2019

Location Tracking and Digital Data: Can Carpenter Build a Stable Privacy Doctrine?

Evan H. Caminker
University of Michigan Law School, caminker@umich.edu

EVAN CAMINKER

LOCATION TRACKING AND DIGITAL DATA: CAN CARPENTER BUILD A STABLE PRIVACY DOCTRINE?

In *Carpenter v United States*,[1] the Supreme Court struggled to modernize twentieth-century search and seizure precedents for the "Cyber Age."[2] Twice previously this decade the Court had tweaked Fourth Amendment doctrine to keep pace with advancing technology, requiring a search warrant before the government can either peruse the contents of a cell phone seized incident to arrest[3] or use a GPS tracker to follow a car's long-term movements.[4] This time, the

Evan Caminker is the Branch Rickey Collegiate Professor of Law and former Dean, University of Michigan Law School.

Author's note: I briefed and argued *Carpenter* on behalf of the United States before the Sixth Circuit Court of Appeals while I was on academic leave and serving as a Special Assistant United States Attorney in the Eastern District of Michigan. Once the Supreme Court granted certiorari, I played no further role in strategizing about, briefing, or arguing the case. This article does not discuss, reflect, or reveal any inside information about the litigation. All of the ideas expressed here are entirely my own, and they do not necessarily reflect any views or even speculation of the United States. I thank Vik Amar, Eve Brensike Primus, Don Herzog, Jerry Israel, David Moran, Deeva Shah, and Geof Stone for valuable input on earlier drafts, and Sam Mancina and the University of Michigan Law Library for excellent research assistance.

[1] 138 S Ct 2206 (2018).

[2] Id at 2224 (Kennedy, J, dissenting).

[3] *Riley v California*, 134 S Ct 2473 (2014).

[4] *United States v Jones*, 565 US 400 (2012) (twenty-eight-day tracking).

978-0-226-64622-0/2019/2018-0012$10.00

Court asked what the Fourth Amendment requires when law enforcement seeks cell phone records revealing the user's approximate location when his cell phone connects to local cell towers. The Court's answer "is a familiar one—get a warrant."[5]

Familiar, yes; but easy, no: the Court split 5–4 with four separate dissenting opinions spanning 115 pages. The case reflects a fundamental clash between long-standing doctrinal approaches and new surveillance and digital information technologies. The government today has unprecedentedly sophisticated ways of seeing, hearing, and tracking people, ways that were unimaginable to the Fourth Amendment's Framers. The question is whether and how the Court should adjust constitutional doctrines to maintain some historical or reasonable equilibrium between privacy and law enforcement, or whether legislatures should be the guardians of privacy in the face of technological innovation.

The Court addressed this question in *Carpenter* at a time when its existing doctrinal approaches are both stressed and uncertain. The Court's primary framework protects individuals from unwarranted invasions of their "reasonable expectation of privacy," a doctrine first announced fifty-plus years ago in *Katz v United States*,[6] and then refined a decade later in *United States v Miller*[7] and *Smith v Maryland*[8] through the third-party doctrine that withheld protection for information voluntarily disclosed to others. Both of these doctrines have come under withering attack from different quarters: *Katz* for protecting privacy too freely, *Miller-Smith* for withdrawing that protection too rigidly, and both for being textually and conceptually ungrounded. Perhaps in response to these criticisms, some Justices recently revived an older framework, most famously articulated in *Olmstead v United States*,[9] holding that the Fourth Amendment protects people only against physical intrusions on or in "material things—the

---

[5] *Carpenter*, 138 S Ct at 2221.

[6] 389 US 347, 360–61 (1967) (Harlan, J, concurring) (requiring warrant to eavesdrop electronically on phone conversations).

[7] 425 US 435 (1976) (holding customer lacks Fourth Amendment interest in bank's records showing his financial transactions).

[8] 442 US 735 (1979) (holding phone customer lacks Fourth Amendment interest in phone company's records showing whom he called).

[9] 277 US 438 (1928) (rejecting challenge to government wiretapping of phone conversations).

person, the house, his papers, or his effects."[10] This test too has raised questions of scope and principled application.[11]

Lurking in the background, moreover, are competing motivations for Fourth Amendment doctrine: to protect atomistic privacy and security interests of individual citizens, and to regulate government conduct that might threaten such values.[12] The atomistic approach suffuses through the doctrine today, for example, by limiting Fourth Amendment standing to people whose rights were arguably violated by, rather than who were just incriminated by, a questionable search.[13] But the regulatory approach has its own foothold, most notably in the exclusionary remedy designed generally to deter illegal searching rather than to vindicate individual rights[14]—and some claim anew that a regulatory approach is required to address privacy threats of the modern age.[15]

What makes the *Carpenter* decision a potential game changer is that neither the *Katz* nor *Olmstead* doctrines, whether viewed through an atomistic or regulatory lens, previously seemed hospitable to many novel Fourth Amendment claims arising in the digital age. Today, given widespread use of the internet, the cloud, corporate digital-data storage, internet-connected personal devices, and related technologies, a huge amount of personal and sensitive information is stored somewhere in the digital records of an institutional third party, be it a phone company, internet service provider, bank, credit-card company, social media giant, phone applications manager, online retailer, wearable technology company, or medical provider.[16] And govern-

---

[10] Id at 464.

[11] See Orin S. Kerr, *The Curious History of Fourth Amendment Searches*, 2012 Supreme Court Review 67, 90–93 (exploring ambiguities).

[12] See, for example, Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 Minn L Rev 349, 367 (1974) ("Does [the Amendment] safeguard *my* person and *your* house and *her* papers and *his* effects against unreasonable searches and seizures; or is it essentially a regulatory canon requiring government to order its law enforcement procedures in a fashion that keeps us collectively secure in our persons, houses, papers, and effects, against unreasonable searches and seizures?").

[13] *Rakas v Illinois*, 439 US 128, 133–38 (1978).

[14] Both the deterrence focus of the exclusionary rule, and its burgeoning exception for good-faith violations, reflect this approach. See *Davis v United States*, 564 US 229, 236–39 (2011).

[15] See, for example, Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 BC L Rev 1511 (2010); Donald A. Dripps, *Perspectives on the Fourth Amendment Forty Years Later: Toward the Realization of an Inclusive Regulatory Model*, 100 Minn L Rev 1885 (2016).

[16] "Use of the Internet is vital for a wide range of routine activities in today's world—finding and applying for work, obtaining government services, engaging in commerce,

ment officials regularly subpoena documents containing this information, without warrants or probable cause, in early-stage crime investigations. Prior to this decision, *Katz*'s reasonable expectations–based approach, as limited by the third-party doctrine, did not protect the privacy interests of the targets of such investigations because the targets had voluntarily shared their information with the third party, thus relinquishing any erstwhile claim to privacy. And the older/revised *Olmstead* property invasion–based approach did not protect the targets' privacy interests because the records being secured weren't "their . . . papers [or] effects" but belonged to the third party.

In his majority opinion in *Carpenter*, Chief Justice Roberts redirected the *Katz* route to require the government to obtain search warrants before securing location-revealing cell phone records, by broadening the scope of privacy interests and narrowing the exception carved out by the third-party doctrine. The issues are complicated and the opinions long. My goal here is to analyze carefully the Court's approach, to explain and critically evaluate its reasoning, to highlight remaining important questions, and to project future directions.

Like Justice Gorsuch in dissent, "I do not begin to claim all the answers today."[17] But my main conclusions are these: To find a Fourth Amendment search, the Court substantially refashioned (though it claimed otherwise) *Katz*'s progeny to replace relatively definitive-though-controversial rules with multivariate standards, primarily by emphasizing the comparative sensitivity of location information; this shift makes doctrine more flexible and hospitable to digital privacy claims but also less coherent and clear. And at key points the Court's reasoning appears to reflect a regulatory as well as atomistic attitude toward privacy protection, motivated to forestall an Orwellian future of rampant surveillance of everyone's movements and activities. The Court purported to move cautiously, crafting a self-described "narrow" opinion addressing cell phone location records and little else, persistently labeling cell phone tracking "novel" and "unique" and creating a "qualitatively different category" of

communicating with friends and family, and gathering information on just about anything, to take but a few examples." *United States v LaCoste*, 821 F3d 1187, 1191 (9th Cir 2016).

[17] *Carpenter*, 138 S Ct at 2268 (Gorsuch, J, dissenting).

sensitive records.[18] But the opinion's reasoning opens the door for lower courts and future Court decisions to protect privacy well beyond this category.

As for the required justification, "get a warrant" is the familiar route for full-scale searches. But it is also a novel approach to requests for private document production, and the Court's ruling raises interesting and either underappreciated or unanticipated questions about broader categories of subpoenas as well. The more broadly the warrant requirement applies, the more it will frustrate "many legitimate and valuable investigative practices upon which law enforcement has rightfully come to rely."[19] So even if the Court's *Katz*-expanding reasoning invites further privacy protection over time, I predict that at some point the warrant's constraint on law enforcement efforts will likely curb that momentum. *Carpenter* takes a strong first step toward digital privacy protection, but the length of the stride remains unclear.

Part I sets the stage by briefly sketching the litigation, existing doctrinal approaches, and the five separate opinions in the case. Part II examines the Court's conclusion that acquiring customers' cell phone records from their service provider constitutes a Fourth Amendment "search" because it violates their reasonable expectation of privacy. Part III examines the Court's conclusion that such searches require a probable cause–backed warrant rather than the lesser showing typically required for document subpoenas, and it considers the majority opinion's potential effect on first-party subpoenas as well. In my view, the Court's path to both conclusions is bumpy at best, though perhaps understandably so as the Court heads in a new direction across fast-changing technological terrain.[20]

If nothing else, *Carpenter* means that a majority of the Justices are searching to find ways to better protect privacy in the modern age. And by retooling long-standing precedent to be more adaptive to privacy concerns, the decision invites much more open and free-spirited dia-

---

[18] Id at 2216–17 (majority).

[19] Id at 2247 (Alito, J, dissenting).

[20] Amsterdam, 58 Minn L Rev at 352 (cited in note 12) (the Court sometimes decides cases based on a new approach "even though it is not prepared to announce the new principle in terms of comparable generality with the old, still less to say how much the old must be displaced and whether or how the old and new can be accommodated.").

logue among lower courts, as they confront what Justice Alito aptly anticipates will be a continuing "blizzard of litigation."[21] We'll find out soon enough whether the decision works a shift in constitutional doctrine that is as "seismic" as the shift in the technology it's chasing.[22]

I. Carpenter's Backdrop and Decision

A. cell-phone tracking a cell phone thief

You really couldn't make up better facts: Timothy Carpenter used his cell phone to help his confederates steal cell phones, and then the government used his cell phone records to help to put him in a prison cell.[23]

In April 2011, police arrested four men suspected of joining a larger, rotating crew committing a months-long string of armed robberies during which they stole brand new cell phones from Radio Shack and T-Mobile stores in Michigan and Ohio. One arrestee confessed and squealed on half-brothers "Little Tim" Carpenter and "Big Tim" Sanders, plus others, providing the FBI with many of the group's cell phone numbers.

Federal officials applied under the Stored Communications Act[24] (SCA) for a court order to obtain Carpenter's and his accomplices' cell phone records for the months covering the crime spree. Specifically, the officials wanted call detail records indicating the phone numbers the men called at what times, and also records indicating which cell phone towers the phones used when the men made or received those calls—otherwise known as cell-site location information, or CSLI.

Cell phones transmit radio signals to cell sites (antennas) mounted on cell towers. Each tower typically has three or six cell sites spread around it in a circle, creating separate sectors that carve the space surrounding the tower into pie-slice-shaped service areas. More sectors create narrower pie slices, and closer towers create shorter slices. When the phone sends or receives a call, text message, or other

---

[21] *Carpenter*, 138 S Ct at 2247 (Alito, J, dissenting).

[22] Id at 2219 (majority).

[23] See generally id at 2211–13; *Carpenter v United States*, 819 F3d 880, 884–85 (6th Cir 2016).

[24] 18 USC §§ 2701–12 (2012).

data, the phone signals the local cell site with the strongest signal.[25] That's usually the nearest tower, so the phone typically connects to the cell site located at the tip of the service area in which the phone resides.[26] Wireless carriers can detect and record which phones connect to which of their cell sites at what times. For various business reasons, such as detecting coverage problems and billing for roaming charges, they maintain records containing their customers' CSLI for up to several years.

The SCA authorizes judges to compel production of cell phone records when government provides "specific and articulable facts showing that there are reasonable grounds to believe" the records sought "are relevant and material to an ongoing criminal investigation"[27]—a significantly weaker showing than the probable cause typically required for a search warrant, though more than required for a grand jury subpoena. Agents requested 152 days of CSLI records from Carpenter's primary carrier MetroPCS (which produced 127), and seven days of records from roaming-in-Ohio carrier Sprint (which produced two, all it had). The records indicated that Carpenter placed cell phone calls from within a half-mile to two miles from several of the robberies just before or while they occurred, corroborating reports that Carpenter was typically the "lookout" who used his phone to signal the actual robbers when to enter the targeted stores.

Combining this location information with other evidence, the United States charged Carpenter with six counts of robbery, Sanders with two counts, and both with related gun offenses. Both defendants moved to suppress Sprint's CSLI data,[28] arguing that its procurement without a probable cause–backed search warrant violated the Fourth Amendment. The district court denied the motion, and at trial the government introduced a few of the CSLI records to locate the

---

[25] Unless turned off or in "airplane mode," the phone continually sends out registration pings to nearby cell sites, measuring in advance the relative strength of available connections so it is ready to go. Aaron Blank, *The Limitations and Admissibility of Using Historical Cellular Site Data to Track the Location of a Cellular Phone*, Richmond J L & Tech 1, 5 (2011).

[26] Weather, topography, and obstructions such as buildings and trees can sometimes cause cell phones to connect to a tower that isn't the nearest one. Id at 6–7.

[27] 18 USC § 2703(d).

[28] Following the Court's lead, *Carpenter*, 138 S Ct at 2219 (referencing "Sprint Corporation and its competitors"), I'll use Sprint to refer to the carriers (including MetroPCS) involved in this case and also generic wireless carriers.

The defendants did not seek to suppress the call detail records linked to the cell-site data.

defendants near some of the robberies when they occurred. A jury found both men guilty, and the court sentenced Carpenter to over 116 years' imprisonment (note: if you rob a store, don't let a buddy use a gun).

The Court of Appeals for the Sixth Circuit affirmed, holding that compelling Sprint to produce CSLI records does not constitute a Fourth Amendment search.[29] This ruling was predictably consistent with other Court of Appeals rulings, because then-binding Supreme Court precedent was fairly clear.[30] But there were equally clear signs of a storm brewing within the Court over the direction of doctrine and its suitability for the digital age. And when the Court granted review despite the lack of a circuit split, one could easily forecast a tempest ahead.[31]

B. COMPETING FOURTH AMENDMENT FRAMEWORKS

The Fourth Amendment declares "[t]he right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures shall not be violated. . . ."[32] The Court over time, and internally today, has split between two quite different doctrinal frameworks and motivating visions.

---

[29] *Carpenter*, 819 F3d at 886–90.

[30] *In re Application of United States for an Order Directing a Provider of Electronic Comm'n Service to Disclose Records to Gov't*, 620 F3d 304 (3d Cir 2010); *In re Application of United States for Historical Cell Site Data*, 724 F3d 600 (5th Cir 2013); *United States v Davis*, 785 F3d 498 (11th Cir 2015) (en banc); *United States v Graham*, 824 F3d 421 (4th Cir 2016) (en banc); *United States v Thompson*, 866 F3d 1149 (10th Cir 2017).

[31] Sanders did not petition for certiorari alongside Carpenter, despite his own fourteen-year sentence. Of course, even a Supreme Court victory would not likely help the half-brothers' plight. Upon remand, Carpenter will (and Sanders would have) likely confront the argument that his CSLI records were still admissible at trial based on the good-faith exception to the exclusionary rule, as the government reasonably followed the SCA's procedures. See *Illinois v Krull*, 480 US 340, 349 (1987) (good-faith exception applies when officials act "in objectively reasonable reliance on a statute" unless it is "clearly unconstitutional"); *United States v Warshak*, 631 F3d 266, 288–89 (6th Cir 2010) (applying good-faith exception to e-mail content records secured under the SCA despite ruling that procuring e-mail content requires a warrant); *United States v Pembrook*, 876 F3d 812, 823 (6th Cir 2017) (applying exception to CSLI records based on alternative argument that no binding judicial precedent then required a warrant). Carpenter will also likely face strong arguments, as Sanders would have too, that the CSLI evidence was cumulative so any error was harmless. See Brief for the United States, *United States v Carpenter*, Nos 15-1572 & 14-1805, *40–47 (6th Cir, filed May 6, 2015) archived at https://perma.cc/78RV-KT83 (*Carpenter* 6th Cir Brief) (advancing good-faith exception and harmless error arguments).

[32] US Const, Amend IV.

1. *The Katz framework: privacy and public exposure*. In *Katz*, FBI agents eavesdropped on the defendant's phone call by placing an electronic listening device on the outside of a public telephone booth. Because the "Fourth Amendment protects people, not places,"[33] the Court announced, it didn't matter that the government had left untouched Katz's person, houses, papers, or effects. As Justice Harlan famously restated the rule in his concurring opinion, a person enjoys a Fourth Amendment protected interest if she has "exhibited an actual (subjective) expectation of privacy and . . . the expectation [is] one that society is prepared to recognize as 'reasonable.'"[34] By shutting the phone-booth door behind him, Katz reasonably expected his conversation would remain private except for the person he was calling.[35] The Court has embraced and applied Justice Harlan's two-part "reasonable expectation of privacy" test ever since.[36]

But from the very beginning, the Court made clear that public disclosure defeats potential Fourth Amendment protection. As *Katz* put it, the Fourth Amendment does not protect "objects, activities, or statements that [a person] exposes to the 'plain view' of outsiders."[37] This principle manifests itself in several ways, two of which are central here:

Exposure of public movements: Revealing yourself to the general public extinguishes any erstwhile privacy interest in your location or visible activities. In *United States v Knotts*,[38] police used a "beeper" planted in a container of chloroform, after visual surveillance failed, to help track a vehicle used by suspected drug manufacturers. The Court held that the tracking did not constitute a search, reasoning that Knotts could not reasonably expect privacy "in his movements from one place to another" because "he voluntarily conveyed to anyone who wanted to look" his route, stops along the way, and final destination.[39] The Court has since invoked this reasoning to deny

---

[33] 389 US at 351.

[34] Id at 361 (Harlan, J, concurring).

[35] Id.

[36] See, for example, *Terry v Ohio*, 392 US 1, 9 (1968); *Smith*, 442 US at 740.

[37] *Katz*, 389 US at 361 (Harlan, J, concurring); see id at 351 (majority) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.").

[38] 460 US 276 (1983).

[39] *Knotts*, 460 US at 281–82.

privacy protection for movement and activities in a variety of contexts where "anyone who wants to look" can see what's going on.[40]

And yet *Knotts* cryptically hinted at a possible limit to what "anyone" can see, as different rules might apply to "dragnet type" twenty-four-hour surveillance practices.[41] Three decades later in *United States v Jones*,[42] five Justices turned the hint into a full-blown alarm. Suspecting Jones of drug trafficking, agents surreptitiously attached a GPS tracking device to his car and remotely monitored the car's movements for twenty-eight days.[43] Justice Scalia wrote the majority opinion, holding that physically affixing the device to the car constituted a Fourth Amendment search under *Olmstead*'s invasion-of-property approach.[44] But Justice Sotomayor (for herself, after joining the majority) and Justice Alito (for himself and Justices Ginsburg, Breyer, and Kagan, rejecting the majority) penned *Katz*-driven concurring opinions, recognizing that modern technologies enable police to track a car without physically intruding upon it.[45] After focusing on ways that GPS location information can reveal sensitive information, they posited that "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[46]

This shadow majority of five Justices embraced what many call a "mosaic" theory: even though discrete movements or locations lack Fourth Amendment protection after being "disclosed to the public at large,"[47] a substantial aggregation of those movements can rise to the level of a protected interest. While privacy advocates cheered this nonprecedential endorsement,[48] critics viewed the mosaic approach

---

[40] See, for example, *California v Ciraolo*, 476 US 207, 213–15 (1986) (no search where police in private plane flew over defendant's yard and spotted marijuana, because defendant voluntarily exposed backyard to visual observation from publicly navigable airspace); *Florida v Riley*, 488 US 445, 449 (1989) (same for helicopter flyover).

[41] *Knotts*, 460 US at 283–84.

[42] 565 US 400 (2012).

[43] Agents exceeded their search warrant authority by attaching the device too late and in the wrong jurisdiction. 565 US at 402–3.

[44] Id at 404. See text accompanying notes 61–63.

