GOOGLE MAPS, https://www.google.com/maps/place/The+Gaylord+Family+Oklahoma+Memorial+Stadium/@35.2057619,

Supreme Court sits, the more precise area would not place someone at the courthouse (again centering a 0.1 square mile circle there), but she would have to be nearby, perhaps visiting the Library of Congress or the Hart Senate Office Building.[36] The larger area, by contrast, would allow her to reach the Verizon Center, the Navy Yard, and well past Lincoln Park.[37] (If one who does not enjoy math wishes to see areas plotted on any Google map, a very useful site is available from DaftLogic—merely bring up a location, left-click some pins into existence, and witness the area of the covered shape.[38])

C. The Sixth Circuit Majority (and Its Mistakes)

Two judges, in an opinion written by Judge Raymond Kethledge, held that Carpenter had no reasonable expectation of privacy in the 127 days of cell-site information, meaning that agents obtaining the data did not constitute a Fourth Amendment search.[39] The court relied upon the long-standing Fourth Amendment third

---

-97.4528656,4441m/data=!3m1!1e3!4m5!3m4!1s0x0:0x1abd3cf33ea1be12!8m2!3d35.2058537!4d-97.4423145.

[36] *See* United States Supreme Court Building, GOOGLE MAPS, https://www.google.com/maps/place/United+States+Supreme+Court+Building,+Washington,+DC+20543/@38.8895761,-77.0117459,15z/data=!4m5!3m4!1s0x89b7b82f32bfd767:0x1ab5dfbb56f376ca!8m2!3d38.8906116!4d-77.0045361.

[37] *See* United States Supreme Court Building, GOOGLE MAPS, https://www.google.com/maps/place/United+States+Supreme+Court+Building,+Washington,+DC+20543/@38.8888094,-77.0120395,4241m/data=!3m1!1e3!4m5!3m4!1s0x0:0x1ab5dfbb56f376ca!8m2!3d38.8906116!4d-77.0045361+States+Supreme+Court+Building,+Washington,+DC.

[38] *Google Maps Area Calculator Tool*, DAFTLOGIC, https://www.daftlogic.com/projects-google-maps-area-calculator-tool.htm [https://perma.cc/PDM4-NZ2U] (last visited Dec. 4, 2017).

[39] United States v. Carpenter, 819 F.3d 880, 890 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (June 5, 2017) (No. 16-402) ("In sum, we hold that the government's collection of business records containing cell-site data was not a search under the Fourth Amendment."). This holding comports with others in the federal courts, but some states disagree as a matter of their constitutional law. *See, e.g.*, United States v. Wallace, 866 F.3d 605 (5th Cir. 2017) (holding a mobile phone customer retains no reasonable expectation of privacy even in prospective CSLI); United States v. Graham, 824 F.3d 421 (4th Cir. 2016) (en banc) (holding a mobile phone customer retains no reasonable expectation of privacy in historic CSLI); United States v. Davis, 785 F.3d 498 (11th Cir. 2015) (en banc) (same); *In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013) (same); United States v. Skinner, 690 F.3d 772 (6th Cir. 2012) (same for prospective CSLI); *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304 (3d. Cir. 2010) (holding the federal Stored Communications Act allows a magistrate to choose to require a probable cause warrant for historic CSLI); Zanders v. State, 73 N.E.3d 178 (Ind. 2017) (holding a mobile phone customer retains no reasonable expectation of privacy in historic CSLI); State v. Jenkins, 884 N.W.2d 429 (Neb. 2016) (same); Taylor v. State, 371 P.3d 1036 (Nev. 2016) (same); Commonwealth v. Estabrook, 38 N.E.3d 231 (Mass. 2015) (holding the Massachusetts Constitution requires a warrant to

party doctrine—the records were business records held by and obtained from a third-party phone company[40]—upon the relative imprecision of the location data,[41] and upon Congress's having spoken through the Stored Communications Act.[42] Each of these grounds is facially attractive on some level but ultimately flawed, at least now that the issue is before the high court.

1. The Third Party Doctrine

The third party doctrine grew out of a series of Supreme Court decisions in the 1960s and 1970s,[43] and is perhaps best summarized by this very expansive language in *United States v. Miller*[44]:

> This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by [the third party] to Government authorities, even if the information is revealed [to the third party] on the assumption that [1] it will be used only for a limited purpose and [2] the confidence placed in the third party will not be betrayed.[45]

It is possible to distinguish *Carpenter*'s facts from even this exceedingly broad claim. The three opinions cited by the *Miller* Court as establishing the 'repeated' holding all concern instances in which a defendant voluntarily spoke to an informant and those words were at issue.[46] Such situations hardly seem to control whether a mobile phone subscriber retains a reasonable expectation of privacy in her location

---

obtain over six hours of CSLI); Tracey v. State, 152 So. 3d 504 (Fla. 2014) (holding the Fourth Amendment requires a warrant for real-time CSLI); State v. Earls, 70 A.3d 630 (N.J. 2013) (holding the New Jersey Constitution requires a warrant to obtain CSLI); *see also* United States v. Lambis, 197 F. Supp. 3d 606 (S.D.N.Y. 2016) (requiring a warrant to use a cell-site simulator, often known as a "Stingray"). Various state statutes also apply. *See Cell Phone Location Tracking Laws by State*, ACLU, https://www.aclu.org/map/cell-phone-location-tracking-laws-state [https://perma.cc/SGW4-X72D] (last visited Dec. 4, 2017).

[40] *Carpenter*, 819 F.3d at 886–89.

[41] *Id.* at 889.

[42] *Id.* at 890.

[43] *See* 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*] (tracing the development of the doctrine).

[44] 425 U.S. 435 (1976).

[45] *Id.* at 443.

[46] *See id.*; United States v. White, 401 U.S. 745, 752 (1971) (permitting use of statements transmitted to undercover agent); Hoffa v. United States, 385 U.S. 293, 302 (1966) (permitting use of statements made to informant); Lopez v. United States, 373 U.S. 427, 438–39 (1963) (permitting use of statements recorded by undercover agent).

information merely because that information happens to be conveyed to her phone provider's switching equipment according to the technologies of 2017.[47]

However, *Miller* itself involved bank records—holding a customer retains no reasonable expectation of privacy therein[48]—and a few years later, in *Smith v. Maryland*,[49] the Court held the same for the telephone numbers which we dial in order to place calls.[50] Taken together with the Court's Fourth Amendment protection for the *content* of such telephone calls,[51] the Court seemed to establish what my scholarship has termed a "limited" third party doctrine.[52] Under this limited doctrine, there is no Fourth Amendment protection for information the government obtains from a third party when—but only when—the information was originally provided for that party's use.

Still, it is hard to know how that 1970s-era limited third party doctrine should apply to twenty-first century technologies. This question is inherently difficult. For one, the doctrine has always been contrary to prevailing theories of information privacy.[53] Moreover, the Court has not applied the doctrine in decades, seeming to purposely avoid at least its robust application.[54] Thus, not a single current Justice participated in the last third party doctrine case.[55] At the very least, then, one should

---

[47] *See In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 317–18 (3d Cir. 2010) (questioning whether mobile phone users 'voluntarily' convey CSLI information).

[48] 425 U.S. at 440.

[49] 442 U.S. 735 (1979).

[50] *Id.* at 743–44.

[51] 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, 51 (1967) (same).

[52] *See* Stephen E. Henderson, *A Rose by Any Other Name: Regulating Law Enforcement Bulk Metadata Collection*, 94 TEX. L. REV. *SEE ALSO* 28, 32–36 (2016) [hereinafter Henderson, *Cell Tower Dumps*] (explaining my theory and applying it to cell tower dumps).

[53] *See* Stephen E. Henderson, *Fourth Amendment Time Machines (And What They Might Say About Police Body Cameras)*, 18 U. PA. J. CONST. L. 933, 954–60 (2016) [hereinafter Henderson, *Fourth Amendment Time Machines*] (explaining information privacy); Stephen E. Henderson, *Expectations of Privacy in Social Media*, 31 MISS. C. L. REV. 227, 229–33 (2012) (same); *see also* Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting) ("Privacy is not a discrete commodity, possessed absolutely or not at all.").

[54] *See* Stephen E. Henderson, *After* United States v. Jones*, After the Fourth Amendment Third Party Doctrine*, 14 N.C. J.L. & TECH. 431, 438–42 (2013) (describing five such cases).

[55] Justice Anthony Kennedy joined the Court in 1988, but not in time to participate in the somewhat relevant case of *California v. Greenwood*, 486 U.S. 35 (1988). He did participate in the public disclosure case of *Florida v. Riley*, 488 U.S. 445 (1989), but that doctrine is importantly different from—or at least an edge case of—the limited third party doctrine potentially at issue in *Carpenter*. *See* Marc Jonathan Blitz, James Grimsley, Stephen E. Henderson & Joseph Thai, *Regulating Drones Under the First and Fourth Amendments*, 57 WM. & MARY L. REV. 49, 65–72, 77–80 (2015) [hereinafter Blitz et al.] (describing both the public disclosure doctrine and the limited third party doctrine).

question the Sixth Circuit's facile equivalence between the telephone numbers we dial in order to place calls and our physical location as we carry a mobile phone.[56] Equally unilluminating is the Sixth Circuit's attempt to differentiate 'content' from 'non-content,'[57] which I and others have explained works only for particular technologies and not as a general rule.[58] An attempted content/non-content distinction simply cannot logically provide the constitutional protection/no-protection trigger.

Moreover, in a different context, the Supreme Court has—consistent with theories of information privacy—derided a third-party principle as a "cramped notion of personal privacy"[59]:

> To begin with, both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person. In an organized society, there are few facts that are not at one time or another divulged to another. Thus the extent of the protection accorded a privacy right at common law rested in part on the degree of dissemination of the allegedly private fact and the extent to which the passage of time rendered it private. According to Webster's initial definition, information may be classified as "private" if it is "intended for or restricted to the use of a particular person or group or class of persons: not freely available to the public."[60]

More recently, in *Riley v. California*,[61] the Court did not question constitutional protection for digital contents also held by a third party[62] and ridiculed the notion that

---

[56] *See* United States v. Carpenter, 819 F.3d 880, 886 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (June 5, 2017) (No. 16-402) (falsely claiming that the federal courts "have long recognized a core distinction" relating to "*that kind* of information" (emphasis added)).

[57] *See id.* at 887.