[45] Id at 414–15 (Sotomayor, J, concurring).

[46] Id at 430 (Alito, J, concurring in the judgment); id at 415 (Sotomayor, J, concurring).

[47] *Carpenter*, 138 S Ct at 2215.

[48] See, for example, 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 L & Pub Pol (Special Issue) 1 (2012); Paul Rosenzweig, *In Defense of the Mosaic Theory* (LawFare, Nov 29, 2017), archived at https://perma.cc/RYX5-DUVS.

as "upend[ing] decades of settled doctrine"[49] and raising significant conceptual and pragmatic questions.[50] Thus the *Jones* concurrences created substantial uncertainty about *Knotts*'s heretofore bright-line public exposure doctrine.

Exposure of third-party records: The Fourth Amendment likewise does not protect information that is willingly disclosed to a third party and then obtained by the government from that party. In *United States v Miller*, federal agents who suspected Miller of running an illegal whiskey distillery subpoenaed his banks to produce his financial records, including some checks, deposit slips, and other account documentation. The Court rejected Miller's Fourth Amendment challenge to the subpoenas, holding that he lacked any reasonable expectation of privacy in the banks' records and therefore he was not "searched" under *Katz*.[51] He had "voluntarily conveyed" the sought-after information to the banks and "exposed [it] to their employees in the ordinary course of business."[52] Miller thus took the risk that the banks would share that information with the government.

Three years later in *Smith v Maryland* the police, suspecting Smith of making badgering phone calls to a woman he had robbed, asked a telephone company to install at its central office a pen register corresponding to Smith's home landline.[53] The pen register recorded only the outgoing phone numbers he dialed, not the content of any communications.[54] The Court rejected Smith's Fourth Amendment challenge to the warrantless request because Smith voluntarily revealed the called numbers to the phone company through his dialing. Smith lacked a subjective expectation of privacy, knowing he had to convey the numbers to complete his calls, and knowing the company could make and keep records of his calls.[55] And, in any event, any subjective expectation of privacy would not be objectively reasonable, as "a person has no legitimate expectation of privacy in information he

---

[49] Matthew B. Kugler and Lior Jacob Strahilevitz, *Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory*, 2015 Supreme Court Review 205, 209.

[50] See, for example, Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 Mich L Rev 311 (2012) (explaining and largely criticizing the mosaic approach).

[51] *Miller*, 425 US at 437–40.

[52] Id at 442.

[53] *Smith*, 442 US at 737.

[54] Id at 741.

[55] Id at 742–43.

voluntarily turns over to third parties."[56] So again, the pen register's use was not a search under *Katz*.

The seminal *Miller-Smith* decisions established the third-party doctrine that cabins *Katz*. As *Miller* summarized:

> the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[57]

Scholars haven't been kind to this doctrine, to say the least, claiming that the doctrine's all-or-nothing treatment of disclosure clashes with any reasonable conception of reasonable expectations.[58] For some critics, *Miller* and *Smith* were wrong when decided; for others, their legacy became increasingly untenable as third parties' digital creation and retention of personal records burgeoned over time. As currently applied to a world in which countless companies digitally store vast amounts of personal information about virtually everyone—including but not limited to records of communications, purchases, finances, computer searches, car operations, media viewing, home and wearable technology use, travel, and medical histories[59]—the doctrine forestalls Fourth Amendment protection and gives government access basically for the asking. After Justice Sotomayor's concurrence in *Jones* echoed this chorus of criticism by proclaiming "it may be necessary to reconsider" the third-party doctrine because the "approach is ill suited to the digital age,"[60] the *Miller-Smith* edifice suddenly wobbled.

2. *The Olmstead framework: property-focused tetrad intrusions*. Along with questions about *Katz*'s "public exposure" principles came questions about *Katz* itself. Because the reasonable expectations of privacy test isn't constrained by the textual tetrad of persons, houses, papers, or effects, Justices inclined toward textual or originalist interpretation predictably looked elsewhere for guidance.

---

[56] Id at 743–44.

[57] *Miller*, 425 US at 443.

[58] See note 170.

[59] See, for example, Stephen E. Henderson, *Our Records Panopticon and the American Bar Association Standards for Criminal Justice*, 66 Okla L Rev 699, 704–7 (2014); id at 704 ("If we step back and think of our everyday experiences, it is easy to see that very significant information about each of us is recorded by third parties that used to be recorded by no one.").

[60] 565 US at 417 (Sotomayor, J, concurring).

In *Jones*, Justice Scalia resurrected *Olmstead*'s property-based approach. In *Olmstead*, the Court rejected a Fourth Amendment challenge to government wiretapping of home and office phone lines used by bootlegging suspects. The Court held that the "amendment itself shows that the search is to be of material things—the person, the house, his papers, or his effects"[61] rather than intangible things such as sounds or sights. In addition, the Court continued, a search occurs only upon "an actual physical invasion" of such material things.[62] Because the agents tapped Olmstead's phone lines "without any trespass upon [his] property,"[63] they conducted no Fourth Amendment search. In *Jones*, Justice Scalia (with four other Justices) applied this test in holding that when agents attached a GPS tracking device to Jones's car, they "physically occup[ied] private property for the purpose of obtaining information" and therefore searched the car.[64]

Justice Scalia posited that this tetrad-invasion approach, in which the Fourth Amendment primarily protects property rather than privacy interests, could coexist with *Katz*.[65] But there is no question that he and other like-minded Justices (presumably including his successor Justice Gorsuch) hoped never to rely on *Katz* going forward, adding additional uncertainty to the mix.[66] Thus, the fissures within *Katz* and its progeny and the resurgence of the property-based approach raised questions about whether and how *Carpenter* might build new doctrine for the digital age.

c. overview of carpenter's opinions

1. *The Court (Chief Justice Roberts, joined by Justices Ginsburg, Breyer, Sotomayor, and Kagan).* Chief Justice Roberts's opinion for the Court applied the *Katz* framework, concluding that when the government acquired Carpenter's cell-site records, it "searched" him

[61] *Olmstead*, 277 US at 464.

[62] Id at 466.

[63] Id at 457.

[64] 565 US at 404.

[65] Id at 409.

[66] As recounted earlier, in *Jones* four Justices embraced the property-based framework, four the reasonable-expectations framework, and one both. In *Florida v Jardines*, 569 US 1 (2013), five Justices held that police searched Jardines's home when they lingered at his front door with a drug-sniffing dog because they thereby physically invaded the house's curtilage without license to do so, three of these Justices held that the lingering was also a search because it invaded Jardines's *Katz*-based reasonable expectation of privacy, and the other four Justices held none of the above.

by invading his reasonable expectation of privacy in information about his whereabouts. The Court invoked some "basic guideposts" for *Katz*'s application: the Fourth Amendment seeks to secure the "'privacies of life' against 'arbitrary power'" and "'to place obstacles in the way of a too permeating police surveillance.'"[67] When confronting "innovations in surveillance tools," Roberts explained, the Court seeks to "'assure[ ] preservation of that degree of privacy against Government that existed when the Fourth Amendment was adopted.'"[68]

Following these guideposts, the Court decided that Carpenter had a protected privacy interest in CSLI data revealing his movements over a week or more, but left open the question for shorter durations.[69] Roberts explained that location information is sufficiently continuous and precise that the records essentially tracked Carpenter back in time to provide an "all-encompassing record of [his] whereabouts"[70]—sufficient to potentially reveal "not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'"[71] Such long-term tracking, Roberts noted, goes beyond what people normally expect to expose publicly as they move around. Embracing the mosaic theory, the Court cabined *Knotts* and recognized Carpenter's reasonable expectation of privacy "in the whole of his physical movements."[72]

The Court then held, for the first time, that the *Miller-Smith* third-party doctrine did not encompass a particular category of stored records. First, given the widespread use of and need for cell phones today, Roberts maintained that CSLI is not voluntarily shared in the same way as bank records and phone calls. Second, he argued, location records are more sensitive than bank and call records. "There is a world of difference," he explained, "between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today."[73] Thus, "[i]n light of the deeply revealing nature of

---

[67] *Carpenter*, 138 S Ct at 2214, quoting *Boyd v United States*, 116 US 616, 630 (1886), and *United States v Di Re*, 332 US 581, 595 (1948), respectively.

[68] *Carpenter*, 138 S Ct at 2214, quoting *Kyllo v United States*, 533 US 27, 34 (2001).

[69] *Carpenter*, 138 S Ct at 2217 n 3.

[70] Id at 2217.

[71] Id, quoting *Jones*, 565 US at 415 (Sotomayor, J, concurring).

[72] *Carpenter*, 138 S Ct at 2219.

[73] Id.

CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection."[74] As a result, Carpenter's location information "was the product of a search."[75]

Absent exigent circumstances, the Court further held, such a search requires a warrant backed by probable cause.[76] The Court dismissed the suggestion that because the SCA requires Sprint or other carriers to produce the CSLI records itself, the lesser Fourth Amendment standard of relevance and nonburdensomeness typically required for subpoenas *duces tecum* (and satisfied by SCA orders) should apply. The Court concluded this lesser standard is not appropriate where the target retains a *Katz*-based privacy interest in the records being sought, a "rare case" justifying the stricter warrant requirement.[77]

2. *Justice Kennedy's dissent (joined by Justices Thomas and Alito).* Justice Kennedy wrote the primary (and his very last) dissent. The main thrust of his argument was that the Court applied *Katz* too expansively and the "public exposure" precedents too narrowly. Justice Kennedy defended the *Miller-Smith* third-party doctrine, arguing first that it faithfully reflects the notion that people cannot claim a privacy interest in papers or effects that are not theirs, and second that the doctrine accords with the government's traditional authority to use (warrantless) subpoenas to obtain documents.[78] Carpenter, Justice Kennedy argued, loses under this doctrine because he does not own, possess, or control Sprint's CSLI records in any meaningful sense.[79]

The Court finds otherwise, Justice Kennedy continued, only by misreading its "public exposure" precedents. While he questioned the Court's use of the *Jones* concurrences to supersede *Knotts*'s privacy waiver for public movements,[80] he trained his fire on the Court's "transform[ing] *Miller* and *Smith* into an unprincipled and unwork-

---

[74] Id at 2223.

[75] Id at 2217.

[76] *Carpenter*, 138 S Ct at 2221. The SCA's statutory standard fell "well short" of the required showing. Id.

[77] Id at 2221–22.

[78] Id at 2227–29 (Kennedy, J, dissenting).

[79] Id at 2229–30 (Kennedy, J, dissenting).

[80] *Carpenter*, 138 S Ct at 2231 (Kennedy, J, dissenting).

able doctrine."[81] In his view, *Miller-Smith* established a bright-line rule extinguishing privacy interests in shared information, rather than a balancing test taking sensitivity into account.[82] And even so, he maintained, the Court erred in its arbitrary judgments that location information is more sensitive than financial and phone call records, that location records are cheaper and easier to acquire, and that cell phone use is less "voluntary" than using banks or credit cards.[83]

Because technological change has "complex effects on crime and law enforcement" and can influence both property norms and expectations of privacy, Justice Kennedy would defer to Congress' judgment in enacting the SCA, which he believed "weighed the privacy interests at stake and imposed a judicial check to prevent executive overreach."[84] Kennedy closed by worrying that the Court's decision would negatively affect law enforcement, noting that access to CSLI is "an important investigative tool for solving serious crimes" and is often "indispensable" in the early stages of an investigation before the government can develop probable cause supporting a warrant.[85]

3. *Justice Thomas's dissent.* Justice Thomas also maintained that the key issue is not "whether" a search occurred (yes), but "whose" property was searched.[86] Although Sprint was "searched," Thomas insisted that Carpenter was not "searched" because neither property, tort, contract, nor federal statutory law supports Carpenter's claim that Sprint's records are *his* papers or effects.[87]

But Justice Thomas wrote separately primarily to lambast *Katz*, which "has no basis in the text or history of the Fourth Amendment" and "invites courts to make judgments about policy, not law."[88] First, he argued, the reasonable expectation of privacy test has no plausible foundation in Fourth Amendment text because it distorts the original meaning of "search," wrongly focuses on privacy rather than property, reads the tetrad list out of the text, excises the word "their"

---

[81] Id at 2230 (Kennedy, J, dissenting).

[82] Id at 2232 (Kennedy, J, dissenting).

[83] Id at 2232–33 (Kennedy, J, dissenting).

[84] *Carpenter*, 138 S Ct at 2233 (Kennedy, J, dissenting).

[85] Id at 2233–34 (Kennedy, J, dissenting).

[86] Id at 2235 (Thomas, J, dissenting).

[87] Id at 2242–43 (Thomas, J, dissenting).

[88] *Carpenter*, 138 S Ct at 2236 (Thomas, J, dissenting).

modifying the tetrad, and wrongly applies "unreasonable" to define searches rather than to justify them.[89] Second, he argued, the *Katz* test has proven unworkable in practice, which he illustrated by stringing together a long list of scholarly epithets, including my favorite, "a mass of contradictions and obscurities."[90] It is not clear, he observed, whether privacy expectations are to be measured empirically or normatively, and (even worse) neither measure is any good.[91] The nicest thing Justice Thomas called *Katz* is a "failed experiment," one that the Court, he maintained, is duty-bound to reconsider.[92] If that happens, it's not hard to guess what Justice Thomas will do.

4. *Justice Alito's dissent (joined by Justice Thomas).* Justice Alito piled on by also attacking the Court's decision to let Carpenter object to the search of a third party's property, arguing that neither the constitutional text nor a proper reading of *Miller-Smith* permits this, and insisting that neither federal statute nor any other law gives Carpenter "any meaningful property-based connection to the cell-site records owned by his provider."[93]

Justice Alito's primary target, however, was the Court's decision to require a warrant for the "search" it defined. To Alito, the Court ignored the basic distinction between a traditional search in which government agents rummage through protected spaces or things, and a constructive search in which government agents simply request the target to produce specified documents. Alito traced the history of subpoenas from British practice through the founding,[94] concluding that "the Fourth Amendment, as originally understood, did not apply to the compulsory production of documents at all."[95] He acknowledged that the Court's doctrine does not reflect this view; instead, document subpoenas must satisfy the Fourth Amendment's "reasonableness" requirement[96]—but they do so when they satisfy the much-relaxed standard of being limited in scope, relevant in purpose,

---

[89] Id at 2238, 2239–40, 2241, 2241–42, 2243–44 (Thomas, J, dissenting).

[90] Id at 2244 (Thomas, J, dissenting).

[91] Id at 2245–46 (Thomas, J, dissenting).

[92] *Carpenter*, 138 S Ct at 2246 (Thomas, J, dissenting).

[93] Id at 2257–60, 2260 (Alito, J, dissenting).

[94] Id at 2247–52 (Alito, J, dissenting).

[95] Id at 2250 (Alito, J, dissenting).

[96] *Carpenter*, 138 S Ct at 2252–57 (Alito, J, dissenting).

and not unreasonably burdensome.[97] SCA orders easily pass this test.[98]

After lamenting the Court's failure to defer to legislative judgments regarding privacy and technology, Justice Alito concluded that "[t]he desire to make a statement about privacy in the digital age does not justify the consequences [of thwarting important law enforcement investigations] that today's decision is likely to produce."[99]

5. *Justice Gorsuch's dissent—or concurrence dressed as a dissent.* Justice Gorsuch also jumped on the *Katz*-bashing bandwagon. He maintained that both the Fourth Amendment's "plain terms" and history show that the "framers chose not to protect privacy in some ethereal way" but only in "particular places and things," meaning the textual tetrad.[100] He also characterized the *Katz* test as both undetermined and indeterminate: after five decades of doctrinal dominance "we still don't even know" whether the test poses an empirical or a normative question,[101] and insufficiently guided judges have reached decisions that are "often unpredictable—and sometimes unbelievable,"[102] inevitably resting on their "own curious judgment."[103] Moreover, he declared, the *Miller-Smith* gloss is "not only wrong, but horribly wrong,"[104] whether the question about post-sharing expectations is empirical or normative, which itself is unclear.[105] And beyond that, he insisted, the Court's effort to tweak and apply *Katz* and *Miller-Smith* to the facts in *Carpenter* made matters worse, now dictating two "amorphous balancing tests"—"*Katz*-squared"[106]—weighing incom-

---

[97] Id at 2256 (Alito, J, dissenting).

[98] Id at 2255 (Alito, J, dissenting).

[99] Id at 2261 (Alito, J, dissenting).

[100] *Carpenter*, 138 S Ct at 2264 (Gorsuch, J, dissenting).

[101] Id at 2265 (Gorsuch, J, dissenting).

[102] Id at 2266 (Gorsuch, J, dissenting), poking fun in particular at *Florida v Riley*'s approval of police snooping around residential backyards via hovering helicopter, 488 US 455 (1989), and *California v Greenwood*'s approval of police rummaging through curbed trash ahead of the raccoons, 486 US 35 (1988).

[103] *Carpenter*, 138 S Ct at 2266 (Gorsuch, J, dissenting).

[104] Id at 2262 (Gorsuch, J, dissenting), quoting Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 Mich L Rev 561, 564 (2009).

[105] *Carpenter*, 138 S Ct at 2262–63 (Gorsuch, J, dissenting), quoting William Baude and James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 Harv L Rev 1821, 1872 (2016).

[106] *Carpenter*, 138 S Ct at 2272 (Gorsuch, J, dissenting).

mensurable variables.[107] But at least Justice Gorsuch graciously allowed that the *Carpenter* majority's doctrinal mishmash was not the Court's fault because, he opined, "this is where *Katz* inevitably leads."[108]

Justice Gorsuch then spent the bulk of his opinion sketching out a potential argument on Carpenter's behalf that purported to protect his privacy interests while remaining true to the traditional property-based framework.[109] The approach combines (1) old-school bailment principles that demonstrate an individual does not necessarily abdicate Fourth Amendment protections for property merely by voluntarily sharing it, (2) a more recent recognition that positive law can create property rights in intangible things such as digital records, and (3) a specific claim that a federal statute prohibiting wireless carriers from publicly sharing their customers' location information[110] might be such a law.[111] The combination, Justice Gorsuch suggested, might give customers a form of bailed ownership interest such that the CSLI records become (at least in part) *their* papers or effects for Fourth Amendment purposes.[112] And perhaps, he continued, this model might generalize to other types of third-party digital records as well. In the end, though, Justice Gorsuch dissented rather than concurred after concluding that Carpenter failed to present any property or positive law-based claim in the courts below.[113]

---

[107] Id at 2267 (Gorsuch, J, dissenting).

[108] Id (Gorsuch, J, dissenting).

[109] I plan to address more fully the promises and pitfalls of Justice Gorsuch's proposed approach in a separate essay. See Evan Caminker, *Rebuilding Carpenter on Property Law Foundations: Justice Gorsuch's Proposed Approach to Protecting Privacy in the Digital Age* (unpublished manuscript, 2018) (on file with author). Given interpretative trends and shifting membership, this approach may reflect an ascendant position on the Court. In my view, while Justice Gorsuch suggests creative ways to update the *Olmstead* approach to better address privacy threats of the digital age, significant questions remain.

[110] Telecommunications Act of 1996, 47 USC § 222.

[111] *Carpenter*, 138 S Ct at 2267–71 (Gorsuch, J, dissenting).

[112] Id at 2272 (Gorsuch, J, dissenting). It is worth nothing that Justice Gorsuch would part company here with his fellow dissenters, all of whom reject this conclusion. See id at 2229–30 (Kennedy, J, dissenting); id at 2242–43 (Thomas, J, dissenting); id at 2257–59 (Alito, J, dissenting).

[113] Carpenter's new counsel (the ACLU) briefed this statutory claim to the Supreme Court. Brief for Petitioner, *Carpenter v United States*, No 16-402, *33–35 (US, filed Aug 7, 2017) (available on Westlaw at 2017 WL 3575179) ("*Carpenter* Petr's Brief"). But Carpenter never mentioned any statutory claim or broader property rights claim before either the district court or court of appeals. Indeed, his district court brief supporting his motion to suppress (joining his co-defendant) never once uses the word "property," and his Sixth Circuit brief uses the term only three times and only when describing the charged robberies. Defendant Timothy Sanders's Motion in Limine to Suppress Cell Phone Data, *United States v Sanders*,

II. Building a New Search Doctrine for Cell Phone Location Records

Carpenter's majority (and Justice Gorsuch) clearly recognized that current doctrinal protections do not "fit neatly" with modern forms of digital data or data analytics.[114] Under the *Katz*-based approach, Chief Justice Roberts explained, "requests for cell-site records lie at the intersection of two lines of cases"[115]—an odd locution when the public and third-party exposure lines don't intersect but rather both lead directly away from Fourth Amendment protection. But Roberts redirected both doctrinal paths, creating more flexible routes of reasoning that better respond to digital data's oft-sensitive nature and the circumstances of its sharing. And while Roberts described the Court's doctrinal revisions as narrow, their rationales appear to leave room for extension to a much broader set of digital records and privacy concerns.