[58] *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, 1020–24 (2007) (arguing that a content/non-content distinction relies upon—and only functions for—the particular architecture of traditional telephony); *see also* United States v. Davis, 785 F.3d 498, 537 (11th Cir. 2015) (Martin, J., dissenting) (arguing against a content/non-content distinction); Steven M. Bellovin et al., *It's Too Complicated: How the Internet Upends* Katz*,* Smith*, and Electronic Surveillance Law*, 30 HARV. J.L. & TECH. 1 (2016) (same).

[59] U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 763 (1989).

[60] *Id.* at 763–64 (quoting *Private*, WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 1804 (1976)).

[61] 134 S. Ct. 2473 (2014).

[62] *Id.* at 2490–91. The Court explained as follows:

> Although the data stored on a cell phone is distinguished from physical records by quantity alone, certain types of data are also qualitatively different. An Internet search and browsing history, for example, can be

contemporary technologies necessarily map onto analog-era precedents.[63] And, of course, Justice Sonia Sotomayor has specifically called the third party doctrine into doubt.[64]

> found on an Internet-enabled phone and could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD. Data on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building.

Id. at 2490. To be clear, this is not a direct repudiation of a limited third party doctrine, because in *Riley* the police would not be obtaining this information *from the third party*, but rather from the defendant's own device. Nobody should claim that merely because police could without justification obtain phone numbers dialed from a phone company, police are therefore free as a matter of Fourth Amendment law to break into the defendant's home to obtain the same. My limited point is that the *Riley* Court understood such information to remain private despite being shared, just as the Court expressed in *Reporters Committee*.

The *Riley* Court continued:

> To further complicate the scope of the privacy interests at stake, the data a user views on many modern cell phones may not in fact be stored on the device itself. Treating a cell phone as a container whose contents may be searched incident to an arrest is a bit strained as an initial matter. But the analogy crumbles entirely when a cell phone is used to access data located elsewhere, at the tap of a screen. That is what cell phones, with increasing frequency, are designed to do by taking advantage of "cloud computing." Cloud computing is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself. Cell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference.

Id. at 2491 (internal citation omitted). It is certainly worthy of note that it makes "little difference" whether information is held by a third party. *See generally* David A. Harris, Riley v. California *and the Beginning of the End for the Third-Party Search Doctrine*, 18 U. PA. J. CONST. L. 895 (2016).

[63] *Riley*, 134 S. Ct. at 2488–89. The *Riley* Court stated as follows:

> The United States asserts that a search of all data stored on a cell phone is "materially indistinguishable" from searches of these sorts of physical items. That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together. Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse. A conclusion that inspecting the contents of an arrestee's pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but any extension of that reasoning to digital data has to rest on its own bottom.

Id. (citation omitted).

[64] United States v. Jones, 565 U.S. 400, 417–18 (2012) (Sotomayor, J., concurring).

So, there are ample grounds for questioning both the wisdom and the logic of applying the Court's limited third party doctrine to CSLI, and, as described below, I believe it would be a substantial mistake for the Court to do so.[65] At the very least, these complications call for a measure of humility in attempting to discern the existing rule, as well as for caution in applying that rule to technologies and social norms that were unheard of when the Court last applied it. Nonetheless, one might defend the Sixth Circuit's ultimate holding under the Supreme Court's strict view of weakened precedent.[66] But now that the issue has reached the high court, any such exceeding deference will no longer be controlling.

2. The Data Precision

As demonstrated above, the CSLI at issue in *Carpenter* did not pinpoint a precise location; instead, it sometimes placed Carpenter within a relatively large geographic area.[67] This was very important to the Sixth Circuit majority, which differentiated law enforcement access to such information from what agents learned via GPS tracking of a vehicle in *United States v. Jones*.[68]

To the extent we are trying to understand the impact of law enforcement access upon privacy—as the Supreme Court has generally directed[69]—it seems unassailable

---

Justice Sotomayor said this:

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

Id. (internal citations omitted).

[65] *See infra* Parts II–III.

[66] *See* Rodriguez de Quijas v. Shearson/Am. Express, Inc., 490 U.S. 477, 484 (1989) ("If a precedent of this Court has direct application in a case, yet appears to rest on reasons rejected in some other line of decisions, the Court of Appeals should follow the case which directly controls, leaving to this Court the prerogative of overruling its own decisions."); United States v. Carpenter, 819 F.3d 880, 888 (6th Cir. 2016) ("On this point, *Smith* is binding precedent."). For a critique of this rule, see generally C. Steven Bradford, *Following Dead Precedent: The Supreme Court's Ill-Advised Rejection of Anticipatory Overruling*, 59 FORDHAM L. REV. 39 (1990). More importantly, one can dispute whether *Smith* has "direct application" to after-arising technologies.

[67] *See supra* Section I.B.

[68] *See Jones*, 565 U.S. at 403; *Carpenter*, 819 F.3d at 889. *Jones* will be discussed more below, including in Part III.

[69] *See* Riley v. California, 134 S. Ct. 2473, 2484 (2014) ("[W]e generally determine whether to exempt a given type of search from the warrant requirement 'by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the

that precision is a relevant criterion. However, as persuasively argued by Judge Jane Stranch in her concurrence in the Sixth Circuit judgment, it is not the *only* criterion; surely duration matters as well.[70] In other words, while the duration of a specific information request will ultimately factor into whether a required level of justification has been demonstrated (e.g., police demonstrating a fair probability that *six months* of information contains evidence of crime should not enable access to *six years* of information),[71] the *potential* for large amounts of an information type to be privacy invasive also critically informs the privacy implications of permitting government access to that information type.[72] For example, if even terribly vague location information relating to an entire life is significantly privacy invasive, and therefore liberty invasive, that argues in favor of some constitutional restriction on law enforcement gathering at least certain amounts of vague location information.[73]

For Carpenter, the amount was 127 days.[74] While the particular line-drawing might be difficult and is sure to be contested, Judge Stranch is right to call for "a new test" that accounts for all relevant factors, as opposed to a test relying solely upon one (location precision).[75] I will shortly return to what I believe that new test should be—or at least to what it should *not* be, which might be enough.[76]

3. The Stored Communications Act

In *Carpenter*, law enforcement agents obtained the CSLI using a court order authorized by the Stored Communications Act (SCA).[77] In particular, they were required to offer "specific and articulable facts showing that there [were] reasonable grounds to believe" the information "relevant and material to an ongoing criminal investigation,"[78] a standard often interpreted to equate to reasonable suspicion.[79] As

---

degree to which it is needed for the promotion of legitimate governmental interests.'" (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999))). To be clear, this does presuppose that there *is* a search. *See infra* Part III.

[70] *Carpenter*, 819 F.3d at 894–96 (Stranch, J., concurring in the judgment as to the constitutional issue).

[71] *See* AM. BAR ASS'N, ABA STANDARDS FOR CRIMINAL JUSTICE: LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS Standard 25-5.2 at 100 (3d ed. 2013), https://www.americanbar.org/content/dam/aba/publications/criminal_justice_standards/third_party_access.authcheckdam.pdf [https://perma.cc/M8CA-ZW6T] [hereinafter ABA LEATPR STANDARDS].

[72] *Id.* Standard 25-4.1 at 69.

[73] Law enforcement gathering location data for a lifetime is not merely theoretical. *See* Grady v. North Carolina, 135 S. Ct. 1368, 1369–71 (2015) (holding lifetime GPS tracking to constitute a search).

[74] *Carpenter*, 819 F.3d at 895 (Stranch, J., concurring).

[75] *Id.* at 896.

[76] *See infra* Parts III–IV.

[77] 819 F.3d at 884.

[78] *Id.* (quoting 18 U.S.C. § 2703(d) (2012)).

[79] *See* Henderson, *Cell Tower Dumps*, *supra* note 52, at 38; Pell, *supra* note 18, at 61.

I discuss below, I agree with Justice Samuel Alito and others who have expressed the importance of legislative determinations in the Fourth Amendment calculus.[80] In this instance, however, the Sixth Circuit majority was wrong to think Congress had meaningfully spoken to the question at hand.

According to the Sixth Circuit, "Congress has specifically legislated on the question before us today . . . . The defendants . . . effectively ask us to declare that [Congressional] balance unconstitutional."[81] In the most literal of senses, this is true. The SCA does generically speak of law enforcement accessing "a record or other information pertaining to a subscriber to or customer of [a] service" that does "not includ[e] the contents of communications."[82] And CSLI is information pertaining to a customer that does not seem to constitute the "contents of a wire or electronic communication" as that phrase is used in the Act.[83] But far from legislating about location surveillance, the SCA was passed in 1986 to address then-novel "computer and telecommunications technologies" that had nothing to do with mobile telephony.[84] As pointed out by Carpenter, when the SCA was enacted, "cell phones cost over $3,000, were the size of a large brick, could connect to only fragmentary cellular networks, and were used by very few people."[85] Today, by contrast, 95% of Americans own a mobile phone.[86]

Thus, while the Sixth Circuit majority considered Carpenter's argument ironic in light of the congressionally enacted SCA—how could he argue for a *reasonable* expectation of privacy when Congress had (allegedly) spoken otherwise?[87]—a better irony would seem to be the court's simultaneously defending a prior circuit precedent that declared a portion of the same Act unconstitutional![88] In *United States v. Warshak*,[89] a Sixth Circuit panel struck down the SCA's provisions permitting warrantless access to emails,[90] a situation more analogous than the *Carpenter* majority—too fixated on 'content' versus 'non-content'—could appreciate.

---

[80] *See infra* Part IV.

[81] *Carpenter*, 819 F.3d at 889.

[82] 18 U.S.C. § 2703(c)(1).

[83] *Id.* § 2703(a)–(b).

[84] S. REP. NO. 99-541, at 1 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3555; *see also* Henderson, *Cell Tower Dumps*, *supra* note 52, at 36–38 (examining SCA application to cell tower dumps). For a different argument—that there is actually no tension with the SCA because the Act separately provides for access with a warrant—see *Carpenter*, 819 F.3d at 897 (Stranch, J., concurring).

[85] Reply Brief in Opposition at 1, *Carpenter*, 819 F.3d 880, *cert. granted*, 137 S. Ct. 2211 (June 5, 2017) (No. 16-402).

[86] *Mobile Fact Sheet*, PEW RES. CTR. (Jan. 12, 2017), http://www.pewinternet.org/fact-sheet/mobile/ [https://perma.cc/RXE4-LF6H].

[87] *Carpenter*, 819 F.3d at 889–90 ("Here, one might say that society itself—in the form of its elected representatives in Congress—has already struck a balance that it thinks reasonable.").

[88] *See id.* at 887 (discussing United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010)).

[89] 631 F.3d 266 (6th Cir. 2010).

[90] *Id.* at 288.

Courts should be extremely cautious of over-relying on legislative determinations when an after-arising technology is at issue. It is one thing to decide that the plain language of a statute continues to control even changed circumstances, at least absent absurd consequences.[91] It is quite another to infer a legislative purpose from that language that never could have been (because the technology at issue did not yet exist in meaningful form), and then apply that mythical purpose to interpret the foundational rights of our Constitution.[92]

II. WHAT IS AT STAKE?

In order to appreciate the significance of *Carpenter*, it helps to identify the law enforcement and private interests in location surveillance. For law enforcement, there are at least two. One, as in *Carpenter* itself, the government has an interest in solving past crime.[93] This would seem to require, for the most part, historic location information: by showing that Carpenter and his brother were near the crimes during their commission, the government proves they might be the perpetrators.[94] However, this requires that such historic data exist. Therefore, in order to solve past crime, the government has an interest in someone conducting prospective tracking and retaining that data.

Two, the government has an interest in preventing future crime,[95] which itself has at least two variants. First, if persons know they are subject to surveillance, they might decide not to commit crime—a generalized deterrence.[96] This is not, as the

---

[91] *See* Green v. Bock Laundry Mach. Co., 490 U.S. 504, 527–30 (1989) (Scalia, J., concurring) (arguing textualism allows avoidance of absurd results).

[92] This is not to say that one cannot smartly attempt to translate the concerns of one time into the facts of another. *See, e.g.*, George C. Thomas III, *Time Travel, Hovercrafts, and the Framers: James Madison Sees the Future and Rewrites the Fourth Amendment*, 80 NOTRE DAME L. REV. 1451, 1463 (2005) ("I seek . . . to offer the piece of the puzzle that is missing in our Fourth Amendment universe: how would the Framers have written the Fourth Amendment if they could have foreseen modern police methods?"). It is merely to urge that such an enterprise requires real intellectual work, not facile claims of equivalence.

[93] *See* United States v. Hensley, 469 U.S. 221, 229 (1985).

[94] *See* United States v. Carpenter, 819 F.3d 880, 884 (6th Cir. 2016).

[95] *See Hensley*, 469 U.S. at 228.

[96] Even a mere reminder of the potential for being watched can modify behavior. *See* Melissa Bateson et al., *Cues of Being Watched Enhance Cooperation in a Real-World Setting*, 2 BIOLOGY LETTERS 412, 412–13 (2006), http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1686213/ [https://web.archive.org/web/20170524214648/http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1686213/] (finding that people contributed nearly three times as much for drinks when an image of human eyes was displayed nearby); Terence C. Burnham & Brian Hare, *Engineering Human Cooperation: Does Involuntary Neural Activation Increase Public Goods Contributions?*, 18 HUM. NATURE 88, 99 (2007) (finding an increase in simulated public good behavior when an image of a robot with human eyes was displayed); Max Ernest-Jones et al., *Effects of Eye Images on Everyday Cooperative Behavior: A Field Experiment*, 32 EVOLUTION

Court has confusingly intimated, a special need that should get any sort of Fourth Amendment pass.[97] But it is a legitimate government concern, albeit one that, if unchecked, would lead to an Orwellian state.[98] Second, real-time surveillance might permit government pre-crime intervention. If a sex offender enters a banned playground, a domestic abuser enters a former victim's neighborhood, or a neighborhood experiences a 'suspicious' volume of activity, and that activity triggers a real-time alert, perhaps officers can intervene before another crime can take place.

Thus, the government has a legitimate interest in both historic and prospective location surveillance of *all of us*.[99] This is not to say, of course, that certain types of location information about certain persons would not be more valuable than others; that is surely true, as when the government seeks a known fugitive.[100] But those differences are matters of degree not always easily assessed and, most importantly, they are variable. In other words, it is not that government will desire only historic information, or only prospective information (whether conveyed in real time or in chunks), or only information of a certain granularity (precision). At least some of the time, the government will want it all—type A in this instance and type B in that—and,

---

& HUM. BEHAV. 172, 176 (2011) (finding that people littered half as often when an image of human eyes was displayed nearby); *see also* MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON 195–228 (Alan Sheridan trans., 1977) (recognizing the internal significance of feeling watched).

[97] *See* City of Los Angeles v. Patel, 135 S. Ct. 2443, 2452 (2015) ("Here, we assume that the searches authorized by [the hotel registry ordinance] serve a 'special need' other than conducting criminal investigations: They ensure compliance with the recordkeeping requirement, which in turn deters criminals from operating on the hotels' premises."). This odd claim has had perverse consequences in other litigation. *See* Belleau v. Wall, 811 F.3d 929, 939–40 (7th Cir. 2016) (Flaum, J., concurring in the judgment) (considering lifetime GPS monitoring of a sex offender to constitute a special need because it was not intended to solve a *particular* crime). Databasing information in order to discourage new crime can, of course, be distinguished from punishing discovered crime to discourage new crime. But *neither* should be considered a special need. Otherwise, police could randomly enter homes and claim the 'special need' of deterring crimes that might otherwise be committed therein—that too would discourage crime, as would the hated general warrants of our founding era.

[98] It is, after all, in the second paragraph of *Nineteen Eighty-Four* that the reader is introduced to the posters of Big Brother:

> At one end of [the hallway] a colored poster, too large for indoor display, had been tacked to the wall. It depicted simply an enormous face, more than a meter wide: the face of a man of about forty-five, with a heavy black mustache and ruggedly handsome features. . . . On each landing, opposite the lift shaft, the poster with the enormous face gazed from the wall. It was one of those pictures which are so contrived that the eyes follow you about when you move. BIG BROTHER IS WATCHING YOU, the caption beneath it ran.

GEORGE ORWELL, NINETEEN EIGHTY-FOUR 3 (1949).

[99] *See* Henderson, *Fourth Amendment Time Machines*, *supra* note 53, at 942–43.

[100] *See, e.g.*, United States v. Wallace, 866 F.3d 605, 606–07 (5th Cir. 2017) (describing use of a mobile phone 'ping' order to locate a fugitive).

therefore, its actors will logically seek out what exists, as well as attempt to ensure that such information will exist. This is, conceptually, why the National Security Agency was creating a telephone metadata 'time machine,'[101] and the utility of a location surveillance time machine follows from the same logic. In the words of CIA CTO Ira "Gus" Hunt,

> [T]he value of any piece of information is only known when you can connect it with something else which arrives at a future point in time. And if you throw away, in our world, information because you didn't think it had any value, or you chose not to bring in or collect information because [it] didn't match what you thought your needs were at that moment in time, you won't have information to connect together as new information and new events emerge in the world. . . . [W]e fundamentally try to collect everything and hang onto it forever.[102]

In other words, in the absence of acquisition and storage costs, and in the absence of liberty concerns and associated economic costs, a government should ensure—via some means—ubiquitous location information. Thus, where technologies and related social norms eliminate, or even seriously lessen, the acquisition and storage costs, the only logical restraint on government location tracking is concern for liberty. This should remain a most significant constraint, because such liberty concerns are fundamental.[103] They should be of constitutional magnitude, and the most logical place to situate them is within the Fourth Amendment, as well as in the First, which protects the freedoms of speech and association.[104] Thus—and this seems amply supported by the opinions in *United States v. Jones*[105]—there should be some Fourth Amendment limitation on location surveillance.

The next question is whether that constitutional limitation should apply to only certain *manners* of government acquisition. In part, it should. As I have written

---

[101] *See* Henderson, *Fourth Amendment Time Machines*, *supra* note 53, at 940–43 (describing the NSA telephony metadata program as a logical, albeit unlawful, "Fourth Amendment time machine").

[102] Ira "Gus" Hunt, CIA Chief Technology Officer, Address at Gigaom Structure Data Event (Mar. 20, 2013), https://www.youtube.com/watch?v=GUPd2uMiXXg (at 20:34).

[103] *See* Henderson, *Fourth Amendment Time Machines*, *supra* note 53, at 954–60 (gathering sources explaining the consequences of lacking information privacy). *See generally* Alex Kozinski & Mihailis E. Diamantis, *An Eerie Feeling of Déjà Vu: From Soviet Snitches to Angry Birds*, *in* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW 420 (David Gray & Stephen E. Henderson eds., 2017).

[104] The First Amendment provides as follows: "Congress shall make no law . . . abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." U.S. CONST. amend. I.

[105] 565 U.S. 400 (2012).

elsewhere, "It would be devastating to legitimate law enforcement, and even downright silly, if a police officer had to get a court order before looking at a person and thereby determining his or her location."[106] But I cannot discern why the constitutional restriction would apply only to location directly measured by law enforcement, as opposed to location measured in the first instance by a third party. If the government has legitimate reason to acquire such information—which we have established it does—and if the cost of acquisition is eliminated—which we are certainly trending towards—then why would any government care which manner of acquisition is used? In other words, if manners A, B, and C are available and each costless, I would think agents would and should arbitrarily choose among them. If manner A is legally restricted, and manner B is fiscally expensive, but manner C is neither, I would think agents would and should overwhelmingly choose manner C. Naturally, then, any system of meaningful regulation must include manner C.

Perhaps manner A—a legally restricted acquisition—consists of the government forcibly collaring an individual with a device that will report real-time location information. Remarkably, some states have required certain individuals to wear such a device *for the rest of their lives* without requiring any individualized determination of government need nor restricting what can be done with the gathered information.[107] Thankfully, the Supreme Court has recognized this to constitute a Fourth Amendment search,[108] and therefore lower courts are considering reasonableness, albeit too often in a dismissive manner.[109] What is important for our purposes is that,

---

[106] Henderson, *Location Surveillance After* Jones, *supra* note 8, at 832 (thus suggesting no legal restraint on less than twenty-four hours of such surveillance); *see also* Blitz et al., *supra* note 55, at 68–72, 74–77 (defending a Fourth Amendment public disclosure doctrine).

[107] *See, e.g.*, Belleau v. Wall, 811 F.3d 929, 931, 935 (7th Cir. 2016).