A. Location Information and the Threat to Privacy: Record, Reality, and Ruling for the Future

Carpenter's privacy claim is straightforward: Sprint's CSLI records reveal his phone's general location at many moments over a long period of time, enabling someone studying those records to infer some activities and associations he might rather keep confidential. CSLI's capacity to threaten his personal privacy depends on how precisely it determines location, how frequently Sprint records phone-tower connections, and for how long Sprint stores the data. Chief Justice Roberts's opinion of the Court depicted CSLI as rivaling GPS tracking in these respects, providing a "detailed chronicle" of a person's physical presence "every moment of every day for five years."[116]

This alarming claim of "near perfect surveillance"[117] is futuristic, projecting well beyond the record data from 2011 and even beyond

Case No 12-cr-20218 (ED Mich, filed Nov 21, 2013) (joined by Carpenter); Appellant's Brief, *United States v Carpenter*, No 15-1572, *3, 41 (6th Cir, filed Mar 2, 2015). So if the doctrine of argument forfeiture means anything (a fair question), it surely applies here.

[114] *Carpenter*, 138 S Ct at 2214.

[115] Id.

[116] Id at 2220; id at 2218 (comparing phone to ankle monitor).

[117] Id at 2218.

present-day reality. To be sure, CSLI data are certainly trending toward greater precision and frequency. But Chief Justice Roberts's willingness to pretend the future is already here (and likely exaggerate it) suggests two things: first, a desire to get ahead of the technology curve rather than rule from behind, reflecting a regulatory rather than atomistic attitude toward Fourth Amendment protection in this context; and, second, an effort to describe the privacy intrusion as particularly acute, so as to limit the precedential scope of the ruling.

1. *Precision of recorded locations.* Given the spacing of cell towers where Carpenter made and received phone calls, the CSLI data merely "locate[d] the defendants' cellphones within a 120- (or sometimes 60-) degree radial wedge extending between one-half mile and two miles in length."[118] Those service areas are "between around a dozen and several hundred city blocks" and "up to 40 times more imprecise" in rural areas.[119] And nothing indicates where in a particular service area the phone was located at any point in time.[120] The location information in the record is therefore "as much as 12,500 times less accurate than the GPS data in *Jones*."[121]

And yet the Court felt unconstrained by the record, declaring that it "'must take account of more sophisticated systems that are already in use or in development.'"[122] Even so, the Court seemed quite aggressive in describing those systems as "rapidly approaching GPS-level preci-

---

[118] *Carpenter v United States*, 819 F3d 880, 889 (6th Cir 2016).

[119] *Carpenter*, 138 S Ct at 2225 (Kennedy, J, dissenting); see also Stephen E. Henderson, *Carpenter v. United States and the Fourth Amendment: The Best Way Forward*, 26 Wm & Mary Bill of Rts J 495, 501 (2017) (calculating service area to range from 0.1 square miles to 4.2 square miles).

[120] See Joint Appendix, *United States v Carpenter*, No 16-402, *86–88 (US filed Aug 7, 2017) (available on Westlaw at 2017 WL 3614549) ("*Carpenter* Appendix") (testimony of Agent Hess): "Q: [Y]ou are not able to say that the phone was at a particular place, right? A: Correct. Q: What you would really say at best is that it is somewhere within that area that could be a half-mile to a mile in distance from the tower and then [as wide as the far crossing line] connecting those two, right? A: Right. . . . [The phone] would be within the footprint of that tower on that sector."

[121] *Carpenter*, 819 F3d at 889. The Court protested that the government could "deduce" when Carpenter "was at the site of the robberies," information "accurate enough to highlight" during closing argument. *Carpenter*, 138 S Ct at 2218. Yes—except the prosecutor's reference to "at the site" meant nothing more than somewhere in the "exact" or "right sector" for a nearby cell tower. *Carpenter* Appendix at *56 (cited in note 120) (government's closing argument).

[122] *Carpenter*, 138 S Ct at 2218, quoting *Kyllo*, 533 US at 36.

sion."[123] Since Carpenter's crime spree, carriers have installed more cell sites so that "the geographic area covered by each cell sector has shrunk, particularly in urban areas."[124] But how much will service areas likely continue to shrink? Even six times the present would leave most service areas measuring two to fifty blocks.[125] And what about other technological developments that might slow or reverse this trend by *reducing* reliance on local cell-site connections?[126]

The Court pointed to "new technology measuring the time and angle of signals hitting their towers" giving carriers "the capability to pinpoint a phone's location within 50 meters."[127] But the cited briefs contain scant evidence that these newer capabilities will ever be regularly used (except when law enforcement requests real-time tracking), or the resulting data will be regularly recorded and stored.[128] The most supportive data show that Verizon keeps more-precise-than-mere-service-area data for just eight days,[129] and one can only speculate if and

---

[123] *Carpenter*, 138 S Ct at 2219.

[124] Id.

[125] Carpenter's own data source (updated) reports a 52 percent increase in cell sites over the past decade (to 323,448) by the end of 2017, and projects another 800,000 or so small cells (typically deployed on streetlights or utility poles, with much smaller service areas) by 2026. CTIA, *The State of Wireless 2018* *20 (2018), archived at https://perma.cc/7QGZ-6EKA. As implied, small cells create much smaller service areas, such as "one floor of a building, the waiting room of an office, or a single home," *Graham v United States*, 824 F3d 421, 448 (4th Cir 2016) (en banc) (Wynn dissenting).

[126] Brief for the United States, *United States v Carpenter*, No 16-402, *27 (US filed Sept 25, 2017) (available on Westlaw at 2017 WL 4311113) ("*Carpenter* US Brief") (discussing device-to-device calling and wi-fi calling, neither of which creates CSLI). See, for example, Tom Simonite, *Future Smartphones Won't Need Cell Towers to Connect* (MIT Tech Rev, Sept 29, 2014), archived at https://perma.cc/HH7T-HZY8 (discussing device-to-device direct connections for shorter-distance data connections).

[127] *Carpenter*, 138 S Ct at 2219, citing Brief for Amici Curiae Electronic Frontier Foundation et al, *United States v Carpenter*, No 16-402, *12 (US filed Aug 14, 2017) (available on Westlaw at 2017 WL 4512266) ("*Carpenter* EFF Amici Brief"). This claim of precision depends on the distance between cell towers. For example, see Phil Locke, *Cell Tower Triangulation—How It Works* (Wrongful Conviction Blog, June 1, 2012), archived at https://perma.cc/R8FK-FYUT (concluding from triangulation modeling "it is possible to determine a phone location to within an area of 'about' ¾ square mile[s]").

[128] For example, the amicus brief the Court cited for this capability in turn cites congressional testimony that describes the process but says only that any use or recording of such data depends on individual carriers' policies, which are not described. *Carpenter* EFF Amici Brief at *11 & n 24 (cited in note 127).

[129] Craig Silliman, *Technology and Shifting Privacy Expectations (Perspective)* (Bloomberg Law, Oct 7, 2016), archived at https://perma.cc/N8N4-XJV5; see also Tom Jackman, *Experts Say Law Enforcement's Use of Cellphone Records Can Be Inaccurate* (Wash Post, June 27, 2014), archived at https://perma.cc/8PU6-2F9B (observing "phone companies do not save GPS or triangulation for an individual phone").

when carriers will find business reasons to record and store more precise location records for long periods of time.[130]

2. *Frequency of recorded connections.* The records in this case showed Carpenter's phone connections only when he made or received phone calls.[131] Admittedly, Carpenter apparently breathed through his phone, making or receiving enough calls to average 101 recorded connections per day[132]—well above average.[133]

Chief Justice Roberts characterized Carpenter's monitoring as far more continuous, claiming that his carriers recorded his cell-tower and sector usage "[e]ach time the phone connects to a cell site."[134] This parrots Carpenter's and his amici's non-record-based (and hence not adversarially tested) assertions that "in recent years phone companies have also collected location information from the transmission of text messages and routine data connections."[135] "Collected," perhaps; but the sources cited in Carpenter's and supportive amici briefs do not connect the dots all the way to long-term *storage* that would

---

[130] See Henderson, 26 Wm & Mary Bill of Rts J at 498 n 19 (cited in note 119) ("But such a precise location [using triangulation and signal strength] will typically not be calculated, let alone recorded in records later received by law enforcement, at least not based upon current business practices.").

An online search for recent federal or state decisions indicating that the government had requested and received historical CSLI data reflecting such triangulation technology reveals none. A few courts discuss such technology only to clarify that the produced records did not include any pinpoint location data. See, for example, *Zanders v State*, 73 NE3d 178, 182 (Ind 2017) (discussing triangulation and other technologies but noting that no "high-resolution location data" were involved in case); *Commonwealth v Augustine*, 4 NE3d 846, 855 (Mass 2014) (same). Agents sometimes request triangulation to assist with prospective or "real-time" CSLI tracking. See, for example, *United States v Alarcon*, 2016 WL 2844164, *1 (D Minn).

[131] That's all the government asked for. See *Carpenter*, 138 S Ct at 2212; *Carpenter* US Brief at *7 (cited in note 126) ("The records . . . did not contain any cell-site information for text messages or for times when petitioner's phone was turned on but was not being used to connect a call."). And indeed that's all Sprint and MetroPCS recorded. Id.

[132] *Carpenter*, 138 S Ct at 2212.

[133] A year earlier the average was ten connections per day (five calls). See Amanda Lenhart, *Cell Phones and American Adults* (Pew Research Center, Sept 2, 2010), archived at https://perma.cc/DSM6-XXMH.

[134] *Carpenter*, 138 S Ct at 2211; id at 2212 (repeated almost verbatim). The Court attributed this claim to FBI Agent Hess's trial testimony, id at 2212, and yet Hess was crystal clear that by "connection" he meant only actively making or receiving phone calls. *Carpenter* Appendix at *61 (cited in note 120) (testimony of Agent Hess) ("Q: So if the phone is just in my pocket, and I'm not calling and no one is calling me, you couldn't really do this? A: Right. It's not populated in the call detail records. Q: Even though it might be communicating in there, — A: That's correct.").

[135] *Carpenter*, 138 S Ct at 2212.

produce records covering "every moment of every day for five years."[136]

This projection of continuous long-term CSLI monitoring is, at a minimum, overconfident. It will probably soon be true for some people at some times in some places; but it is generally still quite a way off.

3. *What can CSLI reveal?* Location data threaten privacy to the extent an observer can (1) compare tower service areas with local maps and (2) determine what places the target visited and how long she stayed there and then (3) infer what she might have been doing there and why.[137] The Court warned that, "[a]s with GPS information, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'"[138] But this GPS comparison exaggerates the capacity for (2) and (3) above. On this record, the typical service area for Carpenter's CSLI "contains about 1000 buildings."[139] Cut that in half—indeed, cut it in hundreds—it's still hard to infer these details with any confidence. So current or even near-future projected CSLI records cannot easily determine the kinds of personal associations about which the Court expressed worry, at least not without significant nonlocation data obtained elsewhere.[140]

That said, there is no question that current CSLI can be used to infer with reasonable confidence *some* sensitive facts. For example, even imprecise data can reveal whether the target visits the same general locations repeatedly, or not. And imprecise data can indicate where a cell phone is *not* (not near one's workplace during the day,

---

[136] Id at 2218.

[137] The Court rhetorically embellishes the capacity to infer by repeatedly describing CSLI location monitoring as "surveillance." See, for example, *Carpenter*, 138 S Ct at 2217–18. That term implies "being watched," as if CSLI can determine not just *where* you are located (however precisely), but also *what* you are doing and *with whom*, as opposed to leaving this to inference. Of course, that is not what the data show.

[138] Id at 2217, quoting *Jones*, 565 US at 415 (Sotomayor, J, concurring).

[139] *Carpenter* US Brief at *25 (cited in note 126).

[140] For example, while the ACLU claimed before the Sixth Circuit that Carpenter's cell phone records placed him at church at a particular time, that claim was based partly on information Carpenter himself provided rather than only on the records themselves. See *Carpenter* 6th Cir Brief at 33 n 4. Without such additional information, CSLI data "does not paint the 'intimate portrait of personal, social, religious, medical, and other activities and interactions'" that Carpenter claims. *United States v Davis*, 785 F3d 498, 515 (11th Cir 2015) (en banc) (citation omitted).

not near one's home all night). Moreover, the Court may appropriately worry about current trends. Surely the Court correctly concluded that CSLI "has afforded law enforcement a powerful new tool" that "*risks* Government encroachment of the sort the Framers . . . drafted the Fourth Amendment to prevent."[141]

4. *Record, reality, and ruling for the future.* Given clear trends and risks, why did Chief Justice Roberts apparently feel a need to embellish CSLI's actual level of intrusion, both in terms of precision and continuity? Perhaps for two reasons.

First, the aggressive depiction of CSLI tracking suggests a regulatory approach to privacy doctrine, reflecting a desire to cabin worrisome surveillance even before the technology reaches highly invasive levels. Given the typical time lag between the development/deployment of new privacy-threatening technology and judicial (especially Supreme Court) review, law enforcement activities might well impinge upon should-be-protected privacy interests for quite some time before courts confined to actual record-based threats catch up.[142] The desire to forestall a "'too permeating police surveillance'"[143] heralds an increasingly regulatory approach to modern surveillance threats, leading the Court to anticipate protections required for atomistic privacy values.

To be sure, the Court does not always rule forward in this manner.[144] Hesitation in the face of technology lag may reflect hope that

---

[141] *Carpenter*, 138 S Ct at 2223 (emphasis added). The far greater risk here involves a myriad and growing number of cell phone applications whose operators collect phone users' location information, sometimes to deliver tailored services (such as local weather news or driving directions) but oftentimes just to collect the information so they can sell it en masse to companies for commercial purposes (such as to provide businesses and advertisers with clues about consumer behavior). Again it's not clear that the app operators store the information in user-identifiable form; rather, the data are typically anonymized before bulk resale. But in some cases a dedicated analyst, once armed with a lot of other facts about particular people's movements and location patterns, can reverse-engineer educated guesses as to which individuals actually made which tracked movements. These apps frequently track location through GPS coordinates, far more precise than CSLI. See, for example, Jennifer Valentino-DeVries et al, *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret* (NYT, Dec 10, 2018), archived at https://perma.cc/98FB-KTXZ (discussing practices and providing examples). Of course, while not necessarily easy to do, users can adjust their cell phone settings to disable the location services that enable such tracking, either wholesale or piecemeal and either indefinitely or for particular periods of time. Id.

[142] See, for example, Neil Richards, *The Third-Party Doctrine and the Future of the Cloud*, 94 Wash U L Rev 1441, 1448, 1464–65 (2017) (describing and applying the "Fourth Amendment lag problem" to digital data and related technology).

[143] *Carpenter*, 138 S Ct at 2214 (citation omitted).

[144] See, for example, *Maryland v King*, 569 US 435, 464 (2013) (joined by Roberts, CJ) (refusing to consider future improvements in DNA testing that might further compromise

legislative bodies, arguably better suited to project and regulate for the future, will step up.[145] But given the conjectured technology growth curve and no congressional action in sight, the Court may reasonably have thought the time to intervene was now.

Of course, Chief Justice Roberts could have candidly recognized that both the monitoring to which Carpenter was actually subjected and the most common location monitoring available today remain quite imprecise and episodic compared to GPS-level tracking, and yet still expressed concern for doctrinal time lag as a reason to rule forward by modifying doctrine prophylactically. Lack of candor comes with a cost; the Court's exaggerated claims will likely be accepted at face value by lower courts, and the underlying technological reality will continue to escape judicial scrutiny.[146]

But here lies the second possible motive for embellishment. The more precise and continuous the Court depicts CSLI tracking, the easier it is to claim both that it violates reasonable expectations of privacy, and that it is distinguishable from more conventional surveillance techniques and other types of third-party records. Let's now see how strong those claims are.

B. A MOSAIC PRIVACY INTEREST IN THE "WHOLE OF ONE'S PUBLIC MOVEMENTS"

Given this futuristic description of CSLI data, the Court easily found that historical location monitoring implicates a *Katz*-based privacy interest. The more difficult question is whether that interest dissipates because the phone user shares his location information, either with the public around him or with Sprint.

---

privacy, despite acknowledging that "science can always progress further, and those progressions may have Fourth Amendment consequences"); *Silverman v United States*, 365 US 505, 508–9 (1961) (refusing to consider "recent and projected developments in the science of electronics" despite foreseeable "Fourth Amendment implications of these and other frightening paraphernalia").

[145] See, for example, Jeffrey S. Sutton, *Courts, Rights, and New Technology: Judging in an Ever-Changing World*, 8 NYU J L & Lib 261, 274–75 (2014) (although "courts have no license to abdicate their duty to enforce constitutional guarantees based on the complexities of new technology," there are virtues associated with deferring to (and presumably encouraging) legislative intervention).

[146] See, for example, *United States v Curtis*, 901 F3d 846, 847 (7th Cir 2018) (accepting without question that CSLI "is capable of 'pinpoint[ing] a phone's location within 50 meters' " and carriers "can collect CSLI as frequently as several times a minute"), quoting and then citing *Carpenter*, 138 S Ct at 2219, 2211–12.

The "public exposure" doctrine holds that people lack a reasonable expectation of privacy in movements or activities that they publicly expose to "anyone who wants to look."[147] The majority in *Carpenter*, however, embraced a form of the mosaic approach championed by the shadow majority of concurring Justices in *Jones*, and announced that heretofore "individuals have a reasonable expectation of privacy in the *whole of their physical movements*."[148] In other words, while *each* public movement may be exposed and hence unprotected by *Katz*, the *aggregate* of such movements may qualify for Fourth Amendment protection. Given that "[t]he sum of an infinite number of zero-value parts is also zero,"[149] how did the Court add this up?

First, Chief Justice Roberts redefined the question. Rather than follow *Katz* and *Knotts* by asking whether public sojourners reasonably expect they are exposing their *discrete* movements to *any* one, meaning to different people at different places and times,[150] the Court in *Carpenter* asked whether the sojourners reasonably expect they are exposing their *entire set* of movements to any *one*, meaning to a single person who sees it all. The question shifted from what bits and pieces of information the sojourners knowingly reveal to random people, to what they might expect a single-but-dedicated viewer to learn from what they reveal.

And the Court answered "not so much." Personal surveillance by law enforcement or private tails using only conventional tools and techniques is both difficult and costly. As a result, people reasonably expect that "law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an [individual] for a very long period."[151] So, while people do not reasonably expect privacy in any *discrete* movement (or perhaps a short series of movements), people do reasonably expect that no one is systematically viewing the "whole" of

---

[147] See text accompanying notes 38–40.

[148] *Carpenter*, 138 S Ct at 2217 (emphasis added).

[149] *United States v Jones*, 625 F3d 766, 769 (DC Cir 2010) (Sentelle dissenting from denial of rehearing en banc).

[150] See *Katz*, 389 US at 351 (exposure to "public"); id at 361 (Harlan, J, concurring) (exposure to "outsiders"); *Knotts*, 468 US at 281 (exposure to "anyone who wanted to look").

[151] *Carpenter*, 138 S Ct at 2217, quoting *Jones*, 565 US at 430 (Alito, J, concurring in the judgment).

their physical movements over any extended period of time.[152] Even for the police, this is wildly inefficient except in extraordinary circumstances.

Second, Roberts emphasized the potential sensitivity of location information. Knowing *all* of someone's movements, a dedicated viewer might be able to construct a "mosaic" of discrete data points from which to infer things about the sojourner that society reasonably believes she should be able to keep to herself—such as her "'familial, political, professional, religious, and sexual associations.'"[153]

Third, Roberts highlighted how easily government can leverage Sprint's CSLI-based monitoring powers. Compared to both "nosy neighbors" and government agents using traditional surveillance techniques, Sprint is a potentially super-powerful tracker due to features of CSLI technology. After all, "[c]ell phone tracking" by the government "is remarkably easy, cheap, and efficient"[154] because Sprint has already done the work. Moreover, the ability to search stored records "gives police access to a category of information otherwise unknowable."[155] Normally, agents can surveil targets only from the moment of suspicion and going forward; stored CSLI data let agents "travel back in time to retrace a person's whereabouts."[156] Although police can always interview eyewitnesses about a suspect's prior movements, such efforts are limited by "the frailties of recollection,"[157] whereas Sprint's memory is "nearly infallible."[158] Another consideration, unmentioned by the Court, is that agents seeking to reconstruct someone's prior movements may have a hard time figuring out who might be plausible human eyewitnesses to interview, but the agents can easily consult the universe of plausibly "witnessing" service providers. In sum, government access to Sprint's records will almost assuredly reveal a more comprehensive and accurate story of the target's movements than whatever can likely be pieced together

---

[152] *Carpenter*, 138 S Ct at 2217.