[108] *See* Grady v. North Carolina, 135 S. Ct. 1368, 1370 (2015).

[109] *See, e.g.*, *Belleau*, 811 F.3d at 934–35 ("The focus must moreover be on the *incremental* effect of the challenged statute on the plaintiff's privacy, and that effect is slight given the decision by Wisconsin—which he does not challenge—to make sex offenders' criminal records and home addresses public."). This is a remarkable claim, asserting there is little privacy difference between home address, on the one hand, and location at every point in time, on the other. But Judge Posner did not stop there: "The additional loss from the fact that occasionally his trouser leg hitches up and reveals an anklet monitor that may cause someone who spots it to guess that this is a person who has committed a sex crime must be slight." *Id.* at 935. I cannot imagine how the effect of such a scarlet letter would be "slight"—the collaring itself is significantly invasive of human dignity—nor do I think the judge is correct to think one has an interest only in wearing "trouser[s]," as opposed to shorts or a bathing suit or, at times, nothing at all. Posner continued with this odd claim: "It's untrue that the GPS device burdens liberty by its continuous surveillance of the offender's activities; it just identifies locations; it doesn't reveal what the wearer of the device is doing at any of the locations." *Id.* at 936 (internal citation and quotation marks omitted).

Posner closed his opinion with this coup de grâce:

> To return to our traffic analogy briefly: no one thinks that a posted speed limit is a form of punishment. It is a punishment trigger if the

in this instance, law enforcement itself gathers the location information by way of a bodily contact.

Perhaps manner B—a fiscally expensive acquisition—consists of law enforcement tracking an individual with a high-altitude autonomous drone that employs facial, gait, and other recognition technologies and reports real-time location information.[110] There are differences in scenarios A and B, and they might have Fourth Amendment and due process relevance. For example, the tracking in the first scenario is demeaning and stigmatizing, while perhaps that in the second is not, at least in the same manner or degree. But as for the intrusion into one's person based upon no longer having any location privacy, the two differ not at all.

Manner C—neither legally nor fiscally restricted—might be, according to the Sixth Circuit in *Carpenter*, when a third party initially gathers, but does not disclose or share, this same location information.[111] Indeed, say the third party guarantees such use restrictions, contractually binding itself to using, after the fact, only anonymized, aggregated location data and only in order to improve the quality of its underlying services.[112] The tracking might occur via a device tethered to or always carried by the person, or via our hypothesized autonomous drone (perhaps the third party offers a security service that intercedes only in the event of an emergency). If another party accesses this location information, either in historic chunks or in real time, then as for the intrusion into the tracked person's security based on lesser location privacy, it seems identical to that of manners A and B. It matters not—or at least not much—that in one instance the data arrives in daily or weekly chunks, while in another it comes by-the-minute. Nor does it matter whose device is recording and how. What matters is that the person will respond to no longer having any location privacy, chilling her expressive and associational autonomy.

> police catch you violating the speed limit, but police are not required to obtain a warrant before stopping a speeding car. The anklet monitor law is the same: it tells the plaintiff—if you commit another sex offense, you'll be caught and punished, because we know exactly where you are at every minute of every day.

Id. at 938. How anyone could think lifetime GPS monitoring of a particular individual can be meaningfully compared to a speed limit is beyond me. It was also seemingly beyond Posner's colleague, Judge Flaum, who concurred only in the judgment. *See id.* ("The challenge presented by this appeal requires addressing *substantial competing interests*: an individual's right to privacy from government monitoring, on the one hand, and the state's interest in protecting children from sexual abuse, on the other." (emphasis added)).

[110] We will assume, for our purposes, a bit of technology that does not yet exist but soon will, including robust biometric recognition from all angles and inflight recharging in order to permit the continuous monitoring.

[111] 819 F.3d 880, 887–89 (6th Cir. 2016).

[112] This private-party limitation is important. If the information is readily accessed by other persons, then agents of law enforcement need not alone "shield their eyes." California v. Ciraolo, 476 U.S. 207, 213 (1986); *see* Blitz et al., *supra* note 55, at 68–72, 74–77.

In other words, in impact, *Carpenter* is not merely a case about CSLI. If there is no constitutional limit to the historic location information that law enforcement can obtain via third-party records, then there is effectively no constitutional limit to law enforcement location surveillance. This would be a startling development in a world that has developed technologies that not only can routinely track and store location, but that increasingly do.

III. IS IT A SEARCH?

Based upon the argument above, I certainly consider law enforcement access to third-party records containing longer term CSLI to constitute a Fourth Amendment search. It does not follow that law enforcement are prohibited from such access, of course, or even that such access requires a certain justification procedure—that is a second consideration of Fourth Amendment reasonableness. But the access should constitute a search. This can be seen in several ways.

First, according to the commonplace dictionary definition—both at the founding and today—acquiring records and looking through them constitutes a 'search.'[113] Although the Court has adopted such a straightforward interpretation of seizure,[114] it has only flirted with the concept for search,[115] and I do not expect the Court to jettison the reasonable expectation of privacy inquiry. Therefore, while I continue to favor a dictionary definition of search that leaves most all of the work to reasonableness, I will not belabor it here.

Instead, in the absence of a physical intrusion to a protected interest, the Court has established reasonable expectation of privacy as the search trigger.[116] I am confident that as an empirical matter, people expect their longer term CSLI information to be kept confidential, and that as a normative matter, it is essential to a free people that the government not have unfettered access to citizen location, at least unless such information otherwise becomes universally accessible.

The first claim is of course one for which data must be gathered. Fortunately, several studies of increasing sophistication are available, and they demonstrate an expectation of privacy in longer term CSLI.[117] In 2015, an empirical study focusing

---

[113] *See Search*, MERRIAM WEBSTER, https://www.merriam-webster.com/dictionary/search [https://perma.cc/Q7G9-DKPT] (last visited Dec. 4, 2017) ("to look into or over carefully or thoroughly in an effort to find or discover something"). Merriam Webster also includes as a definition "to read thoroughly," as in to "*search* land titles." *Id.*; *see also* Henderson, *Nothing New*, *supra* note 43, at 544–46 (agreeing with Akhil Amar and others that the Court should use a dictionary definition of 'search'); DAVID GRAY, THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE 158–60 (2017) (making a sophisticated argument for the same).

[114] California v. Hodari D., 499 U.S. 621, 624 (1991) (using an 1828 definition of seizure).

[115] *See* Kyllo v. United States, 533 U.S. 27, 32 n.1 (2001) (urging an 1828 definition of search).

[116] *See* United States v. Jones, 565 U.S. 400, 406 (2012); *id.* at 419 (Alito, J., concurring in the judgment).

[117] *See generally* Jeremy A. Blumenthal et al., *The Multiple Dimensions of Privacy: Testing Lay "Expectations of Privacy,"* 11 U. PA. J. CONST. L. 331 (2009) (reporting on an

on the third party doctrine concluded that "individuals have far higher expectations of privacy than courts have recognized and that contrary to the perceptions of the courts, privacy expectations are not founded on whether or not information is kept completely secret."[118] Indeed, the majority of study participants favored a warrant requirement for law enforcement access to CSLI.[119] A more recent study similarly found that third party doctrine scenarios "were treated by our survey respondents as more intrusive than [scenarios] the [Supreme] Court considers the *most* intrusive of privacy."[120] In particular, survey respondents considered access to seven months of CSLI as equally invasive to the search of one's bedroom.[121]

While there are always criticisms to be made of any empirical study, or at least limitations therein, surely this recent work provides a better sense of what Americans expect than the guess of any professor or judge—or of nine judges, as the case may be. As for the impact of the amount of information (e.g., the duration of CSLI), there

---

empirical study into the question of Fourth Amendment search); Bernard Chao et al., *Why Courts Fail to Protect Privacy: Race, Age, Bias, and Technology*, 106 CALIF. L. REV. (forthcoming) (draft available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2924744) (same); Henry F. Fradella et al., *Quantifying* Katz*: Empirically Measuring "Reasonable Expectations of Privacy" in the Fourth Amendment Context*, 38 AM. J. CRIM. L. 289 (2011) (same); Matthew B. Kugler & Lior Jacob Strahilevitz, *Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory*, 2015 SUP. CT. REV. 205 [hereinafter Kugler & Strahilevitz, *Actual Expectations*] (same); Matthew B. Kugler & Lior Jacob Strahilevitz, *The Myth of Fourth Amendment Circularity*, 84 U. CHI. L. REV. (forthcoming) (draft available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2922777) [hereinafter Kugler & Strahilevitz, *The Myth*] (same); Marc McAllister, *The Fourth Amendment and New Technologies: The Misapplication of Analogical Reasoning*, 36 S. ILL. U. L.J. 475 (2012) (same); Christine S. Scott-Hayward et al., *Does Privacy Require Secrecy? Societal Expectations of Privacy in the Digital Age*, 43 AM. J. CRIM. L. 19 (2015) (same); Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317 (2008) (same); Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213 (2002) (reporting on another such study); Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society,"* 42 DUKE L.J. 727 (1993) (reporting on a first-of-its-kind empirical study into the question of Fourth Amendment search); Alisa Smith et al., *An Empirical Examination of Societal Expectations of Privacy in the Digital Age of GPS, Cell Phone Towers, & Drones*, 26 ALB. L.J. SCI. & TECH. 111 (2016) (same). The Pew Research Center also gathers relevant data on Americans' perceptions. *See, e.g.*, Lee Rainie, *The State of Privacy in Post-Snowden America*, PEW RES. CTR. (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/ [https://perma.cc/K5NJ-Z5E7]; Kathryn Zickuhr, *Location-Based Services*, PEW RES. CTR. (Sept. 12, 2013), http://www.pewinternet.org/2013/09/12/location-based-services/ [https://perma.cc/E7NG-FRQS].

[118] Scott-Hayward et al., *supra* note 117, at 22.

[119] *Id.* at 52–53.

[120] Chao et al., *supra* note 117 (manuscript at 5) (emphasis added); *see also id.* (manuscript at 57 tbl.4).

[121] *Id.* (manuscript at 47–48).

is, counter to my intuitions, reason to question whether Americans react to this variable.[122] Nonetheless, because there is reason for the Court to be cautious in expounding Fourth Amendment rights—more on this below—I would not disfavor a holding expressly limited to longer term CSLI acquisition like that at issue in the *Carpenter* case.