[153] Id, quoting *Jones*, 565 US at 415 (Sotomayor, J, concurring).

[154] *Carpenter*, 138 S Ct at 2217–18; see also id at 2218 (asserting government can access CSLI "at practically no expense").

[155] Id.

[156] Id.

[157] Id.

[158] *Carpenter*, 138 S Ct at 2219.

through more traditional investigative efforts—precisely why the government wants such access.

The Court's first-ever embrace of a mosaic-defined search has been roundly praised by privacy advocates clamoring for change, and it is truly a significant doctrinal shift. And perhaps not surprisingly, as an initial step in a novel direction, the majority opinion is under-theorized, or at least underexplained. Most fundamentally, the Court did not address or resolve the long-standing conceptual ambiguity underlying *Katz* that so frustrated the dissents. Does the mosaic test assess *empirical* expectations—suggesting that when I walk down the street, I don't *predict* that a single person will see my entire route even though I do predict that lots of different people may collectively see every single step along the way? Or does the test reflect a *normative* standard—suggesting that I *shouldn't assume the risk* that any one person will see the entire route (thereby potentially learning something about my familial/political/professional/religious/sexual affiliations or proclivities), even though I assume the risk that each step is discretely revealed? Nor did the Court clarify an ambiguity raised by *Jones*'s separate opinions by specifying the baseline against which it measures how much monitoring information—whether assessed empirically or normatively—is too much. Is the mosaic-triggered privacy interest invaded when I am monitored for a longer period than I (would or should) expect to be seen by law enforcement officers trying to surveil me; or for a longer period than I (would or should) expect to be seen by a single "nosy neighbor"?[159] Perhaps we will learn more as the doctrine unfolds; but the Court may leave well enough alone,

---

[159] Rather than pick one baseline, the Court referred to both: society expects that "law enforcement agents *and* others would not" and could not monitor the target's entire journey. Id at 2217 (emphasis added). But whether viewed empirically or normatively, these baselines might be quite different. Orin Kerr, for example, traces the law enforcement baseline to Justice Alito in *Jones*, traces the private "others" baseline to the court of appeals in that case, traces yet a third baseline (when the government can learn intimate details "more or less at will") to Justice Sotomayor in *Jones*, notes that the approaches are materially different, and further pinpoints ambiguities within each formulation. Kerr, 111 Mich L Rev at 330–31 (cited in note 50). By acting as if the *Jones* shadow majority had already established the "whole of one's public movements" principle, the *Carpenter* Court avoided the need to explain its views further.

The approach previously espoused by Justice Alito in *Jones*, employing a what-would-law-enforcement-do-through-traditional-surveillance baseline, might hinge (empirical or normative) expectations to the crime being investigated. He ponders whether the more serious the offense, the longer and more intense surveillance would/should be expected. *Jones*, 565 US at 431 (Alito, J, concurring in the judgment). This would add another conceptual trick. The Fourth Amendment protects innocent people too, but how can one of them possibly speculate

sidestepping these underlying questions as it has done with *Katz* for decades.[160]

The mosaic approach, by its very nature, invites line-drawing to distinguish location monitoring that reveals the "whole of one's public movements" from monitoring that merely reveals discrete "publicly exposed" movements unprotected under *Knotts*. The rationale for mosaic-based protection does not justify covering shorter-term CSLI requests. The fewer location data points available, the harder it is to discern patterns or sequences and therefore to infer particular activities, and the more likely it is the target could reasonably expect (empirically and normatively) to be personally viewed throughout that period.[161]

As with other doctrinal questions that hinge on aggregated events or the passage of time (for example, how long may a nonwarrant arrestee be detained prior to a judicial probable cause determination[162]), the Court must establish some cut-off point for when *Knotts*-approved monitoring ends and search-triggering monitoring begins. In *Carpenter*, the Court proclaimed that "accessing seven days of CSLI constitutes a Fourth Amendment search," leaving for another

about how long she would/should expect to be surveilled if she needs to know the severity of an offense she did not commit?

Throughout this discussion the Court also implicitly evinced little care for *Katz*'s "subjective expectation of privacy" component. The Court concluded that Carpenter did not truly expose his long-term location information in the relevant sense; but the Court seemed entirely uninterested in whether Carpenter manifested any intent to keep to himself the underlying kinds of information the Court worried his movements will reveal. For all we know, Carpenter was quite open about his family relations, political views, professional associations, religious views and practices, and sexual interests—perhaps all revealed through his Facebook postings and personal attire (such as wearing a cross or yarmulke, rainbow pin, and gang colors). See generally Orin S. Kerr, *Katz Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U Chi L Rev 113 (2015) (observing demise of subjective test).

[160] That said, the obvious difficulties applying the empirical baseline to any specific instance of long-term monitoring, see *United States v Cuevas-Perez*, 640 F3d 272, 282–83 (7th Cir 2011) (Flaum concurring) (concluding "probabilistic" mosaic approach is "unworkable"), coupled with the Court's not doing so here, strongly suggests the *Carpenter* majority is thinking in normative terms.

[161] As Justice Alito concluded in *Jones*, "relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable." 565 US at 430 (Alito, J, concurring in the judgment). Even Justice Sotomayor, who in *Jones* flagged her concern about "short-term" as well as "longer term" GPS monitoring, id at 415–17 (Sotomayor, J, concurring), still recognized that only "aggregated" records of movements could generate privacy-threatening inferences. Id at 416; see also id at 415 (expressing concern over "comprehensive record of a person's public movements"); id at 416 (expressing concern over "substantial quantum of intimate information").

[162] See *Riverside v McLaughlin*, 500 US 44 (1991) (imposing presumptive forty-eight-hour limit to detention before postarrest probable cause hearing).

day whether government may obtain historical CSLI for a shorter period "free from Fourth Amendment scrutiny, and if so, how long that period might be."[163] One could imagine the Court ultimately embracing a broad prophylactic rule that *any* CLSI request constitutes a search, in part to avoid the appearance of drawing arbitrary lines.[164] I anticipate, however, that the Court will maintain some cut-off point—likely a week, but at least a day or two—both to reflect the underlying mosaic-based justification and, as described below, to balance privacy with law enforcement interests.[165]

Of course, any such cut-off point raises further line-drawing issues as well—some raised by many duration-defined doctrines,[166] but others tailored to the novelty of applying a mosaic approach to law enforcement. Traditionally, courts have looked at a discrete interaction between police and a person or tetrad object and asked

---

[163] *Carpenter*, 138 S Ct at 2217 n 3. The Court apparently focused on a week because the shorter of the two records requests was for a week's worth of data. See id. The Court did not address Justice Gorsuch's poke that Sprint provided only two days of records (because Carpenter's trip to Ohio that triggered roaming was brief) and his query why the search should be measured by the information requested rather than the information actually acquired. See id at 2266–67 (Gorsuch, J, dissenting).

[164] The Court could have also reached this point through a different route, ruling that any CSLI is too much based on a concern about tracking targets in private homes. In *United States v Karo*, 468 US 705 (1984), the Court cabined *Knotts* and held that location monitoring becomes a search when it fixes the target in a private residence such that the government learns "a critical fact about the interior of the premises that the Government . . . could not have otherwise obtained without a warrant." Id at 715. If the Court doubled down on its claim of GPS-like precision, CSLI could suggest that the target entered a home. Because officials would have no way of predicting that in advance, the records might contain some Fourth Amendment–protected as well as some publicly exposed data points. See *Tracey v Florida*, 152 So3d 504, 524 (2014). To be sure, the Court in *Karo* held the public data pings admissible while suppressing the private pings. But on those different facts it was easy to separate the two; here it might be very difficult. Moreover, a broader prophylactic rule would better protect targets who never become criminal defendants.

[165] See text accompanying note 266. Requiring a warrant for short-term CSLI monitoring might hinder criminal investigations much more severely than requiring a warrant only for long-term monitoring.

The non-search status for short-term historical monitoring should also apply to short-term tracking deployed to locate a target in real time. Such tracking might aid law enforcement in arresting her, or rescuing a kidnapping victim, or even providing an alibi for a recent crime. But a short sequence of location fixes (whether through cell tower usage or GPS pings) hardly seems sufficient to lay bare her "privacies of life" by revealing the "whole" of her public movements.

[166] For example, consider remedies. Agents do not search me when they obtain six consecutive days of Sprint's CSLI records for my phone, but they search you when they obtain seven consecutive days. Is your exclusionary rule remedy suppressing records for all seven days, or only the seventh (or perhaps only the first, or only one day of your choice, or of the government's choice)? Is your civil remedy damages for one day or one week of illegal searching? Put differently, have you suffered a single indivisible illegal search, or a legal search for six days and an illegal one for the seventh?

whether that interaction constitutes a Fourth Amendment search. Here, we're left wondering whether that's still true (such that only a single long-term records request from a single third party can create a search-triggering mosaic), or whether a search can be produced by the aggregation of different enforcement activities across time, motives, sovereigns, technologies, etc. For example, suppose Agent Amy requests five days of Sprint's records for your phone. When, if at all, may Agent Barb later ask Sprint for the next three days? Never? Only after a certain amount of time has elapsed? Only when investigating a different crime? Only if Agent Barb represents a different law enforcement agency, or even a different sovereign? And what if two different third-party carriers are involved: suppose given your movements and roaming your phone connects to Sprint towers for four consecutive days and then MetroPCS towers for the next four. Agent Carol requests these four-day series of records from both Sprint and MetroPCS. Both carriers have been searched;[167] have you?[168]

An atomistic view of mosaic theory supports aggregating all of these various information requests for the purpose of defining a search—from your perspective, you don't care whether your nosy neighbor or the police have pieced together the privacy-threatening mosaic from one long stare or many momentary glances. But that means that whether Agent Esther searches you may depend on the completely independent and even then-unknown interactions between many other agents and many other third parties. That's conceptually unsettling, to say the least, let alone a pragmatic quagmire both for officers trying to comply with the Fourth Amendment and for courts trying to sort things through after the fact. I suspect here again that a regulatory perspective will win the day, with the

---

[167] Though subject only to the much relaxed standard for document subpoenas. See text accompanying notes 281–82.

[168] To press the point even further, consider aggregating requests for different kinds of third-party records. For a week-long period, Agent Darcy requests records revealing some of your credit card purchases, some swipes of your building entrance passkey, some passages on toll roads, and some internet protocol addresses, and then she views some surveillance tapes from near your house and office—all of which directly or incidentally reveal timed location information, and which collectively add up to 101 data points per day to match Carpenter's prolific phone use. Now all of those third parties have been searched; again, have you?

For other pragmatic challenges posed by mosaic-required line drawing, see Kerr, 111 Mich L Rev at 328–43, 346–48, 330–31 (cited in note 50); Lucas Issacharoff and Kyle Wirshba, *Restoring Reason to the Third Party Doctrine*, 100 Minn L Rev 987, 1003 (2016) (concluding that mosaic theory "works better as a metaphor than as a constitutional doctrine" due to "impracticality as an administrable standard").

Court favoring easier-to-implement bright-line rules over harder-to-measure-and-enforce aggregation rules, even though the latter more directly track atomistic and mosaic-defined privacy concerns.

c. modifying the miller-smith third-party doctrine to protect csli records

So Carpenter's legitimate claim to privacy in the whole of his public movements overcame *Katz*'s caveat about publicly exposed activities. But he still faced the third-party doctrine's independent caveat that "'a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties'" even just "'for a limited purpose,'"[169] and therefore acquiring such information is not a Fourth Amendment search.

As noted earlier, the *Miller-Smith* mantra that voluntary sharing automatically defeases privacy has been criticized by scholars on a wide variety of grounds,[170] some echoed by Justice Gorsuch's dissent.[171] As an empirical statement of the expectations people generally hold, the doctrine is "quite dubious";[172] surely at least sometimes we expect people or even companies to keep our shared private information to themselves.[173] And as a normative statement of when people are entitled to expect postsharing privacy, "the notion that the answer might be 'never' seems a pretty unattractive societal prescription."[174] Scholars have proposed many different rules to determine

---

[169] *Carpenter*, 138 S Ct at 2216, quoting *Smith*, 442 US at 743–44, and then *Miller*, 425 US at 443.

[170] For a small subset of voluminous critical commentary, see Kerr, 107 Mich L Rev at 563 n 5 (cited in note 104) (collecting sources criticizing the doctrine); Jane Bambauer, *Other People's Papers*, 94 Tex L Rev 205, 208 & n 18 and 214–15 nn 50–51 (2015) (criticizing doctrine and collecting sources).

[171] *Carpenter*, 138 S Ct at 2262–63 (Gorsuch, J, dissenting).

[172] Id at 2263 (Gorsuch, J, dissenting), quoting Baude and Stern, 129 Harv L Rev at 1872 (cited in note 105); see also Kugler and Strahilevitz, 2015 Supreme Court Review at 255 (cited in note 49) (explaining survey data indicate third-party doctrine holds disproportionate appeal to older Americans and has an "apparent lack of resonance with younger Americans").

[173] Context matters: if I tell a friend funny stories about my addiction to college football, I'd generally expect her (absent special admonition) to share them with whomever she sees fit; but if I tell her painful stories about emotional anxieties, I'd generally expect her to keep quiet or perhaps share only with her spouse. And the down-the-line recipient matters: if I confess suicidal thoughts, I'd expect my friend to keep quiet if I insist or perhaps reveal them to my wife or an appropriate caretaker, but not reveal them to my students or my young children.

[174] *Carpenter*, 138 S Ct at 2263 (Gorsuch, J, dissenting); see id at 2262–64 (canvassing and critiquing application of various assumption-of-risk norms). When the Court acknowledged

when sharing does not extinguish privacy interests.[175] Whatever the best approach,[176] it is difficult to rally around a simplistic, binary answer—other than for the sake of being simplistic and binary.[177] While voluntarily sharing "objects, activities, or statements" with others may *sometimes* extinguish privacy interests under *Katz* because "no intention to keep them to himself has been exhibited,"[178] the properly nuanced question is when and why.

In *Carpenter*, Chief Justice Roberts did not accept Justice Sotomayor's suggestion in *Jones* that the Court "reconsider" the entire third-party doctrine as being "ill-suited to the digital age."[179] But Roberts confidently announced that the Court "decline[d] to *extend Smith* and *Miller* to cover these novel circumstances" and that the information's possession by a third party "does not by itself overcome" the user's Fourth Amendment claim.[180] Roberts offered two reasons not to apply the third-party doctrine to CSLI: the information revealed was both highly sensitive and not truly shared volun-

---

in *Katz* that a person cannot claim Fourth Amendment protection for things she "knowingly exposes to the public," 389 US at 351, the Court may well have considered only remarks/activities shared with natural persons, including both any intended recipients of the remarks or viewers of the activities, and also any inadvertent hearers or viewers in a private home or public space such as a park or restaurant. When nine years later *Miller* extrapolated this assumption of risk to encompass information exposed to business entities, changed membership may have made the Court less attuned to privacy interests (though Justices Stewart and White were in the majority for both decisions).

[175] For example, sharing with a company via automated processes where the information is not typically monitored by people, sharing with a person or company who is an "information fiduciary" owing an obligation of silence, sharing information that is particularly sensitive, sharing information for clearly limited purposes, and more. See, for example, Susan Brenner and Leo Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J L & Pol 211, 215–16 (2006) (sharing should not trigger third-party doctrine if customer has broadly defined "trust-based" relationship and a confidentiality agreement with the third party and if the data are maintained at least in part for and are accessible by the customer).

[176] I'm inclined to frame the question this way: if you share information A with person B under circumstances C, do you have a right to complain if B shares your information with person D under circumstances E? That is more a normative than empirical inquiry, though empirics about observed social norms play a role. Borrowing an example from my colleague Don Herzog, I suspect it is pretty unusual for a stranger to poke around in the garbage I place on the curb for pickup, and I would think it quite weird if one did so; but I also think I couldn't persuasively *complain* that she violated my right of privacy.

[177] And as Justice Gorsuch notes, privacy "always wins" is just as clear as "always loses." *Carpenter*, 138 S Ct at 2264 (Gorsuch, J, dissenting).

[178] *Katz*, 389 US at 361 (Harlan, J, concurring).

[179] *Jones*, 565 US at 417 (Sotomayor, J, concurring); id at 418 (suggesting doctrine should "cease[ ] to treat secrecy as a prerequisite for privacy").

[180] *Carpenter*, 138 S Ct at 2217 (emphasis added).

tarily. Because the latter is more traditional terrain, I will address that argument first.

1. *Protecting involuntarily shared information.* The Court offered two seemingly simple reasons why Carpenter cannot reasonably be said to have "voluntarily" shared his location information with Sprint. But neither the reasons nor their analytical roles are as simple as they first appear.

Here are the Court's two arguments in their entirety as to why "[c]ell phone location information is not truly 'shared' as one normally understands the term."[181] First, what I will call the macro-involuntary argument: "cell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society."[182] And, second, what I will call the micro-involuntary argument:

> [A] cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up. Virtually any activity on the phone generates CSLI, including incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates. Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data.[183]

Thus, Roberts reasoned, "in no meaningful sense does the user voluntarily 'assume[ ] the risk' of turning over a comprehensive dossier of his physical movements."[184]

The macro-involuntary argument says everyone needs a cell phone today. Because you need to use your phone, doing so ought not be viewed as a volitional act that "voluntarily" shares the information required to make the phone work.

This is a normative rather than factual claim. The Court cannot mean that using a cell phone is *literally* indispensable to modern life; until quite recently we managed to survive without one. That said, smartphones surely make negotiating daily activities significantly easier, more efficient, more fun, and even safer for all the obvious reasons—constant communicability, easier information retrieval,

---

[181] Id at 2220.

[182] Id, quoting *Riley v California*, 134 S Ct 2473, 2484 (2014).

[183] *Carpenter*, 138 S Ct at 2220.

[184] Id at 2220, quoting *Smith*, 442 US at 745.

faster driving directions, instant Starbucks gratification, and the like. The Court makes a normative judgment that a cell phone's important and convenient functions are so compelling today that we act *as if* we have no real choice, despite the downside of enabling location monitoring. Frankly, I act that way too: I carry my phone everywhere I go, as long as my teenage daughters are around to remind me how to use it. As a matter of social reality, the Court's judgment strikes me as reasonable.[185]

That said, I think the dissents in *Miller* and *Smith* were equally reasonable in claiming that people must use banks and landlines.[186] The Court in *Carpenter* offered no reason to distinguish among these arguable imperatives of daily life, nor thoughts on the comparative societal necessity of using credit cards, computers, cars, or cardiologists. So whether the macro-involuntary argument implicates any of these core features of modern living is not yet clear.

Perhaps the Court's micro-involuntary argument distinguishes CSLI from the rest: cell phones constantly communicate your location "without any affirmative act on the part of the user beyond powering up."[187] The point, I gather, is that you can't effectively self-regulate to control when or whether you share your location, without turning your phone off. If the Court's view is that its macro- and micro-level arguments *together* distinguish *Miller-Smith* (and other third-party digital data), that's probably right. You volitionally provide documents to (or today establish internet connections with) your bank, you dial phones, you swipe or hand over credit cards, you confide in your cardiologist, etc. Maybe some background computer func-

---

[185] Though the conclusion that we all need our cell phones also strikes me as for-this-train-only; somehow I doubt the Court will now conclude that all service-provider agreements are contracts of adhesion.

[186] See *Miller*, 425 US at 451 (Brennan, J, dissenting) ("[I]t is impossible to participate in the economic life of contemporary society without maintaining a bank account.") (citation omitted); *Smith*, 442 US at 750 (Marshall, J, dissenting) (claiming that using landline phones "for many has become a personal or professional necessity" and "individuals have no realistic alternative"); see also *Carpenter*, 138 S Ct at 2233 (Kennedy, J, dissenting) ("[T]he decision whether to transact with banks and credit card companies is no more or less voluntary than the decision whether to use a cell phone.").

Of course, there were alternative ways to keep some specific transactions private in the 1970s; you could pay for your mistress's abortion using cash or a traveler's check, and schedule that abortion from the corner payphone. Similarly, for discrete and highly sensitive trips today, you can temporarily place your phone in airplane mode.

[187] *Carpenter*, 138 S Ct at 2220. Again, this assumes, outside the record, that carriers routinely record such data exchanges other than incoming and outgoing phone calls (which clearly require affirmative acts).

tions and car black-box communications are equally automated, but perhaps even they fail the micro-involuntary test because, unlike phone connections, you intentionally turn on your laptops and start your cars before you use them.

But it is not clear that the Court intends to exclude from the third-party doctrine only technologies that are *both* socially necessary and automated. The two exceptions don't fit well together. If you have no (socially realistic) choice but to use a cell phone that lets your carrier track your location, why should the Court additionally insist for Fourth Amendment protection that the device transmits information automatically? It seems odd to conclude that you still voluntarily share your location for third-party doctrine purposes even when you intentionally place a call knowing that doing so triggers a record, when your making such phone calls "is indispensable" to modern living.