As for the normative assertion—that in a relatively free society the government should not have unfettered access to citizen location—firstly, I agree with Justice Harlan that the Fourth Amendment must have a normative backstop.[123] While there might be reasoned argument upon any such normative claim, when it comes to location surveillance, there seems ample support in everything from classic dystopian literature to efforts of historic totalitarian regimes to the Court opinions in *Jones*.[124] And when considering the normative impact of location surveillance, it is important to keep in mind that location is highly predictable, such that in accessing historic data, law enforcement can also see into the future.[125]

While the analysis above—even the loose normative hand-waving—seems more than adequate to me, we have not yet considered the Fourth Amendment text. It protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches."[126] Five Justices have recognized that longer term government location tracking can constitute a search regardless of the lack of any physical intrusion,[127] which textually must then interfere with the constitutionally

---

[122] *See generally* Kugler & Strahilevitz, *Actual Expectations*, *supra* note 117, at 209 (finding that the duration of vehicle GPS tracking did not affect its perceived intrusiveness); Scott-Hayward et al., *supra* note 117, at 53 (same). On the other hand, there is reason to think Americans' privacy expectations are more robust than many have feared or claimed. *See generally* Kugler & Strahilevitz, *The Myth*, *supra* note 117 (finding that the Supreme Court's cell phone search decision in *Riley* had no lasting impact upon relevant privacy expectations).

[123] *See* United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting) ("Since it is the task of the law to form and project, as well as mirror and reflect, we should not, as judges, merely recite the expectations and risks without examining the desirability of saddling them upon society. The critical question, therefore, is whether under our system of government, as reflected in the Constitution, we should impose on our citizens the risks of the [government surveillance] without at least the protection of a warrant requirement.").

[124] *See* GRAY, *supra* note 113, at 1–17 (making some of these connections).

[125] *See* Chaoming Song et al., *Limits of Predictability in Human Mobility*, 327 SCIENCE 1018, 1021 (2010) (finding that location based upon mobile phone data is 93% predictable). Apparently, I am not the only creature of habit. *See also Dr Seldon, I Presume*, ECONOMIST, Feb. 23, 2013, at 76 (discussing this research).

[126] U.S. CONST. amend. IV. For an argument that the Court has too often neglected this text, see GRAY, *supra* note 113, at 134–72.

[127] United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) (quoting Justice Alito's concurrence, saying that "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy"); *id.* at 430 (Alito, J., concurring in the judgment). No Justice argued otherwise; the remaining four merely thought it unnecessary to decide in the case before the Court. *See id.* at 412–13 (majority opinion) ("We may have to grapple with these 'vexing problems' in some future case where a classic trespassory search is not involved and resort must be had to *Katz* analysis; but there is no reason for rushing forward to resolve them here.").

protected security in our *persons*. This seems right. The Court has also held that even short-term location tracking within a home constitutes a search,[128] while equivalent tracking external to the home does not.[129] This, then, must textually depend upon the constitutionally protected security in our *houses*. This too seems right—law enforcement officers physically present on public thoroughfares need not shield their eyes, but our movements within our home are not similarly shared. And the Court has held that government location tracking that physically intrudes upon a vehicle constitutes a search, interfering with the constitutionally protected security in our *effects*.[130]

The final textually protected interest is in our *papers*, and it was an interest dear to the Framers.[131] I submit that our papers are today often held in trust by third parties,[132] as the Court in *Riley* seemed to appreciate.[133] If there is not protection for such third-party papers, then we risk no Fourth Amendment protection for modern communications, including emails,[134] and for modern data storage, including cloud computing. That is a constitutional risk we should not take.

Moreover, even a first-party-only limitation for papers would not doom Fourth Amendment protection.[135] As I argued in the previous Part, government access to such private information has the same—or at least a very similar—effect on the security in our persons as does direct government tracking. And, as just mentioned, five Justices in *Jones* are on record effectively rejecting the notion that the security in our "persons" covers only physical intrusions. And wisely so, lest there be no Fourth Amendment restraint on government drone tracking and other such emerging technologies.[136]

---

[128] United States v. Karo, 468 U.S. 705, 716–18 (1984).

[129] United States v. Knotts, 460 U.S. 276, 285 (1983).

[130] *Jones*, 565 U.S. at 404 ("It is beyond dispute that a vehicle is an 'effect' as that term is used in the [Fourth] Amendment. We hold that the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search.'" (internal citation omitted)).

[131] *See* Donald A. Dripps, *"Dearest Property": Digital Evidence and the History of Private "Papers" as Special Objects of Search and Seizure*, 103 J. CRIM. L. & CRIMINOLOGY 49, 61–83 (2013).

[132] *See generally* Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV. 611 (2015) (arguing that some third parties should be treated as "information fiduciaries" from which any government access should be regulated by the Fourth Amendment).

[133] *See supra* note 62 and accompanying text.

[134] *Cf.* United States v. Warshak, 631 F.3d 266 (6th Cir. 2010) (holding the Fourth Amendment protects email content residing with a third-party provider).

[135] For such an argued limitation, see Orin Kerr, *How Should an Originalist Rule in the Fourth Amendment Cell-Site Case?*, WASH. POST: VOLOKH CONSPIRACY (June 13, 2017), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/06/13/how-should-an-originalist-rule-in-the-fourth-amendment-cell-site-case/?utm_term=.8840006a40a3 [https://perma.cc/MMJ3-7TW3] (arguing that only certain information held by a third party can constitute a customer's *papers*).

[136] For an overview of how the Fourth Amendment *should* apply to drone flight, see Blitz et al., *supra* note 55.

So, however one spins it, law enforcement accessing generally inaccessible third-party documents containing longer term location information and looking through them in order to learn something should constitute a Fourth Amendment search. This will mean that the third party doctrine as a monolithic, sharp rule will be no more. The Court would replace the anachronistic bright-line rule just as it has replaced other Fourth Amendment doctrines that did not stand the test of time.[137] It need not mean that provision of information to third parties is *irrelevant* to the Fourth Amendment analysis. As recognized in the ABA Standards relating to law enforcement access to such information, sharing can impact how *private* is the information and thus what restraint law enforcement access should require in order to be reasonable,[138] the step to which I now turn.

IV. IS IT REASONABLE?

Reasonableness is designedly ambiguous—and therefore subject to court interpretation—allowing the constitutional regulation of search and seizure to withstand centuries of technological and sociological change. Only some searches and seizures require a warrant to satisfy this threshold, including those that required a warrant at the founding.[139]

---

[137] *See* California v. Acevedo, 500 U.S. 565 (1991) (applying automobile exception to all containers in cars, overruling *Arkansas v. Sanders*, 442 U.S. 753 (1979)); Illinois v. Gates, 462 U.S. 213 (1983) (eliminating separate elements of veracity and basis of knowledge in probable cause, overruling *Aguilar v. Texas*, 378 U.S. 108 (1964) and *Spinelli v. United States*, 393 U.S. 410 (1969)); United States v. Ross, 456 U.S. 798 (1982) (embracing automobile exception for containers in cars, overruling *Robbins v. California*, 453 U.S. 420 (1981)); United States v. Salvucci, 448 U.S. 83 (1980) (eliminating automatic standing, overruling *Jones v. United States*, 362 U.S. 257 (1960)); Chimel v. California, 395 U.S. 752 (1969) (eliminating whole-home search incident to arrest, overruling *Harris v. United States*, 331 U.S. 145 (1947) and *United States v. Rabinowitz*, 339 U.S. 56 (1950)); Camara v. Mun. Court of City & Cty. of S.F., 387 U.S. 523 (1967) (applying Fourth Amendment to noncriminal searches but diluting probable cause for administrative searches, overruling *Frank v. Maryland*, 359 U.S. 360 (1959)); Katz v. United States, 389 U.S. 347 (1967) (protecting telephones against non-trespassory interception, overruling, *inter alia*, *Olmstead v. United States*, 277 U.S. 438 (1928)); Warden, Md. Penitentiary v. Hayden, 387 U.S. 294 (1967) (permitting seizure of mere evidence, overruling *Gouled v. United States*, 255 U.S. 298 (1921)); Mapp v. Ohio, 367 U.S. 643 (1961) (applying exclusionary rule against the states, overruling *Wolf v. Colorado*, 338 U.S. 25 (1949)); Elkins v. United States, 364 U.S. 206 (1960) (rejecting then-relevant "silver platter doctrine," overruling *Lustig v. United States*, 338 U.S. 74 (1949)). There are also several relatively recent cases in which the Court claimed no overruling but in which many see one. *See* Los Angeles v. Patel, 135 S. Ct. 2443 (2015) (permitting Fourth Amendment facial challenges despite *Sibron v. New York*, 392 U.S. 40 (1968)); Arizona v. Gant, 556 U.S. 332 (2009) (limiting automobile searches incident to lawful arrest despite *New York v. Belton*, 453 U.S. 454 (1981)); Virginia v. Moore, 553 U.S. 164 (2008) (permitting arrest on probable cause of non-arrestable offense despite *United States v. Di Re*, 332 U.S. 581 (1948)).

[138] ABA LEATPR STANDARDS, *supra* note 71, Standard 25-4.1(a) at 57–59.

[139] Riley v. California, 134 S. Ct. 2473, 2482–84 (2014).

The Founders had private papers, and their security as against the government was their utmost concern.[140] But those papers did not typically reside with third parties. Nor were there telephones that allowed instantaneous private communication at a distance, let alone phones—not to mention powerful computers—that are ubiquitously carried and can be used at most all times, but which thereby incidentally track and log location. Lacking such "precise guidance from the founding era," the Court "generally determine[s] whether to exempt a given type of search from the warrant requirement by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests."[141]

The *Carpenter* facts themselves demonstrate the legitimate governmental interest in cell site location, as do the many other cases in which such evidence is used. Several years ago, a public defender commented that, "In every major case in Los Angeles, they use cell-tower information, . . . It's like fingerprints, it's that common."[142] It is unlikely that investigatory use has decreased since then, although hopefully there has been an increased attention to scientific accuracy.[143] As for the corresponding intrusion into privacy by acquiring large amounts of location information, the Supreme Court recognized its significance in *Jones* and *Riley*, albeit for the more precise GPS.[144]

As for balancing these interests, the Court has acknowledged that achieving the appropriate constitutional balance is especially difficult when technologies are advancing as quickly as they are today.[145] Thus, four justices have urged that "the best solution to privacy concerns may be legislative"—citing the work of Orin Kerr—because "[a] legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."[146] Indeed, Justice Alito more recently suggested that he would change a previous

---

[140] *See* Entick v. Carrington (1765) 95 Eng. Rep. 807, 807, 817–18 (K.B.) (permitting officers to "read over, pry[ ] into, and examine[ ] all the private papers . . . of the plaintiff" "would destroy all the comforts of society; for papers are often the dearest property a man can have."); *see also* United States v. Jones, 565 U.S. 400, 405 (2012) ("*Entick v. Carrington* is a case we have described as a monument of English freedom undoubtedly familiar to every American statesman at the time the Constitution was adopted, and considered to be the true and ultimate expression of constitutional law with regard to search and seizure." (internal citation and quotation marks omitted)); Dripps, *supra* note 131, at 61–83 (artfully describing this legal landscape).

[141] *Riley*, 134 S. Ct. at 2484 (internal quotation marks omitted).

[142] Jackman, *Experts Say*, *supra* note 19 (statement of Jennifer Friedman, Chief of Forensics for the Los Angeles County Public Defender).

[143] *See id.*

[144] *See Riley*, 134 S. Ct. at 2490; *Jones*, 565 U.S. at 415–16 (Sotomayor, J., concurring); *id.* at 430 (Alito, J., concurring in the judgment).

[145] City of Ontario v. Quon, 560 U.S. 746, 759–60 (2010).

[146] *Jones*, 565 U.S. at 429–30 (Alito, J., concurring in the judgment) (citing Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 805–06 (2004)); *see also* Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1515 (2010) ("In an ideal world, government information gathering would be regulated by a comprehensive statutory regime. Courts would analyze

holding if a different, after-enacted and comprehensive legislative solution appeared reasonable.[147] I too have argued that "[w]e require 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."[148] And I have attempted to articulate at least portions of what could become a statutory solution.[149]

So, both state legislatures and Congress should step up to the plate and comprehensively regulate not only law enforcement access to location information, but also to other types of information. In doing so, they can look to thoughtful guides established by the American Bar Association and others.[150] Until legislatures fulfill that responsibility, however, "[t]he best that [courts] can do . . . is to apply existing Fourth Amendment doctrine" to decide the cases before them.[151] This is a role courts cannot abdicate. And as Kiel Brennan-Marquez and I have argued, the Supreme Court's recent opinion in *Birchfield v. North Dakota*[152] "can be read as a re-affirmation of a fundamental principle: when privacy and liberty norms are in flux, as they are given recent and rapid technological change, police *should* seek the assistance of legislatures in governing investigatory methods, and they *must* seek the approval of courts."[153] I certainly believe that law enforcement should be required to seek judicial approval before accessing longer term CSLI.[154]

---

whether the rules in this statutory regime met basic Fourth Amendment principles rather than craft the rules themselves. A pronouncement as short and vague as the Fourth Amendment best serves as a guidepost to evaluate rules, rather than as a source of those rules.").

[147] *See Riley*, 134 S. Ct. at 2497 (Alito, J., concurring in the judgment) ("While I agree with the holding of the Court, I would reconsider the question presented here if either Congress or state legislatures, after assessing the legitimate needs of law enforcement and the privacy interests of cell phone owners, enact legislation that draws reasonable distinctions based on categories of information or perhaps other variables.").

[148] Henderson, *Location Surveillance After* Jones, *supra* note 8, at 808.

[149] *See id.* at 815–21, 823–25, 826–35; Henderson, *Cell Tower Dumps*, *supra* note 52, at 47–57. *See also generally* Christopher Slobogin, *Making the Most of* United States v. Jones *in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST. L. & PUB. POL'Y 1 (2012) (articulating another such solution).

[150] *See* ABA LEATPR STANDARDS, *supra* note 71.

[151] *Jones*, 565 U.S. at 430 (Alito, J., concurring in the judgment); *see also* Solove, *supra* note 146, at 1515.

[152] 136 S. Ct. 2160, 2166–67, 2168–69, 2186–87 (2016) (permitting a breathalyzer as a routine incident of a DUI arrest but not a blood draw).

[153] Kiel Brennan-Marquez & Stephen E. Henderson, *Fourth Amendment Anxiety*, AM. CRIM. L. REV. (forthcoming) (draft available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2955077) (internal citation omitted).

[154] *See* Johnson v. United States, 333 U.S. 10, 13–14 (1948) ("The point of the Fourth Amendment, which often is not grasped by zealous officers, is not that it denies law enforcement the support of the usual inferences which reasonable men draw from evidence. Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime.").

A court need not, however, reach out to decide more than is before it, and while Supreme Court guidance to police is important, providing untimely guidance can have significant negative consequences. As the Court, per curiam, recently noted, "[t]his Court, after all, is one of review, not of first view."[155] Justice Neil Gorsuch cautioned the same in his first concurrence, counseling that "[t]his Court often speaks most wisely when it speaks last."[156] Had the Court not embraced unnecessarily expansive dicta in *Miller*,[157] perhaps lower courts and legislatures might have done more over the years to thoughtfully regulate law enforcement access to varying types of third-party information. By the same token, such organic development is unlikely to occur when courts entirely avoid merits decisions by invoking reasonable reliance, thereby speaking only to the suppression remedy and not to the underlying Fourth Amendment right.[158] There is a world of difference between incremental development and stagnation, and, in the case of CSLI, Congress in particular has recognized this issue for the better part of a decade but has done nothing in response.[159]

So, what to do in *Carpenter*, in which agents obtained 127 days of cell site location information?[160] The Court could hold such access requires a warrant or a lesser court order, the Court could remand the issue for the Sixth Circuit to consider in the first instance, or the Court could hold—even assuming a Fourth Amendment violation—there was reasonable reliance on a facially valid statute and thus the evidence should not be suppressed.[161]

---

[155] Hernandez v. Mesa, 137 S. Ct. 2003, 2007 (2017) (quoting Expressions Hair Design v. Schneiderman, 137 S. Ct. 1144, 1151 (2017)) (internal quotation marks omitted).

[156] Maslenjak v. United States, 137 S. Ct. 1918, 1932 (2017) (Gorsuch, J., concurring in the judgment). Justice Gorsuch continued as follows:

> Respectfully, it seems to me at least reasonably possible that the crucible of adversarial testing on which we usually depend, along with the experience of our thoughtful colleagues on the district and circuit benches, could yield insights (or reveal pitfalls) we cannot muster guided only by our own lights. So while I agree with the Court that the parties will need guidance about the details of the statute's causation requirement, I have no doubt that the Court of Appeals, with aid of briefing from the parties, can supply that on remand. Other circuits may improve that guidance over time too. And eventually we can bless the best of it.

Id. at 1931–32 (internal citation omitted).

[157] *See supra* Section I.C.1.

[158] *See* Davis v. United States, 564 U.S. 229, 245–49 (2011) (discussing but dismissing concerns of Fourth Amendment ossification via reasonable reliance upon court precedent); *see, e.g.*, United States v. Carpenter, 819 F.3d 880, 894 (6th Cir. 2016) (Stranch, J., concurring in the judgment on Fourth Amendment issue); Brief for the United States in Opposition at 10, 29–31, *Carpenter*, 819 F.3d 880, *cert. granted*, 137 S. Ct. 2211 (June 5, 2017) (No. 16-402).

[159] *See Location Based Technologies Hearing*, *supra* note 16 (taking place in 2010).

[160] 819 F.3d at 886.

[161] *See* Illinois v. Krull, 480 U.S. 340, 342 (1987) (establishing an "exception to the exclusionary rule . . . when officers act in objectively reasonable reliance upon a *statute* . . . ultimately

I would personally be comfortable with a warrant requirement vaguely applying to 'longer term' CSLI acquisition, recognizing that 127 days is longer term. Anything more precise—establishing a particular duration threshold—seems premature and inconsistent with the Court's recent more cautious approach. While sometimes it makes sense for the Court to articulate at least approximate hour or day thresholds in interpreting the federal Constitution, it would seem better to avoid them when possible, at least in the first instance.

For example, in *County of Riverside v. McLaughlin*,[162] the Court held that judicial determination of probable cause within forty-eight hours is expected in order to constitute the 'prompt' review required for an arrestee remaining in custody.[163] But not only did that remain a somewhat fluid trigger,[164] most importantly, the holding came sixteen years after the Court first required 'prompt' judicial determination, and only then because there remained significant lower court confusion.[165] When specific durations are declared spontaneously, like *Maryland v. Shatzer*'s fourteen-day rule in the context of invocation of *Miranda* rights in custody,[166] they are less likely to be carefully considered and correspondingly less likely to be well received.[167]

So, again, the Court would be well within its better norms to declare a warrant requirement for 'longer term' CSLI acquisition that includes—but is not defined by—a period of 127 days. But is it clear that a reasonable-suspicion court order could not *reasonably* obtain that information, especially if that access restraint were accompanied by restrictions upon information use?[168] If that too is reasonable, the Court could instead require what is often interpreted to be necessary under the Stored Communications Act. To be clear, this would not be a deferential finding since, as discussed above, that Act was not written with this information in mind.[169] It would be an independent decision that such a court order adequately balances the governmental investigatory needs with citizens' liberty and privacy interests.

---

found to violate the Fourth Amendment").

[162] 500 U.S. 44 (1991).

[163] *Id.* at 56.

[164] *Id.* at 56–57 (acknowledging the varied circumstances of criminal investigation and therefore recognizing both that a delay of less than forty-eight hours could be too long and that a delay of more than forty-eight hours could, in extraordinary circumstances, be constitutionally acceptable).

[165] *See id.* at 55–56 (explaining lingering confusion); Gerstein v. Pugh, 420 U.S. 103, 124–25 (1975) (requiring "prompt" determination). In *Gerstein*, Justice Stewart wrote separately to urge caution regarding judicial overreach. 420 U.S. at 127 (Stewart, J., concurring) (arguing against dicta declaring more than is necessary to decide the case at hand).

[166] Maryland v. Shatzer, 559 U.S. 98, 110 (2010) (holding an in-custody invocation retains significance through fourteen days of a break in custody).

[167] *See id.* at 119–20 (Thomas, J., concurring); *id.* at 120–22 (Stevens, J., concurring in judgment).

[168] *See* Henderson, *Fourth Amendment Time Machines*, *supra* note 53, at 960–63 (explaining use restrictions).

[169] *See supra* Section I.C.3.