Alternatively, perhaps the Court views its macro- and micro-involuntary arguments as separately sufficient (rather than jointly necessary) to exempt technology from the *Miller-Smith* rule. Understood this way, you would waive your reasonable expectation of privacy only if you *both* enjoyed and exercised a real choice to use a cell phone in the first place, *and* did something volitional each time that your phone generates CSLI. This alternative reading is far more privacy-protective, further narrowing the sharing exception to *Katz*. But as noted above, it raises questions about the continuing vitality of *Miller* and *Smith* themselves given the realistic need to use banks and phones.[188]

---

[188] Consider this four-square comparison, which for the sake of illustration assumes that credit cards are "indispensable" for modern living but Fitbit health monitors and voice-activated TVs are not.

	micro-level = automatic data sharing	**micro-level = volitional data sharing**
macro-level ➜ use is necessary	(1) CSLI	(2) using credit cards
macro-level ➜ use is discretionary	(3) Fitbit health monitors	(4) voice-activated TVs

If the macro- and micro-involuntary arguments are necessary conditions to avoid the third-party doctrine, then only (1) CSLI remains protected under *Katz*. If the macro- and micro-involuntary arguments are separately sufficient, then (1) CSLI, (2) credit cards, and (3) Fitbits all remain *Katz*-protected. Given the potential sizes of categories (2) and (3), that is a huge difference.

The Court didn't say what it means[189]—and, indeed, it's possible the Court had neither alternative in mind. Perhaps the Court intended only to make two arguments against voluntary sharing that carry the day for this particular technology, remaining open to different antisharing arguments for other technologies. Although we know that Carpenter didn't voluntarily share his location data with Sprint, we "do not know," as Justice Gorsuch surely grew tired of lamenting,[190] just how doctrine has changed to make this so. As is often the case when the Court marks out a new path, we await further direction.

2. *Protecting especially sensitive information.* The Court could have stopped right here: *Miller-Smith* does not apply because there was no voluntary sharing, period. Instead, the Court injected data sensitivity into the third-party equation. Actually, Chief Justice Roberts claimed that the doctrine already considers sensitivity:

> The third-party doctrine partly stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another. But the fact of "diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely." *Riley* [*v California*[191]]. *Smith* and *Miller*, after all, did not rely solely on the act of sharing. Instead, they considered "the nature of the particular documents sought" to determine whether "there is a legitimate 'expectation of privacy' concerning their contents." *Miller*, 425 U.S., at 442.[192]

But this claim is forced, quoting non-third-party cases out of context.[193] Rather, the Court has repeatedly explained that sharing in-

---

[189] The locution "In the first place, . . . Second, . . . As a result . . ." does not help. Id at 2220.

[190] Id at 2266, 2267, 2272 (Gorsuch, J, dissenting).

[191] 134 S Ct 2473, 2488 (2014).

[192] *Carpenter*, 138 S Ct at 2219 (majority). Some scholars agree that case law already reflects, if only implicitly, some emphasis on information sensitivity. See, for example, Michael Gentithes, *The End of Miller's Time: How Sensitivity Can Categorize Third Party Data After Carpenter*, 53 Ga L Rev *14–16 (forthcoming 2019), archived at https://perma.cc/6SYG-Q4TQ (referencing cases protecting communicative content, medical records, and hotel rooms). Current law aside, some scholars believe sensitivity should be considered going forward. See, for example, id at 24–25 (proposing new test should evaluate information on "sensitivity continuum" reflecting mosaic approach); Kugler and Strahilevitz, 2015 Supreme Court Review at 212 (cited in note 49) (advocating a *Katz* prong 1 focusing on general expectations of privacy, and a *Katz* prong 2 focusing on the sensitivity of the collected information, both measured in part by survey research).

[193] The quotation from *Riley* about "diminished" interests refers to arrestees rather than third-party records. And the Court's subsequent claim that *Jones* "already show[ed] special solicitude for location information in the third-party context" is equally misplaced, as *Jones* is likewise not a third-party records case. *Carpenter*, 138 S Ct at 2219.

formation completely extinguishes rather than merely diminishes privacy interests, as the dissenters pointed out[194] (and as Roberts, apparently inadvertently, recited elsewhere in his opinion[195]).

True, *Miller* looked at the "nature of the particular documents sought," but context shows it did so to determine whether the documents were shared with the bank, not whether they were especially sensitive.[196] In *Carpenter*, Roberts noted *Miller*'s caution that the "checks were 'not confidential communications but negotiable instruments to be used in commercial transactions.'"[197] But *Miller*'s point was that all of the information shared with the bank was *conveyed to the bank itself*, rather than kept "confidential" from the bank but conveyed to the bank so the bank could pass it along to another recipient (which apparently doesn't count as third-party sharing with the bank).[198]

The Court's claim that *Smith* considered sensitivity also overreads that decision. *Smith* did note the limited capabilities of a pen register,

---

[194] See id at 2226, 2232 (Kennedy, J, dissenting) (interpreting *Miller-Smith* as categorical rule); id at 2262, 2272 (Gorsuch, J, dissenting) (same).

[195] "We have previously held that 'a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.'" Id at 2216 (majority). That's not a novel characterization for the Chief Justice. See, for example, *Georgia v Randolph*, 547 US 103, 128 (2006) (Roberts, CJ, dissenting) ("If an individual shares information, papers, or places with another, he assumes the risk that the other person will in turn share access to that information or those papers or places with the government"—note no mention of sensitivity at all) (emphasis omitted).

[196] Here is the full quotation:

> [I]in *Katz* the Court also stressed that "[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection." We must examine the nature of the particular documents sought to be protected in order to determine whether there is a legitimate "expectation of privacy" concerning their contents.

Miller, 425 US at 442 (citation omitted).

[197] *Carpenter*, 138 S Ct at 2216, quoting *Miller*, 425 US at 442.

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

Recall that *Miller* was applying *Katz*, where the caller was *not* held to convey the content of his call to his phone company; rather, the company (like the postmaster for letters) was merely an intermediary tasked with passing the confidential communicative content to Katz's bookie. *Miller* just references, though distinguishes, the general rule that communicative content shared with intermediaries whose function is to pass the content to someone else (phone calls, letters, now e-mails) is not *shared with the intermediaries* in the way that triggers third-party waiver. See, for example, Wayne R. LaFave et al, 2 *Criminal Procedure* § 4.4(c) at 525 (West, 4th ed 2015).

and telephone call logs reveal little in the way of "identifying information."[199] But again the Court's language suggests that its point was to distinguish *Katz* and to show that the information revealed in call logs is information conveyed to the phone company, unlike communicative content for which the company is merely a transmitting intermediary. And the Court then concluded that Smith's privacy interest in the noncontent information was extinguished, not because it was nonsensitive, but because by making calls he "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business."[200]

Of course, in *Smith* the Court did not state that the third-party doctrine would apply to the caller's substantive message had the phone company created and stored a copy of that message after forwarding it to the caller's intended recipient. And while lower courts' subsequent decisions protecting various forms of communicative content typically invoke the just-described technical distinction between conveying to an intended recipient versus an intermediary,[201] those decisions might well reflect a sense that the Court would bend its brightly articulated line as necessary in order to maintain *Katz*-based protection for highly sensitive information such as personal communications. So perhaps lower courts' sensitivity to sensitivity quietly shaped the outer contours of *Miller-Smith* through the years. But even if so, Chief Justice Roberts in *Carpenter* unabashedly and explicitly injected a sensitivity analysis for the first time into what used to be described as an inquiry focused solely on voluntary exposure. Both the doctrine (at least substantially) and its articulation (quite clearly) have changed. As Justice Gorsuch put the point, we now have "*Katz*-squared."[202]

3. *Miller-Smith revised: but how?* How should courts square *Katz* in the future? The Court in *Carpenter* said there are two separate rationales underlying the third-party doctrine—lack of special sensitivity and voluntary exposure—and that CSLI triggers nei-

---

[199] *Carpenter*, 138 S Ct at 2219 (citation omitted).

[200] *Smith*, 442 US at 744.

[201] See, for example, *United States v Warshak*, 631 F3d 266, 288 (6th Cir 2010) (concluding e-mail content is protected because internet service provider transmitting content is "an *intermediary*, not the intended recipient of the emails").

[202] *Carpenter*, 138 S Ct at 2272 (Gorsuch, J, dissenting).

ther.[203] As with its involuntary arguments, however, the Court does not explain how the two rationales relate as part of the overall doctrine.

The Court might mean that the third-party doctrine applies when *either* of the two rationales is present. In other words, if highly sensitive information was voluntarily conveyed (think Fitbit health data), *or* if nonsensitive information was involuntarily shared (perhaps computer internet protocol addresses?), then the privacy interest dissipates. This reading fits with the Court's decision to address both variables, rather than to end its analysis after finding no voluntary sharing.

Or, the Court might mean that privacy dissipates only if *both* rationales apply, and the information is both voluntarily shared *and* nonsensitive. That seems perfectly logical too, though it seems less likely because it would mean that the third-party doctrine can *never* apply to sensitive information, no matter how clearly it was voluntarily shared (think of Carpenter posting his own location history on Facebook, or celebrities publishing tell-all memoirs).

And then there is a third possibility, raised and criticized by the dissents: an open-ended multifactor test. Justice Gorsuch, for example, lamented a "*second Katz*-like balancing inquiry, asking whether the fact of disclosure . . . outweighs privacy interests in the 'category of information' so disclosed."[204] Justice Kennedy also viewed the Court as announcing a balancing test that encompassed both privacy interests and CSLI tracking properties by "considering intimacy, comprehensiveness, expense, retrospectivity, and voluntariness."[205] Of course, the Court often articulates doctrine through multifactor tests, but Justice Kennedy feared that this one would particularly put "the law on a new and unstable foundation"[206] as lower courts would be left to figure out for themselves how the doctrinal variables relate when they address other surveillance technologies and types of digital data.

---

[203] Id at 2219–20 (majority).

[204] Id at 2267 (Gorsuch, J, dissenting) (emphasis in original).

[205] Id at 2234 (Kennedy, J, dissenting); see id at 2231 (the Court "establish[es] a balancing test" weighing "the privacy interests at stake" against "the fact that the information has been disclosed").

[206] *Carpenter*, 138 S Ct at 2234 (Kennedy, J, dissenting).

As Professor Anthony Amsterdam sagely admonished just before *Miller-Smith* emerged, scholarly critics should tread softly when the Supreme Court first steps onto an intuitively defensible but undertheorized new doctrinal path. Sometimes the Court recognizes that "the application of clear and consistent [existing] theories would produce unacceptable results" and a new direction is appropriate, even though the Court is not prepared to announce the new doctrine with the same level of specificity as the old doctrine, or to explain the extent to which the new doctrine displaces or can be accommodated with the old.[207] I am sympathetic to the Court's enterprise, even while recognizing the many unsatisfying aspects of its explanations. Unlike scholars, however, lower courts may not "take a sabbatical, or otherwise procrastinate till muddy waters clear";[208] they must now decide how to pave this new path while awaiting further blueprints.

D. LOCATION MONITORING EXCEPTIONALISM—OR DISMANTLING THE THIRD-PARTY DOCTRINE?

Privacy advocates hail *Carpenter* as heralding a broad Fourth Amendment reformation for the digital age. By recognizing new privacy interests and softening the third-party doctrine, they predict, hopefully, that the new approach will eventually constrain other intrusive technologies and protect other types of personal records.[209]

The decision itself, however, admits no such thing. Indeed, the Court's opinion suggests the opposite—that perhaps its privacy-protecting analysis covers CSLI and little else. Given "the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection,"[210] Chief Justice Roberts repeatedly claimed that long-term historical location information is "unique," "qualitatively different," a "world of difference" from *Miller* and *Smith*, and an "entirely different species"

---

[207] Amsterdam, 58 Minn L Rev at 351, 352 (cited in note 12).

[208] Id at 352.

[209] See, for example, Sharon Bradford Franklin, *Carpenter and the End of Bulk Surveillance of Americans* (LawFare, July 25, 2018), archived at https://perma.cc/X6F6-75MP; Louise Matsakis, *The Supreme Court Just Greatly Strengthened Digital Privacy* (Wired, June 22, 2008), archived at https://perma.cc/UV9S-PK5X; Paul Ohm, *The Broad Reach of Carpenter v. United States* (Just Security, June 27, 2018), archived at https://perma.cc/8LJQ-BN6B.

[210] *Carpenter*, 138 S Ct at 2223.

of business record.[211] A search warrant will be required, he maintained, only in a "rare case."[212] As Roberts summarized the Court's holding:

> Our decision today is a narrow one. We do not express a view on matters not before us: real-time CSLI or "tower dumps" (a download of information on all the devices that connected to a particular cell site during a particular interval). We do not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information. Further, our opinion does not consider other collection techniques involving foreign affairs or national security. As Justice Frankfurter noted when considering new innovations in airplanes and radios, the Court must tread carefully in such cases, to ensure that we do not "embarrass the future."[213]

In truth, though, the Court's underlying reasoning may not be so easy to cabin to CSLI; and it is not at all clear that the Justices in the majority would want to do so. Let's consider how stable and deeply rooted the Court's proposed or suggested distinctions might be.

1. *Other forms of direct location monitoring.* The Court's reasoning sends this clear message: government's use in domestic criminal investigations of tracking technologies that reveal a target's relatively precise historical locations over an extended period of time now triggers a Fourth Amendment search. This includes CSLI data, GPS tracking, and future equivalents, whether the technology tracks the target personally[214] or through her phones,[215] cars,[216] or anything else

---

[211] Id at 2217, 2216, 2219, 2222.

[212] Id at 2222.

[213] Id at 2220 (citation omitted). This caution rests in substantial tension with the Court's aggressiveness in describing CSLI as approaching GPS-level tracking. See Part II.A.

[214] For example, law enforcement agencies increasingly use various technologies to track individuals directly, including aerial surveillance drones and body cameras linked with facial recognition software. Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 Emory L J 527, 539–44 (2017) (video cameras and drones); id at 547 (body cameras).

[215] I use my cell phone for driving directions, finding coffee shops and gas stations, and sometimes (shh, don't tell them) tracking my teen daughters; all of these functions share my or another phone's GPS coordinates with a third party.

[216] For example, fixed-place license plate readers or intersection cameras can identify and record car traffic. Levinson-Waldman, 66 Emory L J at 544–47 (cited in note 214) (noting ICE use of license plate readers). And smart boxes and dashboard infotainment services installed in cars can transmit information about car location and operation to manufacturers and other third parties. Michael J. D. Vermeer, Dulani Woods, and Brian A. Jackson, *Identifying Law Enforcement Needs for Access to Digital Evidence in Remote Data Centers* *22

that frequently accompanies her as she moves;[217] and this conclusion surely governs government-initiated monitoring as well as accessing third-party location records. (As explained earlier, I suspect the Court will maintain at least some durational trigger, excluding short-term monitoring from Fourth Amendment coverage.)[218]

The Court's insistence that it does *not* "call into question conventional surveillance techniques and tools, such as security cameras," raises interesting questions.[219] I assume "conventional" techniques include old-fashioned eyes-on personalized surveillance of the sort Justice Alito compared to GPS tracking in his *Jones* concurrence, potentially involving "a large team of agents, multiple vehicles, and perhaps aerial assistance."[220] At first glance, it would seem that such conventional, personalized surveillance should be subject to the same durational limits as more high-tech location monitoring. After all, around-the-clock personal surveillance reveals at least the same "privacies of life" and is "reasonably unexpected" to the same degree.[221] So

---

(Rand, 2018), archived at https://perma.cc/7ANK-TB3Z (noting that "Carfax, Hertz, and other vehicle-related companies collect vehicle histories, including oil changes, vehicle locations, and potentially even snapshots from an in-car camera that could have evidentiary utility").

[217] For example, Fitbits and other body-worn biometric assessment devices generally track movement and location, among other things. Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 Cornell L Rev 547, 558–59 (2017).

[218] See text accompanying note 165. Because the Court assumed (contra the record) that CSLI reveals the user's location pretty much continuously, the Court had no need to consider whether it might have felt differently about a week's worth of records if each day produced significantly fewer data points. If a different tracking technology fixed the target's location just once per hour or once per day, perhaps the Court would recognize that only a longer period of location monitoring would pose a sufficient mosaic-based privacy risk to constitute a Fourth Amendment search.

[219] As noted above, I assume that even "conventional tools" such as security cameras no longer qualify as "conventional surveillance techniques" once their videos or photos are aggregated into a long-term database that is searchable through facial recognition technology so as to constitute a form of historical location tracking. The distinction is less clear for long-term surveillance through an around-the-clock video camera feed targeting suspects' homes. Compare, for example, *United States v Houston*, 813 F3d 282, 287–88 (6th Cir 2016) (holding that 24/7 video monitoring of suspect's home for ten-week period was not a Fourth Amendment search), with *State v Jones*, 903 NW2d 101, 113 (SD 2017) (holding that similar video monitoring for eight-week period was a search); see also *United States v Kubasiak*, 2018 WL 4846761, *6–7 (ED Wis) (holding that *Carpenter*'s reasoning does not apply to four-month and 24/7 video camera surveillance of defendant's backyard).

[220] *Jones*, 565 US at 429 (Alito, J, concurring in the judgment).

[221] See Slobogin, 8 Duke J Const'l L & Pub Pol at 27 (cited in note 48) (recognizing that naked-eye "[o]vert surveillance by the police can be just as intrusive as covert tracking or monitoring"). These conclusions apply as well to private surveillance, for example where a private detective is hired to confirm a spouse is cheating or unfit to parent.

if a week-long CSLI request (or shorter, if the Court later shrinks the duration trigger for a search) violates Carpenter's reasonable expectation of privacy, why not also a same-length old-school stakeout and tail, or a same-length use of low-tech tools such as fixed-position security and traffic cameras?

But the Court's refusal to question conventional or low-tech surveillance is no surprise. Calling old-school tailing a search would significantly hamper what heretofore has been universally considered good investigative policing. And there is no sign that the Court intended that, as evidenced by its repeated references to CSLI tracking being "unique." What explains this?

Perhaps this again reflects a regulatory rather than atomistic bent, given how much the Court emphasized CSLI's detailed, comprehensive, infallible, cheap, and retrospective nature. It is hard to see why these features make high-tech surveillance categorically more privacy-revealing from the *target's* atomistic perspective. First, good old-school surveillance might be just as detailed and comprehensive—and potentially more so, because it can reveal not just the target's location but also how she appears, what she's doing, and with whom. Second, while CSLI is nearly infallible, good traditional surveillance might produce records that are not far off, especially if cameras are used and observations are meticulously documented. And, in any event, the Court has previously rejected the normatively dubious proposition that targets can expect privacy due to witnesses' faulty recall.[222] Third, the fact that CSLI tracking is relatively cheap doesn't add to a target's privacy intrusion for a comparably long surveillance. Finally, the fact that CSLI records can effectively turn back time is similarly atomistically irrelevant, as there is no reason to think that the target's activities for some week in the past are categorically more revealing than for some week in the present. Overall, it's hard to see why the target's atomistic privacy expectation in the whole of her public movements for any particular span of time turns on whether the government uses high-tech or low-tech location-monitoring measures.

That said, these features plus more may lead government to *track more people* using CSLI than it would track using only traditional

---

[222] See, for example, *Lopez v United States*, 373 US 427, 439 (1963) (admitting in evidence undercover agent's electronic recording of conversation because defendant has no "constitutional right to rely on possible flaws in the agent's memory" and assumes risk that witness's testimony will be "accurately reproduced in court"); *Smith*, 442 US at 744–45 (explaining that shift from human operator to automated switchboard does not affect privacy analysis).

measures, such that a CSLI tracking regime might be more privacy-intrusive *in the aggregate*, even if not so for individual targets. Though not as hassle-free as some suggest,[223] seeking CLSI from Sprint avoids typical hurdles to setting up a successful stakeout and tail. First and foremost, it is far less costly for the government. Traditional surveillance efforts typically require money, manpower, and equipment; generally, the longer the effort, the higher the cost. Resource constraints limit how much around-the-clock surveillance law enforcement can handle, forcing officials to prioritize and to intensively track only relatively important targets. Comparatively costless access to CSLI records will likely lead government to monitor the movements of many more suspects for less significant crimes. Second, CSLI tracking avoids any risk of community pushback for establishing longer-term eyes-on surveillance operations that might inconvenience or otherwise irritate neighboring residents or workers.[224] Third, CSLI data can *locate* as well as follow a target if her cell phone number is known, whereas traditional surveillance works only if agents already know where the target can be found so they can start the tail. For these reasons, agents might employ high-tech tracking even though they would not otherwise choose to bear the costs of low-tech alternatives—especially where, by hypothesis, they do not yet have probable cause to support their intuitions.[225] Finally, CSLI is more user-friendly in a different way: being able to discover a target's past rather than only her present/future locations enables agents to focus on the time frame that best fits their investigatory goals and to access information that is "otherwise unknowable."[226] Therefore, the Court could reasonably worry that the capacity for high-tech track-

---

[223] Compare *Carpenter*, 138 S Ct at 2218 ("with just the click of a button"), with Vermeer, Woods, and Jackson, *Identifying Law Enforcement Needs* (cited in note 216) (canvassing difficulties law enforcement faces in securing digital data from third-party service providers). It also costs something for officials to decipher the data, with experts mapping towers onto real locations.

[224] See *Jones*, 565 US at 416 (Sotomayor, J, concurring) (explaining that, because GPS monitoring is cheap and "proceeds surreptitiously, it evades the ordinary checks that constrain abusive police practices: 'limited police resources and community hostility'") (citation omitted).

[225] Using surveillance cameras might also cost little at the margin, if the costs of installing and maintaining the cameras are borne by others as with private store security cameras; or if the government uses cameras that it previously mounted on utility poles or over traffic lights, etc.

[226] As noted earlier, see text accompanying notes 157–58, it will likely be comparatively difficult and costly to reconstruct the target's past movements through nosy neighbors' eyewitness testimony.

ing will encourage officials to do it more often and hence acquire far more sensitive location information about people in the aggregate, even if the extent of any given intrusion is the same.

This explanation fits the Court's expressed desire "to place obstacles in the way of a too permeating police surveillance."[227] While the Court focused primarily on CSLI's capacity for individual-target intrusion, at key points the opinion also suggested concern for the overall flow of information to the government. For example, as Chief Justice Roberts noted, "[t]he Government's position fails to contend with the seismic shifts in digital technology that made possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for years and years."[228] One can almost hear a background whisper of "Big Brother" throughout the analysis, as well as in Justice Sotomayor's earlier warning in *Jones* about government gathering intimate information "more or less at will."[229]

Concerns over frequency do not typically play a role in determining whether an investigatory method constitutes an atomistically intrusive search. But, in the end, I suspect such concerns are driving much of the distinction here between high- and low-tech surveillance methods for those Justices who worry that the former "may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'"[230] If so, this doctrinal line will likely remain stable over time.[231]

2. *Other types of sensitive third-party records.* The Court also purported in *Carpenter* neither to "disturb the application of *Smith* and *Miller*" nor to "address other business records that might incidentally reveal location information," let alone to address records that reveal nonlocation information.[232] The *Smith-Miller* category

---

[227] *Carpenter*, 138 S Ct at 2214 (citation omitted)

[228] Id at 2219.

[229] *Jones*, 565 US at 416 (Sotomayor, J, concurring); id (questioning the "appropriateness of entrusting to the Executive, in the absence of any oversight from a coordinate branch, a tool so amenable to misuse").

[230] Id (citation omitted).

[231] And this might provide a reason to treat "tower dumps," a "download of information on all the devices that connected to a particular cell site during a particular interval," differently from short-term historical or real-time tracking of a single target. *Carpenter*, 138 S Ct at 2220. While the intrusion per individual is the same, the aggregate information grab by the government is vastly greater for tower dumps.

[232] Id. As Carpenter did not move to suppress the information contained in his carriers' records showing the phone numbers he dialed, he presented no direct challenge to *Smith*.

obviously includes sensitive financial and call-record information; the second category includes such things as credit card swipes, ATM withdrawals, and computer wi-fi connections through IP addresses; and the third category includes such things as accountant, utility, medical, and internet-of-things records.[233] The dissenters rightly pressed back by asking why location information is more sensitive and deserving of Fourth Amendment protection than, say, credit card or phone records.[234] After all, many private facts can be inferred from these other types of records as well.

In response, Chief Justice Roberts did not address the comparison between location and phone call, financial, or other information in the abstract. Instead, he purported to distinguish *Miller* and *Smith* by emphasizing the quantity as well as the quality of the CSLI at stake. Rather than information about "a person's movement at a particular time," this case is "about a detailed chronicle of a person's physical presence compiled every day, every moment, over several years" and thus "implicates privacy concerns far beyond those considered in *Smith* and *Miller*."[235]

But that compares a truckload of apples to a handful of oranges. The proper question, one would think, is whether a week of location monitoring works a qualitatively greater privacy intrusion than a week of phone call records or credit card purchases.[236] As to that comparison, the dissenters either were agnostic[237] or thought quite the opposite.[238] Reasonable people clearly can reasonably disagree.[239]

---

[233] While many of these examples reveal information linked to fixed locations (e.g., in-person bank transactions, landline phones, home-based utility or appliance usage, in-person doctor visits), the location sensitivity is typically dwarfed by other privacy concerns.

[234] Id at 2224, 2229, 2232–33 (Kennedy, J, dissenting); id at 2267 (Gorsuch, J, dissenting).

[235] Id at 2220 (majority).

[236] I'm accepting here the Court's focus on number of days as the proper metric, but perhaps one ought to compare *X* number of location data points with *X* number of phone calls or *X* number of purchases, whether they take the same or different time periods to generate.

[237] "Why is someone's location when using a phone so much more sensitive than who he was talking to (*Smith*) or what financial transactions he engaged in (*Miller*)? I do not know. . . ." *Carpenter*, 138 S Ct at 2262 (Gorsuch, J, dissenting).

[238] Because who you call and what you buy can reveal so much about what you do and with whom, "[t]he troves of intimate information the Government can and does obtain using financial records and telephone records dwarfs what can be gathered from cell-site records." Id at 2232 (Kennedy, J, dissenting).

[239] Surveys show people are sensitive about location information as well as many other kinds of surveillance and third-party records, with some ranking their various sensitivities quite differently than do others. See, for example, Christopher Slobogin, *Privacy at Risk: The*

And if Justice Kennedy is correct that the Court intends CSLI's operative properties of "comprehensiveness, expense, [and] retrospectivity" to weigh in the balance, those too are a wash. Whether the government seeks CSLI records or call, banking, or credit card records, it is just requesting similarly stored information from a different record-holder. For each category of information, officials can collect all stored records fairly effortlessly, going far back in time.[240]

In the end, while location information is surely *different* from other kinds of information, whether it is categorically *more sensitive* reflects a multifaceted subjective judgment.[241] And there is still the question of *how* sensitive information must be to trigger Fourth Amendment protection. Is protection limited to mosaic-creating information, meaning the records reveal something (how much is unclear) about someone's familial, political, professional, religious, and sexual associations? Or should protection be triggered for highly sensitive information that offers little mosaic-creating potential, such as records of third-party DNA testing revealing someone's ancestry composition and a genetic proclivity for adult-onset vision loss?[242]

A close friend and brilliant lawyer undoubtedly spoke for many when he summarized the Court's reasoning as follows: historical location monitoring "feels kind of invasive to me, so it must be subject to the 4th Amendment." Put differently, short of defining a search by social survey data (which would raise conceptual and methodological quandaries),[243] the Court's *Katz*-based approach in *Carpenter*, in the

---

New Government Surveillance and the Fourth Amendment 183–85 (Chicago, 2007) (survey results ranking sensitivity over twenty types of transactional records); Kugler and Strahilevitz, 2015 Supreme Court Review at 239 (cited in note 49) ("Contemporary polling on sensitivity produces a hierarchy that many readers will find intuitive . . . [but] some readers may prefer to construct the hierarchy differently than the median citizen does").

[240] The comparison between CSLI and call records is particularly salient, since Sprint keeps these types of information in the exact same records and therefore one is no more comprehensive, cheap, and historical (or infallible, for that matter) than the other.

[241] See Kugler and Strahilevitz, 2015 Supreme Court Review at 237 (cited in note 49) ("Determining what information counts as sensitive requires numerous subjective judgments. Sensitivity depends a great deal on context, on the identity of the recipient of the information, on the preferences of the data privacy subject, the risks posed by present or future disclosure, and the priors of the person evaluating the information.").

[242] Consider *Carpenter*, 138 S Ct at 2262 (Gorsuch, J, dissenting) (musing that, despite the apparent applicability of *Miller-Smith*, the notion that agents can "secure your DNA from 23andMe without a warrant or probable cause . . . strikes most lawyers and judges today—me included—as pretty unlikely").

[243] See, for example, Christopher Slobogin and Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized*

words of Justice Gorsuch, inevitably entails some intuitive judgment based on "I do not know [what] and the Court does not say."[244]

Is the Court serious about hewing to its articulated line and ensuring that exceptions to the *Miller-Smith* doctrine will be "rare"? Only time will tell. But there is no question the line will be tested early and often. In addition to privacy advocates, every criminal defendant whose investigation includes *any* third-party record request, or *any* more than *de minimis* surveillance, will surely press the claim. And lower courts now can listen. While they were previously bound mechanically to apply both the *Knotts* and *Miller-Smith* exposure rules, the amorphous nature of the Court's new doctrinal tests now gives judges license, if not permission, to deviate, to innovate, and even to anticipate technological change.

Perhaps that is precisely what the majority intended. The Court could have buttressed its cautionary prose by resting its conclusion on far narrower grounds, deploying reasoning less likely to invite open-ended interpretation than its mosaic approach coupled with sensitivity considerations.[245] But by embracing a broader if more uncertain approach, the majority can benefit from unleashed lower-court efforts to help map *Carpenter*'s new doctrinal paths. While the doctrine remains unsettled, law enforcement officers will likely err on the side of securing search warrants. And where they cannot or do not get warrants, the officers' reasonable mistakes (viewed in hindsight, if

and Permitted by Society," 42 Duke L J 727 (1993) (empirically testing how people rate different searches' intrusiveness); Jeremy A. Blumenthal, Meera Adya, and Jacqueline Mogle, *The Multiple Dimensions of Privacy: Testing Lay "Expectations of Privacy,"* 11 U Pa J Const L 331 (2009) (updating and modifying survey methodology and analysis).

[244] *Carpenter*, 138 S Ct at 2262 (Gorsuch, J, dissenting).

[245] The Court could have distinguished *Knotts* by embracing a private space–protective prophylactic rule based on *United States v Karo*, 468 US 705 (1984), see note 164; or distinguished *Miller-Smith* just by its micro-involuntary argument (automated connectivity rather than volitionally triggered sharing) and stopped there, see text accompanying note 192.

Or here is a third narrow path: the Court could have held that Carpenter did not actually share (voluntarily or otherwise) the information extracted from Sprint's records because he didn't know the specific towers/sectors his phone signaled when in use. To be sure, sometimes we are deemed (under current doctrine) to share information that we don't *actively* know in the sense of being consciously aware of it in the moment; for example, when we swipe a credit card at a gas station and we functionally transmit the store's address to American Express even though we don't really know that address, or we hit "call back" or "Mom's office" on our smartphones and functionally transmit the corresponding call numbers even though we don't currently remember them. See *In re United States for Historical Cell Site Data*, 724 F3d 600, 613 (5th Cir 2013). But in those and similar contexts, we know we can easily find out the content of the data we are transmitting. Here, by contrast, Carpenter *could not* realistically have known or learned the specific towers/sectors his phone signaled when in use because of the way cell service works. See note 26 and accompanying text.

and when *Carpenter*'s coverage expands) will be excused under the good-faith exception to the exclusionary rule. From the Court's perspective, what's not to like?[246]

III. Get a Warrant

After all that, had the Court concluded that the warrantless search of Sprint's CSLI records was not "unreasonable" under the Fourth Amendment, perhaps its uncertain narrowing of *Katz*'s carve-outs for public or third-party exposure would be much ado about nothing. The Court could have found the search justified because the government satisfied the mid-level "reasonable suspicion" standard, or the lower-level standard for compulsory document production, or even the SCA's own requirement of "specific and articulable facts showing reasonable grounds to believe" that the records were "relevant and material to an ongoing criminal investigation."[247] But the Court confidently announced that "the Government's obligation" to justify this search "is a familiar one—get a warrant."[248] Although this conclusion might be familiar, in this context it is far from axiomatic.

Indeed, the Court might profitably have refrained from addressing this issue at all, instead remanding for further lower-court consideration. Although a Fourth Amendment search typically triggers a warrant requirement, it does not always do so; and critics of the third-party doctrine have taken different positions on the issue.[249] Lower courts through the years have paid much less attention to the justification than to the search question.[250] And, in particular, few courts

---

[246] And of course, while courts debate and refine the new mosaic approach and narrowed third-party doctrine, other actors may explore their own interventions. Congress, state legislatures, and state courts may create positive law protections for privacy interests in third-party records that would overlay any Fourth Amendment protection (or, under the alternative property-based approach Justice Gorsuch tentatively advanced, that would themselves create new property interests deserving Fourth Amendment protection, see text accompanying notes 109–12). And perhaps service providers seeking to assuage old customers and woo new ones will consider storing far fewer name-identified records for far fewer days, limiting the information a search would reveal.

[247] See discussion in Parts III.B and III.C.

[248] *Carpenter*, 138 S Ct at 2221. The Court acknowledged that case-specific exceptions may support warrantless searches in conventionally recognized exigent circumstances, such as "pursu[ing] a fleeing suspect, protect[ing] individuals who are threatened with imminent harm, or prevent[ing] the imminent destruction of evidence." Id at 2222–23.

[249] See note 276 and accompanying text.

[250] For most courts (including the Sixth Circuit here) the second question became moot after finding there was no Fourth Amendment search to justify.

have meaningfully considered the dissents' primary argument (discussed below) that the traditional standard governing subpoenas *duces decum* should apply.[251] Despite professing caution when deciding the search question, the Court appeared decidedly uninterested in what lower courts, or even Congress, might have to say about Fourth Amendment reasonableness after they consider the Court's new view of the privacy interests at stake.[252]

Although the warrant requirement typically follows a newly defined search, the connection here is worth a closer look for two reasons. First, for Justices who care (and surely some do), the trade-off between privacy protection and law enforcement interests may undergird the desire to keep "[o]ur decision today . . . a narrow one." Requiring probable cause for long-term CSLI tracking will, unsurprisingly, hinder and sometimes thwart investigations into various crimes. Applying the same requirement to single-data-point or very short-term tracking (historical or prospective) will expand and amplify the burden while protecting, by definition, thinner mosaic-based privacy interests. And applying the same requirement to a much broader swath of third-party records will magnify those costs considerably, as law enforcement is far more dependent on early-investigation access to certain other records for certain types of crimes. Obviously, the privacy/enforcement trade-off has no formal place within the Court's search analysis. But as a matter of simple prediction, I suspect the Court will be reluctant to extend *Carpenter*'s new search definition to encompass short-term location tracking or financial, phone, and other forms of communications metadata if the warrant requirement would inevitably apply.

Second, Chief Justice Roberts's response to the dissents' pressure to apply the much more relaxed reasonableness standard traditionally governing subpoena-compelled production of documents may have implications well beyond this case. While articulating a new sensi-

---

[251] None of the five Court of Appeals decisions did so. See note 30.

[252] Lower courts might have looked to experience from the nine states that by statute or constitutional provision currently require warrants to obtain CSLI. See *Carpenter* Petr's Brief at *22 & n 11 (cited in note 113).

And prompted by the Court's holding that a search occurred, perhaps Congress would have amended the Stored Communications Act to require a showing greater than investigatory relevance but still short of probable cause, a decision potentially deserving deference down the road. See *United States v Di Re*, 332 US 581, 585 (1948) (noting Court has "be[en] reluctant to decide that a search thus authorized by Congress was unreasonable"); *Jones*, 565 US at 429–30 (Alito, J, concurring in the judgment) (suggesting preference for legislative resolution).

tivity constraint on third-party subpoenas to protect Carpenter's CSLI, the Court (perhaps inadvertently) raised questions as to whether and how that same constraint may apply to a broad array of first-party subpoenas as well.

A. THE WARRANT REQUIREMENT AND EARLY-STAGE CRIMINAL INVESTIGATIONS

Police use CSLI tracking because it works; and not just to solve store thefts.[253] "Historical cell tower location records are routinely used to investigate the full gamut of state and federal crimes, including child abductions, bombings, kidnappings, murders, robberies, sex offenses, and terrorism-related offenses."[254] For example, historical CSLI was recently used to identify the person alleged to have mailed pipe bombs to various Democratic officials and supporters and CNN.[255]

Surely, at times police have used SCA court orders to secure historical CSLI even where they had sufficient probable cause to secure a warrant.[256] But CSLI is generally requested during the early stages of criminal investigations, when police lack probable cause with respect to any given suspect.[257] Many lower courts have described the government's use of location data in solving serious crimes where the stories make clear the data were very helpful long before officials could establish probable cause.[258] Early access to location information is particularly useful to determine who among several potential

---

[253] Those who have characterized Carpenter's spree of cell phone robberies as relatively mundane might be forgetting or at least underappreciating the gang's frequent use of a gun.

[254] *United States v Davis*, 785 F3d 498, 518 (11th Cir 2015) (en banc) (citing cases).

[255] After federal agents identified a possible suspect, they used his historical CSLI records to confirm he had signaled a cell tower in the vicinity of the post office used to mail some of the packages (and then they apparently used real-time cell-tower tracking to locate and arrest him). Kara Scannell, Evan Perez, and Shimon Prokupecz, *How the Alleged Bomber Was Caught* (CNN, Oct 27, 2018), archived at https://perma.cc/6Y56-GHWL.

[256] Some commentators assert that was true for *Carpenter*. See Lior Strahilevitz and Matthew Tokson, *Quick Reactions to Today's Carpenter Oral Argument—Post 2* (Concurring Opinions, Nov 29, 2017), archived at https://perma.cc/A85G-M7K3 ("There probably was probable cause in *Smith v. Maryland*, and in *Carpenter*, for that matter."). I'm dubious as to the latter, especially given the breadth of the records request.

[257] *Davis*, 785 F3d at 518; see also id ("In such cases, [SCA] § 2703(d) orders—like other forms of compulsory process not subject to the search warrant procedure—help to build probable cause against the guilty, deflect suspicion from the innocent, aid in the search for truth, and judiciously allocate scarce investigative resources.").

[258] See, for example, *United States v Pembrook*, 876 F3d 812, 816–19 (6th Cir 2017) (using CSLI initially to identify common phones near two jewelry heists that were over 150 miles

suspects deserves further scrutiny,[259] to exclude potential suspects where a wrong accusation might stymie the investigation or cause other harms,[260] and to identify members and significant places (e.g., for meetings, hideouts, and stashes) for criminal groups such as gangs, mobs, and other conspiracies.[261]

Some privacy advocates assert that a warrant requirement will have little impact on criminal investigations, claiming that officials can almost always establish probable cause if they just work a little harder.[262] That strikes me as quite optimistic, as more sober privacy experts concede.[263] More likely, sometimes additional sleuthing will produce probable cause to support a warrant for CSLI records; and sometimes it will not, leaving the records unobtainable.[264]

---

apart and finding a recently activated prepaid "burner" phone with no associated name; call detail records then identified the perpetrators).

[259] See, for example, *United States v Reynolds*, 626 Fed Appx 610, 612 (6th Cir 2015) (identifying one among several plausible suspects because only he was in the vicinity of the house where and when a computer downloaded child pornography).

[260] For example, quietly ruling out a father or boyfriend as a child kidnapping suspect because CSLI shows he was not near the abduction scene, where a false accusation or even just further investigation might both preclude his good-faith assistance and create a long-term family rift. See *Davis*, 785 F3d at 518 (noting that CSLI can reveal that "an individual suspect was . . . far away in another city or state").

[261] See Jim Baker, recorded in *The Lawfare Podcast: Jim Baker and Orin Kerr on the Carpenter Ruling* (Lawfare, June 30, 2018), archived at https://perma.cc/8P4G-RH2U.

[262] Aziz Huq, *The Latest Supreme Court Decision Is Being Hailed as a Big Victory for Digital Privacy. It's Not* (Vox, June 23, 2018), archived at https://perma.cc/R895-XL9N (explaining that CSLI data are "routinely relevant to conspiracy charges" and asserting that in such cases "it will often be very easy for the police to meet the (exceedingly weak) probable cause standard"); see also *Davis*, 785 F3d at 543 (Martin dissenting) ("But if my view of the Fourth Amendment were to prevail, all the officers in this case had to do was get a warrant for this search. That is no great burden.").

[263] As Jane Bambauer advises, "[m]ost [privacy] scholars know that recognizing access to third-party records as a full-fledged search requiring a warrant and probable cause is an unworkable solution. Police need some way to build up suspicion about a suspect, and keeping every last third-party record off limits until the case progresses to probable cause would unacceptably frustrate investigations." Bambauer, 94 Tex L Rev at 215 (cited in note 170); id at 216–17 ("If courts open the definition of 'search' to cover more things, they must have the latitude to work exclusively within the Reasonableness Clause of the Fourth Amendment and to avoid the Warrant Clause.").