Thus, perhaps even more discretion is the better part of valor. In *Grady v. North Carolina*,[170] the Court unanimously held that attaching a GPS device to a person in order to track location is a search, leaving to lower courts in the first instance what the Fourth Amendment restraints might be.[171] In *Jones*, five Justices proposed that "longer term GPS monitoring in investigations of most offenses" constitutes a search,[172] again leaving reasonableness to lower courts in the first instance.[173] In *Carpenter*, the Sixth Circuit held that the government acquisition of CSLI did not constitute a search.[174] If the high court reverses merely this holding, the Sixth Circuit, other courts, and hopefully legislatures can consider the particular demands of reasonableness in the first instance.

V. POTENTIAL CONCERNS

The doctrine can thus develop in time, with *Carpenter* presenting the opportunity to put the Fourth Amendment on the right path. Before starting down any path, of course, one wants to be confident it presents no insurmountable obstacles. Here I briefly consider two—the compatibility of multiple parties sharing Fourth Amendment rights and so-called 'mosaic' concerns—before briefly concluding with some thoughts on the importance of state constitutions in the Fourth Amendment analysis.

A. Third-Party Consent

If a customer retains Fourth Amendment rights in information held by another, how does that mesh with the rights of that third party? After all, although I retain Fourth Amendment rights in a letter sent to my mother while that letter is in transit,[175] it would seem odd if I could constitutionally restrain her from providing that letter to law enforcement.[176] As far as the Fourth Amendment is concerned, upon receipt,

---

[170] 135 S. Ct 1368 (2015).

[171] *See id.* at 1371.

[172] United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring in the judgment); *id.* at 415 (Sotomayor, J., concurring).

[173] *Id.* at 430 n.11 (Alito, J., concurring in the judgment) ("In the courts below the Government did not argue, and has not argued here, that the Fourth Amendment does not impose these precise restrictions and that the violation of these restrictions does not demand the suppression of evidence obtained using the tracking device. Because it was not raised, that question is not before us." (internal citations omitted)).

[174] United States v. Carpenter, 819 F.3d 880, 890 (6th Cir. 2016) ("In sum, we hold that the government's collection of business records containing cell-site data was not a search under the Fourth Amendment."), *cert. granted*, 137 S. Ct. 2211 (June 5, 2017) (No. 16-402).

[175] *See Ex parte* Jackson, 96 U.S. 727, 733 (1877).

[176] A contrary rule in this circumstance would seem odd, but is not legally impracticable—the sender retains a copyright in the letter that, at least in theory, continues to restrict what the recipient may do with the letter. For a skeptical view of this law, see Jeffrey L. Harrison, *Privacy, Copyright, and Letters*, 3 ELON L. REV. 161 (2012).

the letter is hers. She can stand upon her own rights, retaining the letter in her home or purse and requiring a warrant—or maybe a subpoena—to access it.[177] Or, she can choose to waive those rights, selling me out. Knowing what is in that letter is now mom's life too, and she should be free to share it, including with the government.

Imagine I am a customer of Telecommunications World (TW), and as part of providing contracted-for services, TW gathers information about my activities. And say that law enforcement, for its own reasons, would like to have a look at that information. Post-*Carpenter*, if that information is protected by the Fourth Amendment warrant requirement, what happens? Sometimes, either for reasons of genuine principle, economic interest, public relations, or some combination thereof, TW will also want to insist upon the warrant—witness the 'Snowden effect.'[178] So, TW points out the legal restriction and awaits any court order;[179] if law enforcement does not like that, it can contact me—the customer—and request my voluntary consent.

Other times, however, TW will be happy to disclose the information. After all, it is not the company's technology, nor the privacy of its board members or employees, that is at issue. And, again for reasons of genuine principle, economic interest (the government is an important customer or regulator), or public relations, the company might like to play nice with police. In such a case, as between me and TW, whose desire prevails?[180]

In a sense, this situation is well-known to the Fourth Amendment under the doctrine of common authority. In most situations, one with common authority over information can choose to consent to requested law enforcement access, regardless

---

[177] For an argument that subpoenas, including grand jury subpoenas, should not get unregulated access to all private documents, see Andrew E. Taslitz & Stephen E. Henderson, *Reforming the Grand Jury to Protect Privacy in Third Party Records*, 64 AM. U. L. REV. 195 (2014).

[178] *See* Nicole Perlroth & Vindu Goel, *Internet Firms Step Up Efforts to Stop Spying*, N.Y. TIMES (Dec. 5, 2013), http://www.nytimes.com/2013/12/05/technology/internet-firms-step-up-efforts-to-stop-spying.html (describing a 'Snowden effect' in companies' increased attention to customer privacy).

[179] Orin Kerr has raised a concern that a third party like TW might not be permitted to require the warrant if its records are typically accessible under a lower legal threshold. *See* Orin Kerr, *Third Party Rights and the* Carpenter *Cell-Site Case*, WASH. POST: VOLOKH CONSPIRACY (June 15, 2017), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/06/15/third-party-rights-and-the-carpenter-cell-site-case [https://perma.cc/PRY6-WC2S]. But that seems wrong. Anytime different types of records are commingled, each having a different legal access restraint, government access to the whole should require the highest relevant restraint. And many third parties—attorneys, psychologists, hospitals, banks, etc.—should be well acquainted with considering not only their own rights in information but also the rights of their customers, at least in some contexts. Statutes have successfully added to these traditional parties, and other institutions should be able to learn to follow suit. *See, e.g.*, 18 U.S.C. § 2702 (2012) (restricting voluntary disclosure by telecommunications and internet providers).

[180] Kerr also raises this concern. *See* Kerr, *supra* note 179.

of what others enjoying the same authority might desire.[181] Although a line employee at TW likely would not share such 'common authority,' surely, it seems *somebody* at TW must. However, common authority claimed in this greater sense is not always effective. For example, a physically present co-tenant who makes a threshold objection to home entry renders the consent of other co-tenants ineffective as against her.[182] More importantly, the Supreme Court has recognized a distinction when one of the actors is a business.

Despite businesses enjoying certain aspects of some constitutional rights,[183] they do not have a human autonomy interest in choosing to share information with law enforcement.[184] Thus, even if an apartment manager or hotel employee is privileged to enter a (temporary) home, she is *not* thereby privileged to permit a law enforcement desire to join.[185] In the words of the Court, in such a situation "no common authority could sensibly be suspected," for "[a] person on the scene who identifies himself, say, as a landlord or a hotel manager calls up no customary understanding of authority to admit guests without the consent of the current occupant."[186] In other words, this is common sense: in such situations, we don't care that the businesses would like to share because it is not theirs to give. Surely nobody thinks that a Bank of America employee can consent to the access of a safety deposit box or that a Microsoft employee can consent to the access of customer emails.[187] I am not sure why anyone would—or should—think otherwise as to Verizon with respect to my location information. Once a legislature or court has announced third-party rights in information types, the norms naturally follow, and both the company and the police can be expected to know of them and to follow them.

---

[181] United States v. Matlock, 415 U.S. 164, 171 (1974). Indeed, so long as police reasonably believe the consenting individual had common authority, that consent is effective. *See* Illinois v. Rodriguez, 497 U.S. 177, 186 (1990).

[182] Fernandez v. California, 134 S. Ct. 1126, 1133–34 (2014); Georgia v. Randolph, 547 U.S. 103, 106 (2006).

[183] *See* Citizens United v. FEC, 558 U.S. 310 (2010) (holding that a federal statute barring independent corporate expenditures for electioneering communications violated the First Amendment).

[184] *See* Christopher Slobogin, *Transaction Surveillance by the Government*, 75 MISS. L.J. 139, 185–86 (2005) ("Human information sources, such as [a] sexual partner, should have a right to decide what to do with the information they possess; in such cases, the subject's privacy interest is outweighed by the source's autonomy interest. When the third party is an impersonal record-holder, on the other hand, concerns about denigrating 'personhood' through limitations on when information may be revealed are non-existent." (internal citations omitted)); *see also* Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049 (2000) (considering the First Amendment requirements and implications of information privacy speech restrictions).

[185] Stoner v. California, 376 U.S. 483 (1964) (hotel employee); Chapman v. United States, 365 U.S. 610 (1961) (landlord).

[186] *Randolph*, 547 U.S. at 112.

[187] *See* 18 U.S.C. § 2702 (2012) (restricting voluntary disclosure of emails).

So, there is a critical difference between my mother holding 'third-party information' in my letter—over the disclosure of which she has an underlying autonomy and dignitary interest, a freedom to speak her mind—and a company like our imagined TW holding customer information. Of course, things might be different if the information relates to a TW employee, or if it directly impacts TW—say it is evidence of hacking of its own servers. But these will not be the ordinary case. Instead, in a situation like *Carpenter*, no company employee has even perused the requested information; if it is to be turned over to law enforcement, it must first be gathered precisely—and solely—for this purpose. Think of it this way: if law enforcement were to enter any Verizon store or corporate office in America and request my location information, *nobody* would be able to respond from personal knowledge because *nobody* would know it.[188] An employee would need to pull it from Verizon's database.

Thus, in the American Bar Association Criminal Justice Standards relating to law enforcement access to third-party records, the relevant *consent* is solely that of the customer who is the focus of the record.[189] Two categories of acquisition from institutional third parties, however, are entirely carved out of the Standards' scope.[190] The first is when an institutional third party "that is a victim of crime [is] disclosing information that is evidence of that crime or that is otherwise intended to protect its rights or property."[191] In that instance, the third party has a relevant self-interest, and existing federal privacy statutes acknowledge such a distinction.[192] The second exception is when a third party "decid[es] of its own initiative and volition to provide information to law enforcement,"[193] meaning it was the private business—*not* law enforcement—that initiated the specific contact leading to the records transfer.[194] In such instance, the third party's action is genuinely private conduct that would seem unregulated by the Bill of Rights just as it would be unregulated by *criminal* justice standards.

In short, there seems to be no reason that third-party businesses and law enforcement cannot accommodate recognition of constitutional rights in certain third-party information. If doing so were impossible, the same would seem to follow for statutory rights, and that would seem a rather striking—and counterfactual—claim.

---

[188] If this is not true, Verizon, we need to talk. Seriously, what is your obsession with me?