[264] Two potential unintended consequences are worth noting. First, where agents do the extra work and manage to develop probable cause to support a CSLI records request, might the agents then consider broadening the scope of their intended search? Armed with probable cause, why not also seek even more precise GPS data created by location or driving-directions apps? Or also seek the content of text messages or e-mails sent or received within a few days of the crime? Once agents have probable cause to believe location records would reveal evidence of criminality, they likely also have probable cause to believe GPS data and text and e-mail content would do so as well.

Second, many conventional sleuthing efforts are prone to error and stereotyping, and they tend to disproportionately focus on poor and minorities communities—tendencies

Expanding Carpenter's search definition to include single-datapoint or very short-term CSLI monitoring would not only protect records less susceptible to privacy-threatening mosaic creation,[265] but also make it harder for police to use CSLI precisely when it offers the most unique investigative benefits, such as checking to see whether a phone was near a single relevant place at a single relevant time.[266] In other words, the privacy/law enforcement trade-off is quite sensitive to monitoring duration.

That said, it is worth noting that although both long- and short-term CSLI records requests are useful for investigating many *different* types of crime, they are not crucial for investigating any *particular* type of crime. So the inevitable costs to law enforcement will likely be distributed across many different kinds of criminal investigations. And, of course, access to location records for use in criminal investigations is relatively new.

By contrast, the impediment to effective and efficient investigations would likely both be more widespread and have a greater impact on particular crimes if the Supreme Court or lower courts broaden *Carpenter*'s "narrow" ruling to hold that securing other types of third-party records likewise requires a warrant. Many other types of third-party records (especially financial, credit card purchases, internet protocol addresses, and phone/text noncontent metadata) are routinely relied upon in early-stage investigations.[267] And certain types of crimes would largely defy successful prosecution without early access to such third-party records. Obvious examples include white-collar financial crimes, identity theft, "[m]alicious hacking, possession of child pornography, laundering money through gambling websites, and insider trading," which among other crimes "leave very few clues in the physical world."[268] And proactive efforts to identify and thwart

---

that digital records generally avoid. See Bambauer, 94 Tex L Rev at 244–48 (cited in note 170); see also Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U Penn L Rev 327, 391 (2015) ("The accuracy that big data provides not only increases the likelihood that police target the right suspects, but also, in turn, prevents the resulting physical, face-to-face interactions [of conventional policing] that generate tension.").

[265] See note 161 and accompanying text.

[266] See notes 259–60 and accompanying text.

[267] See *Carpenter*, 138 S Ct at 2229 (Kennedy, J, dissenting) (referencing crimes ranging from drug trafficking to health-care fraud to tax evasion).

[268] Bambauer, 94 Tex L Rev at 249 (cited in note 170); id ("Some crimes offer little hope of detection without the aid of third-party data."); Christopher Slobogin, *Transaction Surveillance by the Government*, 75 Miss L J 139, 185–86 (2005) (explaining that "requiring a uniform

potential acts of terrorism require lots of background location and movement data from which computer algorithms can predict conventional behavior in order to discern unconventional and perhaps threatening aberrations.[269]

The ultimate impediments to law enforcement efforts posed by requiring a warrant to access CSLI and other third-party records cannot easily be quantified, though surely they are real. The Court has previously voiced concern over these impediments when protecting grand juries' long-standing authority to compel access to documentary evidence in order to determine whether there is probable cause to believe a crime was committed; requiring a warrant up front "would stop much if not all investigation in the public interest at the threshold of inquiry."[270] Justice Alito echoed this concern in *Carpenter*, warning that requiring search warrants for document production requests "will seriously damage, if not destroy, their utility."[271]

Perhaps that alarm is a bit dramatic. But whatever impact *Carpenter*'s warrant requirement will have on criminal investigations where early-stage CSLI data could be useful, the impact of further extending *Carpenter*'s search analysis to protect short-term CSLI and especially other third-party records—assuming the warrant requirement comes along for the ride—will be broader and sharper. That recognition at least invites a closer look at the warrant requirement's plausible alternatives, if only for future consideration.

b. why not impose a mid-level reasonableness standard?

The Fourth Amendment prohibits unreasonable searches, not warrantless ones. The United States argued that the SCA's "reasonable grounds to believe . . . relevant" standard, perhaps somewhat

---

standard of probable cause for all [third-party] records searches . . . provides far too much protection for some types of information" because certain kinds of investigations "would probably never get off the ground"); Wayne R. LaFave, 2 *Search and Seizure: A Treatise on the Fourth Amendment* § 4.13 at 1081 (West, 5th ed 2012) (noting IRS subpoena power "is critical to determining tax liability properly").

[269] See Baker, *Jim Baker and Orin Kerr on the Carpenter Ruling* (cited in note 261).

[270] *Oklahoma Press Pub. Co. v Walling*, 327 US 186, 213 (1946); see also, for example, *United States v R. Enterprises, Inc.*, 498 US 292, 297 (1991) ("[T]he government cannot be required to justify the issuance of a grand jury subpoena by presenting evidence sufficient to establish probable cause because the very purpose of requesting the information is to ascertain whether probable cause exists.").

[271] *Carpenter*, 138 S Ct at 2256 (Alito, J, dissenting); see id at 2257 (Alito, J, dissenting) ("Today a skeptical majority decides to put that understanding to the test.").

less stringent than the more commonplace "reasonable suspicion" standard, is a more appropriate measure of constitutional reasonableness for CSLI searches than is probable cause.[272] The Court has previously signaled that a subprobable-cause standard suffices in exceptional circumstances involving "special law enforcement needs, diminished expectations of privacy, minimal intrusions, or the like."[273] The United States claimed that cell phone users' privacy interests are at least somewhat diminished, the document request to a third party visits only "minimal intrusions" upon the target, and law enforcement's heavy reliance on early-stage access to records before it can establish probable cause presents a special need. And over the past few decades, the Supreme Court has been increasingly receptive to nonwarrant reasonableness determinations.[274]

But the *Carpenter* Court wasted no words—literally zero—rejecting this argument. Presumably the Court, having described CSLI tracking as uniquely invasive and involuntary, simply rejected the premise of "diminished" expectations and "minimal" intrusions.[275]

---

[272] *Carpenter* US Brief at *50–55 (cited in note 126).

[273] *Maryland v King*, 569 US 435, 447 (2013), citing *Illinois v McArthur*, 531 US 326, 330 (2001); see *Riley v California*, 134 S Ct 2473, 2484 (2014) ("Absent more precise guidance from the founding era, we 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 degree to which it is needed for the promotion of legitimate governmental interests.' "), citing *Wyoming v Houghton*, 526 US 295, 300 (1999); *United States v Martinez-Fuerte*, 428 US 543, 561 (1976) ("[T]he Fourth Amendment imposes no irreducible requirement of such suspicion.") (citation omitted).

[274] See, for example, Tinsley E. Yarbrough, *The Rehnquist Court and the Constitution* 222–27 (Oxford, 2000) (canvassing Rehnquist Court decisions upholding warrantless searches in various contexts).

[275] Perhaps the Court found the warrant requirement additionally attractive for ensuring that the decision to invade privacy is made by a judge. But if the Court required only reasonable suspicion or some other intermediate standard to CSLI requests, agents would still need to seek a court order to comply with the SCA.

For other third-party records requests, the traditional subpoena process might frequently lead to judicial preclearance. Many statutes (including the SCA) either require or permit under many circumstances third parties served with a subpoena seeking customer information to notify the customer. See Ellen S. Podgor et al, *White Collar Crime* § 17.5 at 576 (West, 2d ed 2018). When a customer receives notice, she can move in court to quash the subpoena—formerly on grounds of overbreadth, harassment, and the like; but after *Carpenter* presumably to protect her own reasonable expectation of privacy. Id § 16.9 (D) at 514–15; id § 16.12(G) at 563.

And where the first-party target does not receive such notice, the third-party record-holder can move to quash the subpoena itself, perhaps increasingly motivated by marketplace pressures to protect consumer confidentiality. Conventional Fourth Amendment standing rules appear to preclude the company from raising the target's claim as well as its own. *Rakas v Illinois*, 439 US 128, 133–34 (1978). Perhaps in this atypical context, how-

That was predictable here. But if the search holding ultimately extends to other types of third-party records, then the same question will arise there. After emphatically requiring a warrant here, the Court may feel compelled to apply the same rule for all other third-party record searches, even though there might be a more persuasive argument for diminished expectations (due to some measure of voluntariness) and minimal intrusions (due to lesser sensitivity) in other contexts. And many privacy scholars critical of *Miller-Smith*'s reach have advocated reasonable suspicion or some other intermediary or graduated standard rather than across-the-board probable cause as properly balancing the competing privacy and law enforcement interests.[276] The Court could have been more cautious, reserving some flexibility for itself and lower courts facing challenges to other record requests, by conceding room for nuance. But the Court's self-described caution in keeping its search holding narrow found no visible expression here.

Of course, there is another plausible explanation. As described above, a broadly applied warrant requirement for third-party record requests likely would significantly hamper many criminal investigations, especially for particular crimes such as child pornography, tax fraud, financial crimes, internet hacking, and the like. Perhaps the Supreme Court wants the apparent remedial consequences to discourage lower courts (and its future self) from expanding its Fourth Amendment search finding beyond what it portrays as continuous, precise, and long-term location monitoring. Put differently, if it might be difficult to find principled ways to cabin the Court's

---

ever, Sprint should have third-party standing to champion the rights of a customer who receives no advance notice of the search, and indeed will never learn about it unless she is ultimately prosecuted based on its fruits. But see *Microsoft Corp. v United States Dep't of Justice*, 233 F Supp 3d 887, 912 (WD Wash 2017) (denying service provider third-party standing to represent non-noticed customers' Fourth Amendment interests).

[276] See, for example, Slobogin, 75 Miss L J at 169 (cited in note 268) (matching different types of records with either a probable cause, reasonable suspicion, or relevance requirement); Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 Pepperdine L Rev 975, 1025 (2007) (after canvassing nine relevant factors, advocating "flexible reasonableness criterion that considers the totality of the circumstances"). See also Bambauer, 94 Tex L Rev at 242 (cited in note 170) (expressing discomfort that an across-the-board warrant requirement for third-party records would mean "a policeman might be able to holler at a person, forcibly spin him around, press him to the hood of a car, and publicly feel up his entire body more easily than he could get access to his Amazon records"; and advocating "[m]ore modest reforms" than an across-the-board warrant requirement to avoid "adding a new set of paradoxes.").

reasoning to "rare" cases like this, perhaps these real-world implications stemming from a warrant requirement will encourage courts to try harder.[277] This hypothesized disincentive might not be pretty, but it could be potent.

c. why not impose the low-level reasonableness standard for document subpoenas?

The United States also argued, and this time three dissenting Justices (most vociferously Justice Alito) agreed, that to be constitutionally reasonable a CSLI records request need satisfy only the much-less-than-probable-cause standard applicable to a conventional subpoena *duces tecum*.[278] For both CSLI and other compulsory records requests, officials demand that the request recipient produce the specified documents, rather than themselves enter the recipient's space and rummage around until they find and take the documents.

Justice Alito, after spending many pages arguing that "the Fourth Amendment, as originally understood, did not apply to the compulsory production of documents at all,"[279] conceded that in the late nineteenth century the Court began to view compulsory process as a type of "figurative" or "constructive" Fourth Amendment search.[280] But the Court has long applied a different and lower standard of reasonableness to constructive rather than full-blown rummage searches: while the latter generally require a probable cause–backed

---

[277] See Akhil Reed Amar, *Fourth Amendment First Principles*, 107 Harv L Rev 757, 769 (1994) ("Because it creates an unreasonable mandate for all searches, the warrant requirement leads judges to artificially constrain the scope of the Amendment itself by narrowly defining 'search' and 'seizure.'").

[278] *Carpenter* US Brief at *44–50 (cited at note 126); *Carpenter*, 138 S Ct at 2228–29 (Kennedy, J, dissenting); id at 2247–57 (Alito, J, dissenting).

[279] *Carpenter*, 138 S Ct at 2250 (Alito, J, dissenting). According to Alito, a request to produce is neither a textual "search" nor "seizure." Id at 2251 (Alito, J, dissenting). And the Founders opposed the Crown's practice of general warrants because "[p]rivate area after private area becomes exposed to the officers' eyes as they rummage through the owner's property in their hunt for the object or objects of the search." Id (Alito, J, dissenting). A request to produce raises no such privacy concerns, beyond revealing the secured object's contents. And no historical evidence supports the Fourth Amendment's application to compulsory process. Id at 2252 (Alito, J, dissenting). Justice Gorsuch appears more equivocal on this latter point, noting there may be no good historical evidence either way in the form of common law decisions. Id at 2271 (Gorsuch, J, dissenting).

[280] *Carpenter*, 138 S Ct at 2254 (Alito, J, dissenting); see generally id at 2252–54 (tracing history).

search warrant, the former require only that a subpoena or similar court order demanding documents "'be sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome.'"[281] This lower standard, which I will refer to as the "burdensome" test, reflects a "'basic compromise' between the 'public interest' in every man's evidence and the private interest 'of men to be free from officious meddling.'"[282]

This compromise is essential, Justice Alito maintained, to law enforcement's ability to investigate crime. As noted previously, various forms of compulsory process (including grand jury, legislative, administrative subpoenas and similar law enforcement document demands) are used regularly "to determine '*whether* there is probable cause to believe a crime has been committed,'" which by definition means that they are not supported by probable cause.[283] After citing numerous cases in which the Court across many decades has applied the lower burdensome standard to document subpoenas issued to third parties for their business records,[284] Justice Alito concluded that the same standard should govern here—especially because he thought it quite odd for Carpenter to enjoy greater Fourth Amendment protection than Sprint does in Sprint's own records.[285]

Not so odd at all, rejoined the Court. Almost all of Justice Alito's cited examples either "contemplated requests for evidence implicat-

---

[281] Id at 2255 (Alito, J, dissenting), quoting *Donovan v Lone Steer, Inc.*, 464 US 408, 415 (1984); see also *Oklahoma Press*, 327 US at 209 (holding that subpoena satisfies Fourth Amendment reasonableness if "the investigation is authorized by Congress, is for a purpose Congress can order, and the documents sought are relevant to the inquiry," and the "specification of the documents to be produced [is] adequate, but not excessive, for the purposes of the relevant inquiry"). The lower standard also reflects the fact that the subpoena recipient has an "opportunity to present objections" to a judicial officer before producing the records, which further minimizes the intrusion. Id at 195.

[282] *Carpenter*, 138 S Ct at 2254 (Alito, J, dissenting), quoting *Oklahoma Press*, 327 US at 213. Mild differences in the constitutional standards applied to different subpoena sources, see Podgor, *White Collar Crime* § 17.4(A) at 570 (cited in note 275), are not important for present purposes, and none of the opinions in *Carpenter* distinguished among them. See, for example, *Carpenter*, 138 S Ct at 2234 (Kennedy, J, dissenting) (referencing decision's impact on "the subpoena practices of federal and state grand juries, legislatures, and other investigative bodies" as well as the "court-approved compulsory process in this case").

[283] *Carpenter*, 138 S Ct at 2256 (Alito, J, dissenting).

[284] Id at 2254 (Alito, J, dissenting).

[285] Id at 2256 (Alito, J, dissenting) (citation omitted). Justice Alito's assertion that the Stored Communications Act order for Sprint's records regarding Carpenter satisfied that standard is hard to contest, given the Act's required showing of relevance is more stringent, and Sprint could produce the records without much effort. Id at 2255 (Alito, J, dissenting).

ing diminished privacy interests" because the sought-after information had been publicly exposed, or requests for "a corporation's own books" containing information such as "corporate tax or payroll ledgers."[286] The lone exception is *Miller*, where the Court had already determined that Miller lacked a cognizable privacy interest in the bank records.[287] This observation's relevance, presumably, is that the Court had sometimes justified applying the lower burdensome standard to traditional corporate records on the ground that legislatures have a special interest in regulating the corporations whose formation they authorized, and such regulations could realistically be enforced only through self-revelation of internal corporate operations—basically, creating a form of reduced expectations of privacy in core corporate activities.[288]

Once again Chief Justice Roberts was a bit aggressive in characterizing precedent. Even assuming that corporations have diminished privacy interests in their own tax, payroll, and similar business records, at least two of the cited decisions addressed types of records that seem far afield and are awash with sensitivity concerns.[289] Moreover,

---

[286] Id at 2221–22 (majority).

[287] *Carpenter*, 138 S Ct at 2221–22.

[288] See, for example, *Oklahoma Press*, 327 US at 204–5 (explaining that private corporations are historically subject to "broad visitorial power" and "Congress may exercise wide investigative power over them, analogous to the visitorial power of the incorporating state"); *United States v Morton Salt*, 338 US 632, 652 (1950) ("corporations can claim no equality with individuals in the enjoyment of privacy"); LaFave, 2 *Search and Seizure* § 4.13(e) at 1085 (cited in note 268).

[289] Wayne R. LaFave et al, 3 *Criminal Procedure* § 8.7(a) at 34 n 38.550 (West, 4th ed, 2018–19 Pocket Part) ("LaFave 2018–19 Pocket Part § 8.7(a)") ("However, not all of the cases cited involved corporate records, not all involved business records, and not all involved business regulations."). The Court described *United States v Powell*, 379 US 48 (1964), as regarding "corporate tax records," *Carpenter*, 138 S Ct at 2221 n 5, without acknowledging that the demanded tax documents may include records pertaining to "a variety of non-business activities (e.g., charitable contributions and medical expenses)." LaFave 2018–19 Pocket Part § 8.7(a) at 23 (cited earlier in this note). And the Court describes *McPhaul v United States*, 364 US 372 (1960), as regarding "books and records of an organization," *Carpenter*, 138 S Ct at 2221 n 5, without letting on that the House Un-American Activities Committee was seeking "all records, correspondence and memoranda" pertaining to the Civil Rights Congress's structure, affiliation with other organizations, and all monies received or expended by it to determine whether the Civil Rights Congress was "being used for subversive purposes" and "affiliated with known Communist organizations." *McPhaul*, 364 US at 381.

Importantly, even *Miller* does not clearly state that the customer, had he retained a reasonable expectation of privacy in his banks' records, would have been entitled to insist on a warrant. The court of appeals had held that Miller possessed a sufficient Fourth Amendment interest to challenge the subpoenas that produced those records, but the subpoenas were defective (because they were issued by the wrong entity and for a date when the grand jury was not in session), and

Roberts ignored an entire body of lower-court cases applying the burdensome standard to subpoenas seeking sensitive information equally far afield from traditional corporate records.[290] So claiming that "this Court has never held that the Government may subpoena third parties for records in which the suspect has a reasonable expectation of privacy"[291] means less than at first appears.[292]

The Court's stronger response is that the burdensome standard is simply too weak to adequately protect the privacy interests at stake. The "critical issue . . . [is] that CSLI is an entirely different species of business record—something that implicates basic Fourth Amendment concerns about arbitrary government power much more di-

therefore Miller was not afforded "sufficient 'legal process.'" *United States v Miller*, 500 F2d 751, 758 (5th Cir 1974) (citation omitted). The Supreme Court reversed after finding Miller lacked Fourth Amendment standing to challenge the subpoenas. But the Court did not clearly indicate that if Miller retained a privacy interest affording him standing he could insist on a search warrant rather than just properly issued subpoenas. See *Miller*, 425 US at 445 (holding that Miller's motion to suppress was correctly denied "since he possessed no Fourth Amendment interest that could be vindicated by a challenge to the subpoenas"); id at 451 (Brennan, J, dissenting) (decrying government access to bank records "'without any judicial control as to relevancy or other traditional requirements of legal process'") (citation omitted); compare id at 456 (Marshall, J, dissenting) (asserting that statute mandating that banks maintain customers' records triggers "warrant and probable cause" requirement, and customers have standing to complain).

The Court also ignored another line of cases discussing other potential constitutional limits on the subpoena power, in which the targets did not even raise Fourth Amendment concerns notwithstanding the obviously sensitive nature of the requested documents. The *Carpenter* Court's claim that it had never previously upheld a third-party subpoena for records in which first parties retained a privacy interest is at least "inconsistent" with these other cases. LaFave 2018–19 Pocket Part § 8.7(a) at 23–25 (cited earlier in this note). See, for example, *Branzburg v Hayes*, 408 US 665 (1972) (rejecting First Amendment challenge to subpoenas issued to newspaper reporters for interview notes); see also *Fisher v United States*, 425 US 391, 401 n 7 (1976) (rejecting Fifth Amendment challenge to business records; flagging "[s]pecial problems of privacy which might be presented by subpoena of a personal diary," but only because of an overbreadth concern for rummaging rather than a privacy concern for the requested information), citing *United States v Bennett*, 409 F2d 888, 897 (2d Cir 1969).

[290] Podgor, *White Collar Crime* § 16.10(D) at 534–35 (cited in note 275) ("A long line of lower court rulings have upheld grand jury subpoenas demanding from individuals personal records and correspondence, including emails stored on a computer."); LaFave 2018–19 Pocket Part § 8.7(a) at 25 (cited in note 289) (noting that Court's rule would also "require rejection of a body of federal lower court precedent also not discussed in the *Carpenter* opinions"); id at 35–36 nn 38.780–38.820 (citing and discussing cases).

[291] *Carpenter*, 138 S Ct at 2221.

[292] See also id at 2228–29 (Kennedy, J, dissenting) ("[I]t is well established that subpoenas may be used to obtain a wide variety of records held by businesses, even when the records contain private information.").

rectly than corporate tax or payroll ledgers."[293] Moreover, Justice Alito's position would prove too much, Roberts continued, because then the warrant requirement would *never* protect any type of self-producible record no matter the privacy interest retained in it. Rather, "private letters, digital contents of a cell phone—any personal information reduced to document form, in fact—may be collected by subpoena" so long as the request isn't too burdensome.[294] Surely that's not right; and the Court noted that even Justice Kennedy "declines to adopt the radical implications of this theory, leaving open the question whether the warrant requirement applies when the Government obtains the modern-day equivalents of an individual's own 'papers' or 'effects,' even when those papers or effects are held by a third party."[295] Such an exception would sensibly "prevent the subpoena doctrine from overcoming any reasonable expectation of privacy."[296]

Thus, the Court reached its purportedly humble conclusion: just as these individual papers and effects receive full Fourth Amendment protection, "[w]e simply think that such protection should extend as well to a detailed log of a person's movements over several years."[297] Government can continue using subpoenas in the "overwhelming majority" of investigations, but a warrant is required "in the rare case" where the suspect retains a legitimate privacy interest in third-party records.

But here again, the Court may have bitten off more than it wants to chew. While the Court affirmed that a warrant would heretofore be required for the modern-day equivalents of an individual's own papers or effects in third-party hands, it is unclear why the Court's logic doesn't equally apply to (1) such papers even when in the hands of the first rather than third party, and (2) other types of sensitive documents as well. If so, the warrant-over-subpoena rule announced here might have much broader application than the Court admitted.

---

[293] Id at 2222 (majority).

[294] Id.

[295] *Carpenter*, 138 S Ct at 2222.

[296] Id.

[297] Id.

D. DID THE COURT (INADVERTENTLY) MODIFY SUBPOENA DOCTRINE MORE GENERALLY?

A thought experiment: what if the government subpoenaed Carpenter directly, ordering him to turn over documents he personally possessed that revealed his historical movements? Perhaps his cell phone maintained such records within itself or in the cloud.[298] Perhaps his job required him to keep detailed location records.[299] Perhaps he exercised his federal statutory right under the Telecommunications Act of 1996 and requested Sprint to send him a copy of their records.[300] Most intriguingly, perhaps the government earlier ordered him by subpoena to obtain a copy of Sprint's records precisely so that the government could then demand that he turn them over.[301]

One might fight the hypothetical, as government officials would usually prefer to get potentially incriminating records from third rather than first parties. If asked directly, the target might destroy or alter the evidence, alert co-conspirators, etc. And he might also refuse to comply, claiming that the act of producing the records would itself violate his privilege against self-incrimination.[302] But these worries won't always arise. Here, Carpenter would not likely despoil the CSLI records knowing that Sprint has an accurate copy, and perhaps the government does not mind him knowing he's been fingered. And Carpenter may have no valid Fifth Amendment objection, either because his possession of the documents is a foregone conclusion,[303] or he has been granted immunity, or the records might incriminate someone else but not him.

---

[298] Chief Justice Roberts himself suggested this possibility in *Riley*, noting that "[h]istoric location information is a standard feature on many smart phones . . . ." 134 S Ct at 2490. See also Huq, *Decision Is Being Hailed* (cited in note 262) ("Locational data is held not only by [the] telephone company. It is also contained on a person's phone, even if she chooses to disable locational tracking.").

[299] For example, perhaps he's a cross-country truck driver who takes constant notes of time and location to prove that he's neither shirking nor exceeding maximum permissible driving hours.

[300] 47 USC § 222.

[301] See LaFave 2018–19 Pocket Part § 8.7(a) at 20–21, 30 nn 38.280–38.290 (cited in note 289) (noting this possibility).

[302] *United States v Hubbell*, 530 US 27, 36 (2000) ("[T]he act of producing documents in response to a subpoena may have a compelled testimonial aspect.").

[303] Id at 44.

The point is that the government could seek the same CSLI directly from Carpenter, and it would make no sense for the Court, based on its own reasoning, to grant him less privacy protection for the copy he possesses than for Sprint's original. So the heightened protection for CSLI necessarily applies to first-party as well as third-party subpoenas.[304] And indeed this conclusion flows naturally from the Court's endorsement of Justice Kennedy's caveat: if the warrant requirement shields a target's papers or effects "*even when*" they are held by a third party,[305] surely it also shields them when they remain with the target herself. This in itself is a significant statement: heretofore first parties served document subpoenas were generally thought protected by the same low-level burdensome standard as their third-party counterparts.[306] *Carpenter*—perhaps inadvertently—suggests otherwise.

This, then, raises the question: how broadly applicable is this warrant requirement that supersedes first-party subpoenas? Following the Court's language, it is at least expansive enough to include the "modern-day equivalents" of papers and effects, and presumably the original forms as well. This clearly addresses Justice Kennedy's reference to letters and e-mails.[307] But the Court also wanted to cover Justice Alito's broader reference to "private letters, digital contents of a cell phone—*any personal information reduced to document form*, in fact."[308] This sounds pretty broad.

Perhaps the adjectives "individual's own" and "personal" suggest the Court would stop short of saying that *anything* that's technically a tetrad paper or effect now deserves warrant-level rather than subpoena-level protection. Perhaps "personal" papers such as diaries and letters are in, whereas "impersonal" papers such as drug ledgers

---

[304] Otherwise, the Court's holding has no bite. The government could always force targets to get a copy of their "own" records from any and all third parties as a prelude to producing them to the government in response to a subpoena *duces tecum*—and the foregone conclusion doctrine would take the Fifth Amendment privilege out of the picture.

[305] *Carpenter*, 138 S Ct at 2222 (emphasis added).

[306] See, for example, Kerr, *Initial Reactions to Carpenter v. United States* (USC Law Legal Studies Paper No 18-14, July 6, 2018), archived at https://perma.cc/2SZV-TSKJ ("A [first-party] recipient does have Fourth Amendment rights at stake, but he can challenge the subpoena only on the ground that it is overbroad or compliance is overly burdensome.").

[307] *Carpenter*, 138 S Ct at 2230 (Kennedy, J, dissenting).

[308] Id at 2222 (majority) (emphasis added). For his part, Justice Gorsuch would appear to protect from warrantless subpoenas all records that are "sufficiently similar to letters in the mail." Id at 2271 (Gorsuch, J, dissenting).

and porn magazines are out. But it isn't clear where this line comes from, nor where one would draw it (intimate photos? appointment books? the Kamasutra?). The Fourth Amendment text offers no help: all papers and effects appear on the same footing, and indeed the whole point of the *Katz* test is to identify and place other privacy interests on the *same* footing as papers and effects, not on some higher plane. So the Court again seems to invite a sensitivity test, whereby future courts must decide if various documents or effects are sufficiently "personal" to qualify for warrant rather than subpoena-level protection.[309] A broad definition could significantly ratchet up the showing required to serve a large swath of first-party document subpoenas.

Maybe the Fifth Amendment's privilege against self-incrimination renders this largely an academic discussion, as the act of production doctrine typically presents a separate and high barrier for government to hurdle. But, as already noted, there may well be circumstances that naturally (or government can manufacture to) counter the Fifth Amendment claim, and then the level of Fourth Amendment protection becomes significant. This is another question for judges to work through, with little guidance from the Court. And even the Court's assurance that CSLI presents the "rare case" applies only to "records held by a third party"; it offers no guidance on how rare it should be for first-party document requests to require a warrant.

And now let us return to corporations and organizations, which have no Fifth Amendment rights.[310] Many entities generate and house all sorts of documents containing sensitive information that seem far

---

[309] Justice Thomas observes that the original meaning of "papers" might exclude *business* records that don't reveal "'personal or speech-related confidences.'" Id at 2241 n 8 (Thomas, J, dissenting), quoting Eric Schnapper, *Unreasonable Searches and Seizures of Papers*, 71 Va L Rev 869, 923–24 (1985). This statement leaves unclear whether that original meaning might also exclude a similar category of *nonbusiness* records possessed by individuals. Either way, Justice Thomas's observation implies that any such insufficiently personal or speech-related documents receive no Fourth Amendment protection at all, not that they are protected but only as second-class citizens.

Of course there is nothing inherently odd about hinging the required justification on the nature or extent of privacy invasions. That happens with rummage searches, where it takes more to search someone's body cavities than pockets. But those privacy invasions are measured by the nature of the *search* (body or pockets), not the nature of the *information* that will be revealed (drugs or passwords). Police do not, for example, need greater suspicion to search a house known to be stuffed with personal effects than a house known to be almost empty.

[310] Wayne R. LaFave et al, 3 *Criminal Procedure* § 8.12(b) at 349 (West, 4th ed 2015) (describing entity exception to self-incrimination privilege).

afield from the kinds of "corporate tax and payroll ledgers" used to rationalize the weaker protection for general business records. What about subpoenas requesting state election precincts to produce voting records during a voter fraud investigation; or subpoenas requesting dioceses to produce priests' personnel records during a sexual abuse investigation?[311] With perhaps some debate and handwringing, heretofore documents of these kinds have been considered subject to warrantless subpoena.[312] But these are not standard business documents of the sort traditionally deemed to have diminished privacy interests, and indeed they might contain very sensitive and "personal" information about the organization, people within it, and even people outside of it.

So, in the end, the Court's understandable desire not to let subpoena doctrine circumvent a CSLI warrant requirement seems to land us here: the Fourth Amendment's warrant requirement extends to compulsory process served on third parties or first parties ordering them to produce either all traditional papers and effects, or at least the "personal" subset thereof, as well as their modern-day equiva-

---

[311] See *Society of Jesus of New England v Commonwealth*, 808 NE2d 272 (Mass 2004) (rejecting motion to quash such a subpoena on free exercise of religion grounds; Fourth Amendment challenge not even raised).

[312] See, for example, Christopher Slobogin, *Subpoenas and Privacy*, 54 DePaul L Rev 805, 844 (2005) (noting that Fourth Amendment provides "minimal protection against document subpoenas, whether addressed to third parties or to the target of an investigation, and whether aimed at organizational or personal records").

Courts moved to protect personal privacy interests implicated by subpoenas issued to corporations or their officers generally do so, if at all, by ensuring the information is requested in good faith or tightening the required showing of relevance—not by requiring a showing of anything approaching probable cause. See, for example, *In re McVane v FDIC*, 44 F3d 1127, 1131 (2d Cir 1995) (requiring "more exacting scrutiny" of relevance where government seeks personal financial records of family members of corporate director suspects); *In re Administrative Subpoena (Doe)*, 253 F3d 256, 270–71 (6th Cir 2001) (enforcing subpoena requesting personal financial documents of children of doctor suspected of health-care fraud where request was "sufficiently narrowly-tailored to pass the reasonable relevance standard"). This approach applies even where companies claim that compliance will chill exercise of their or others' First Amendment rights. See, for example, LaFave, 3 Criminal Procedure § 8.8(d) at 229–43 (cited in note 310) (canvassing cases); id § 8.8(d) at 231 ("With few exceptions [generally involving fishing expeditions], such challenges have not succeeded in obtaining the quashing of the grand jury directive"); *In re Grand Jury Subpoena (Glassdoor, Inc.)*, 875 F3d 1179, 1188 (9th Cir 2017) (applying a "good-faith" test and rejecting application of heightened "substantial connection" relevancy test to subpoena requesting identity and credit card/billing information for anonymous on-line reviewers).

It is worth nothing that "[i]n white collar cases, subpoenas commonly require production of such potentially private items as 'reminder pads, notepads, diaries, calendars, day books, telephone directories, [and] telephone call logs.'" Podgor, *White Collar Crime* § 16.11(A) at 539 n 146 (citation omitted) (cited in note 275).

lents. Perhaps this extension is troubling, as it might unsettle longstanding understandings and practices;[313] and perhaps instead it is welcome, as necessary to conform those practices to fully protect Fourth Amendment interests.[314] But it seems clear that the Court was not well positioned in *Carpenter* to think this important issue through. And at the very least, the ambiguity invites widespread but good-faith resistance by those served with any and all subpoenas, until the questions are sorted out.

Finally, what do we make of this observation by Justice Alito: if the Fourth Amendment (and warrant requirement) "applies to the compelled production of documents, then it must also apply to the compelled production of testimony—an outcome that we have repeatedly rejected and which, if accepted, would send much of the field of criminal procedure into a tailspin"?[315] That extension certainly makes superficial sense. Suppose the government subpoenas Carpenter's co-defendant and half-brother Sanders to testify as to Carpenter's whereabouts over a week-long period.[316] Assuming they spent lots of time together, Sanders's testimony might threaten Carpenter's reasonable privacy interests just as much as any sensitive document might. In addition to revealing a great deal about Carpenter's location and movements (along with what he did where and with whom), Sanders might also have surreptitiously read Carpenter's diary and snooped throughout his house, learning additional sensitive information that Carpenter did not voluntarily share. Why should the government need a probable cause–backed warrant to se-

---

[313] Marty Lederman, *Carpenter's Curiosities (and Its Potential to Unsettle Longstanding Fourth Amendment Doctrines)* (Balkanization, June 26, 2018), archived at https://perma.cc/2NTR-NXUB (*Carpenter*'s potential for "fundamental transformation of national subpoena practices (and other compulsory process practices) remains to be seen").

[314] See, for example, Slobogin, 54 DePaul L Rev at 845 (cited in note 312) (advocating that Fourth Amendment *should* be "interpreted to demand that all 'papers' that contain personal information—whether held by the subject or by a third-party institution—be afforded protection similar to that extended to the individual's house, person, and effects").

[315] *Carpenter*, 138 S Ct at 2251 n 1 (Alito, J, dissenting), referencing *United States v Dionisio*, 410 US 1, 9 (1973) ("It is clear that a subpoena to appear before a grand jury is not a 'seizure' in the Fourth Amendment sense, even though that summons may be inconvenient or burdensome.").

[316] Sanders could not refuse merely because testifying "might prove embarrassing or result in an unwelcome disclosure of his personal affairs." *United States v Calandra*, 414 US 338, 353 (1974). And the Fifth Amendment would offer Sanders no shield if the questions were carefully designed not to elicit answers that could incriminate him, or if the government immunized his testimony in advance.

cure Carpenter's CSLI records from Sprint, but not need to meet even "the minimal requirement of 'reasonableness'"[317] to secure Sanders's testimony?

Advocates for overturning or cabining *Miller-Smith* primarily justify treating documents and live testimony differently by invoking a norm of counterparty autonomy. For Sanders, as a human being with his own interests and motivations, autonomy over information is central to "personhood." This autonomy principle, they claim, entitles Sanders to do what he wants with what he knows, and the principle assertedly trumps Carpenter's expectation of privacy. By contrast, the argument runs, Sprint as an institution lacks the "personhood" underpinning an autonomy claim, so Sprint has no valued reason to squeal that can trump Carpenter's privacy interests.[318]

This proffered distinction raises more questions than I can address here, such as what autonomy entails, who gets to claim it, and why it ostensibly supersedes privacy values across the board. For now, I will just highlight two concerns. First, why would we say that Sanders's autonomy interest in sharing his thoughts with the government (so strong as to override Carpenter's privacy concerns) is greater than his autonomy interest in sharing documents that he possesses? And, even more fundamentally, why would autonomy play a role here at all,

---

[317] *Dionisio*, 410 US at 15.

[318] See, for example, Slobogin, 75 Miss L J at 185–86 (cited in note 268):

> The reason we should treat interviews differently from records requests is not because privacy is somehow irrelevant in the former situation, but because the target's interest in privacy is countered by an even stronger interest—the third party's autonomy. Human information sources . . . 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.

See also ABA Standards for Criminal Justice: Law Enforcement Access to Third Party Records 39 (3d ed 2013), archived at https://perma.cc/8CUC-3JUZ (asserting that "an individual [possessing information about a target] has an autonomy and free speech interest in choosing to share information that will often trump any privacy interest" of that target; but "the balance in cases involving institutional record-holders is different"). Compare Henderson, 34 Pepperdine L Rev at 1012 (cited in note 276) (questioning distinction between third-party records and recollections and arguing that third-party doctrine should be modified to restrict government access to both—which concededly "makes the adoption of a rational third-party doctrine more far-reaching than one might have imagined").

One might also suggest that, in general, live testimony is more fallible than documentary evidence. But that is contingent on the nature of the evidence; maybe so for CSLI, and maybe not for other kinds of documents. And, in any event, it is not the Fourth Amendment's job to regulate evidentiary quality. See note 222 and accompanying text.

when by hypothesis Sanders does not *want* to either testify or produce documents, and he is being forced to do so by threat of contempt? It seems paradoxical to distinguish between Sanders and Sprint based on Sanders's autonomy when he is not legally permitted to exercise it.

And this distinction seems especially vulnerable in this case, because Sprint looks an awful lot like an (admittedly alert and ever-present) eyewitness being called to testify as to what it knows about Carpenter's whereabouts. As the Court recounts the transaction and especially the involuntary nature of the information flow, and given that Carpenter himself does not (and cannot) know the information that Sprint is actually recording,[319] one can fairly describe the transaction as follows: Carpenter wants his cell phone to connect to Sprint's towers so the phone will function as contracted. Every now and then, sometimes consciously (phone calls) and sometimes not (background app refreshing), Carpenter essentially waves his hand and says "hey Sprint, here I am, figure out your nearest cell tower so you can direct some radio signals my way." And Sprint says "Okay, and I'll write myself a note recording which tower we use, so I can keep track for business purposes." And now the government wants Sprint to share that information, either by producing the written notes or by having someone testify as to what they say. At some point, the distinction between Sprint qua third-party record-holder and Sprint qua neighbor-with-good-notes seems thin indeed.

Of course Justice Alito correctly implied that there is no way the Court would ever lead law enforcement into a "tailspin" by requiring warrants for subpoenas *ad testificandum*, and I am not suggesting that *Carpenter* will inevitably slip down that slope. But absent a persuasive answer to the question, the argument highlights the ever-growing pile of seemingly fuzzy distinctions required to keep this decision's ripple effects "rare."

IV. Conclusion

Justice Breyer was doubly correct in conceding at oral argument that "this is an open box. We know not where we go."[320] We don't know how modern surveillance methods and digital technology

---

[319] See note 26 and accompanying text.

[320] Transcript of Oral Argument, *Carpenter v United States*, No 16-402, 35 (Nov 29, 2017), archived at https://perma.cc/EYN8-3XYE.

will progress; and we don't know where Fourth Amendment doctrine will take us after *Carpenter*. It is certainly possible that this decision will eventually be viewed "as being as important as *Olmstead* and *Katz* in the overall arc of technological privacy";[321] the Court's initial embrace of the mosaic theory alone might qualify for such recognition. But the scope of overall doctrinal and practical change will turn on many factors and future decisions.

A majority of the Court is clearly motivated to tackle the challenges that new technologies present to "ensure that the 'progress of science' does not erode Fourth Amendment protections."[322] And while the Court's holding is self-professedly narrow, much of its reasoning is neither narrow nor clear. Many criminal defendants and privacy advocates are already lining up to press further expansions of *Katz* as a bulwark against digital and other technological threats to privacy.

But lurking in the background of this decision—and the forefront of law enforcement minds around the country—is a concern that reasonable and early government access to at least short-term CSLI and certain types of third-party (and perhaps first-party) records is crucial for investigating, prosecuting, and perhaps even forestalling crime. Privacy is a paramount societal value; security is too. And if the Court consistently applies a warrant requirement wherever third-party records implicate first-party Fourth Amendment interests, then any accommodation for law enforcement needs will necessarily come through the continuing life, in some form or another, of the *Miller-Smith* framework. For this reason, in my view, excited reports that "the third-party doctrine is almost dead"[323] are greatly exaggerated. The Court has surely unsettled the old balance to combat new digital threats. It will take time for the Court to construct a new one.

---

[321] Ohm, *The Broad Reach of Carpenter* (cited in note 209).

[322] *Carpenter*, 138 S Ct at 2223, quoting *Olmstead*, 277 US at 473–74.

[323] Ohm, *The Broad Reach of Carpenter* (cited in note 209).