[189] ABA LEATPR STANDARDS, *supra* note 71, Standard 25-5.1 at 95–99. The "focus of a record" is a defined term in order to differentiate, for example, the subscriber to which calling records relate, on the one hand, from every person whose phone number is included in those particular records, on the other. The subscriber is the "focus of [the] record." *See id.* Standard 25-1.1(c) at 29. There can of course be multiple such persons, as for a joint telephone or bank account. *See id.* Standard 25-5.1(c) at 98–99.

[190] Law enforcement access from someone who is not acting as an institutional third party is entirely outside the Standards' scope. *See id.* Standard 25-2.1(d) at 38–40.

[191] *Id.* Standard 25-2.1(f)(i) at 41.

[192] *See, e.g.*, 18 U.S.C. § 2511(2)(a)(i) (2012) (articulating such a provider exception for wiretap acquisitions); 18 U.S.C. § 2702(b)(5) (2012) (articulating such a provider exception for stored communications).

[193] ABA LEATPR STANDARDS, *supra* note 71, Standard 25-2.1(f)(ii) at 41.

[194] *See id.* Standard 25-2.1(f)(ii) at 41–44.

Not only do such statutes exist, but, as described below, some states have already gone further, recognizing such constitutional protections.

B. Mosaics

Fourth Amendment rights in third-party information thus can be workable, though—as we have already acknowledged—it is not easy to be confident in selecting administrable lines in the first instance. Should law enforcement be able to obtain twenty-four hours of data *A* on ground *x*, but need a warrant for anything more? Or should the line be forty-eight hours, or a week? What about for data types *B* and *C*? Legislatures, and then courts, have their work cut out for them.[195]

But are there concerns of administrability even *after* these lines are legally declared?[196] On the one hand, as I have pointed out elsewhere, there is nothing novel in the constitutionality of law enforcement conduct depending upon the totality of law enforcement behavior.[197] This is true for such commonplace considerations as whether police conduct constitutes a seizure requiring reasonable suspicion,[198] whether police conduct constitutes a de facto arrest requiring probable cause,[199] and whether a suspect is in custody such that *Miranda* warnings are required.[200] These lines are not absolute: sometimes drawing a firearm will elevate a stop into a de facto arrest and *Miranda* custody; other times it will be permissible as part of a limited *Terry* stop.[201] And sometimes constitutionality, or at least admissibility, depends upon what other officers have done, such as the impact of an invocation of the *Miranda* right to counsel in an unrelated interrogation.[202]

Nonetheless, while policing has always required some difficult determinations, we should consider the practical impact upon a law enforcement officer if the legal standard for access to CSLI is tiered according to duration. To make the example concrete, say access to a week or more of CSLI requires a probable cause warrant,

---

[195] As for records including both data types *A* and *C*, the legal restriction should be the greater of the two individual restrictions. *See id.* Standard 25-4.2(a) at 20.

[196] *See generally* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012) (expressing concerns with any "mosaic" standard).

[197] *See* Henderson, *Location Surveillance After* Jones, *supra* note 8, at 823–25. Much of the following content is taken directly from this article, but for ease of reference it is repeated here.

[198] *See* United States v. Drayton, 536 U.S. 194, 202 (2002) (asking "whether a reasonable person would feel free to decline the officers' requests or otherwise terminate the encounter" (citation omitted)).

[199] *See* Dunaway v. New York, 442 U.S. 200, 212–13 (1979) (looking to movement, show of authority, and duration in differentiating a de facto arrest from a *Terry* stop).

[200] *See* Berkemer v. McCarty, 468 U.S. 420, 440–42 (1984) (defining custody as when a reasonable person would feel her freedom of movement had been curtailed to the degree associated with a formal arrest).

[201] *See* United States v. Hensley, 469 U.S. 221, 224, 234–36 (1985) (holding that a detention constituted a *Terry* stop despite the drawing of a service revolver).

[202] *See* Arizona v. Roberson, 486 U.S. 675, 682–85 (1988) (holding invocation effective as against a different officer unaware of that invocation).

access to less than a week but more than twenty-four hours requires a lesser court order, and access to twenty-four hours or less is permissible upon officer request. For an officer wanting to obtain sixteen hours of such information, the path should be clear. But does that officer first need to scour her files to make sure that no CSLI was previously requested? And if ten hours of CSLI was previously obtained, does that push her current request into the court-order tier? Does it matter whether that previous request was for purposes of this same investigation or another one? Does it matter whether it took place three weeks ago or three years ago? What if the officer's colleagues might have made such requests in *their* investigations? What about the investigations of sister departments?

My solution has been to offer a "mildly mosaic" approach that does *not* typically consider previous requests, but that permits some ultimate court review in order to deter gaming of the system.[203] We do not want an officer who desires forty-eight hours of CSLI to request twenty-four of those hours, wait a day, and then request the second twenty-four, all designed to avoid the requirement of a court order.[204] On the other hand, investigations are fluid, and a genuine new request should not be unduly hampered. Whatever the specific solution, courts should thus ultimately review access, probably considering whether the requests objectively appear designed to avoid the legal restraints, thereby diminishing respect for the rule of law. Whether such violations should lead to suppression of the evidence or to other sanctions (e.g., administrative discipline, civil penalties, and even criminal sanctions), should ideally be left to legislatures in the first instance. For example, Pennsylvania has enacted a novel provision regarding the abuse of wiretaps that might be superior to any remedy involving suppression of the evidence.[205]

What is critical here is that, once again, while there will be good work to do, recognition of constitutional rights in third-party information need not derail effective police investigation.

C. State Constitutions

In closing, it is worth briefly emphasizing an obvious point: the federal Supreme Court is supreme, but only in its sphere. A number of state supreme courts have

---

[203] *See* Henderson, *Location Surveillance After* Jones, *supra* note 8, at 825.

[204] This hypothetical can be analogized to banking anti-structuring law, which criminalizes a customer breaking up a single cash transaction in order to evade financial institution reporting requirements. *See generally* Ratzlaf v. United States, 510 U.S. 135 (1994) (examining mens rea for those criminal provisions).

[205] *See* 18 PA. CONS. STAT. § 5726(a) (2017) ("Any aggrieved person shall have the right to bring an action in Commonwealth Court against any investigative or law enforcement officer, public official or public employee seeking the officer's, official's or employee's removal from office or employment on the grounds that the officer, official or employee has intentionally violated the provisions of this chapter. If the court shall conclude that such officer, official or employee has in fact intentionally violated the provisions of this chapter, the court shall order the dismissal or removal from office of said officer, official or employee.").

taken their own path when interpreting their respective state constitutional analog to the federal Fourth Amendment, including rejection of the federal third party doctrine.[206] And at least two have already done so with respect to cell site location information in opinions which should be carefully considered by the United States Supreme Court.[207]

The high court indeed has a tradition of considering such state jurisprudence in making Fourth Amendment decisions.[208] For example, in *Payton v. New York*,[209] the Court had to decide whether the Fourth Amendment allowed warrantless home entry for purposes of arrest.[210] The Court not only looked to state constitutional jurisprudence, but relied upon a *trend* of courts declaring such entry unconstitutional:

> Only 24 of the 50 States currently sanction warrantless entries into the home to arrest, and there is an obvious declining trend. Further, the strength of the trend is greater than the numbers alone indicate. Seven state courts have recently held that warrantless home arrests violate their respective *State* Constitutions. That is significant because by invoking a state constitutional provision, a state court immunizes its decision from review by this Court. This heightened degree of immutability underscores the depth of the principle underlying the result.[211]

A federal system of government certainly has downsides, but one of the certain upsides are the many laboratories of democracy.[212] The Court has been right to consider them in its constitutional interpretation in the past, and it should do so again in *Carpenter*. And no matter what the Supreme Court decides, such thoughtful state constitutional interpretation should continue. Increasingly, even those state high courts that have never diverged from the federal Fourth Amendment are careful to

---

[206] *See generally* Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373 (2006) [hereinafter Henderson, *Learning from All Fifty States*].

[207] *See* Commonwealth v. Estabrook, 38 N.E.3d 231, 234 (Mass. 2015) (holding Massachusetts Constitution requires a warrant to obtain over six hours of CSLI); State v. Earls, 70 A.3d 630, 644 (N.J. 2013) (holding New Jersey Constitution requires a warrant to obtain CSLI).

[208] *See* Henderson, *Learning from All Fifty States*, *supra* note 206, at 374–76.

[209] 445 U.S. 573 (1980).

[210] *Id.* at 574.

[211] *Id.* at 600 (internal citations omitted).

[212] *See* New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting) ("It is one of the happy incidents of the federal system that a single courageous State may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country.").

recognize that they *could* do so,[213] and this is an encouraging trend in a country in which we all enjoy two layers of constitutional protections.

CONCLUSION

In the timeless words of Justice Felix Frankfurter, "Wisdom too often never comes, and so one ought not to reject it merely because it comes late."[214] *Carpenter* has the potential to be a monumental Fourth Amendment decision, holding that there is not a monolithic third party doctrine that annihilates all constitutional protection for information residing with a third party. Such a holding is essential to balancing privacy and liberty with government need in the twenty-first century or, as the Fourth Amendment text would put it, to guaranteeing security in our persons and papers against unreasonable searches. The Court need go no further than acknowledging a search took place, however, and prudence dictates that it not. Admittedly, the resulting litigation and, hopefully, legislation, will not make the next few years easy for police, criminal defendants, and other litigants. But this path will make it much more likely that we can find a constitutional balance that best ensures our safety and security in the coming decades, as the Fourth Amendment commands.

---

[213] *See, e.g.*, State v. Ward, 604 N.W.2d 517, 530 (Wis. 2000) ("Although we generally conform art. 1, § 11 to Fourth Amendment jurisprudence, it would be a sad irony for this court to exhort magistrates to act as something more than 'rubber stamps' when issuing warrants, and to then act as mere rubber stamps ourselves when interpreting our Wisconsin Constitution. It is our responsibility to examine the State Constitution independently. This duty exists even though our conclusions in a given case may not differ from those reached by the Supreme Court when it interprets the Fourth Amendment."); *see also* Gomez v. State, 168 P.3d 1139, 1144–45 (Okla. Crim. App. 2007) ("It is well established that this State may grant protections to its citizens that are more expansive than those conferred by federal law. It is also settled that this Court's independent interpretation of Oklahoma constitutional provisions is not circumscribed by United States Supreme Court interpretations of similar federal provisions." (internal citations omitted)).

[214] Henslee v. Union Planters Nat'l Bank & Trust Co., 335 U.S. 595, 600 (1949) (Frankfurter, J., dissenting).