Unpacking the Affirmative Act Distinction: An Analysis of the Applicability of Carpenter v. United States to Location Data Stored by Ride-Hailing Companies

Conor Kelly*

TABLE OF CONTENTS

*J.D., May 2020, The George Washington University Law School; B.A., with high distinction, History and Government, May 2016, University of Virginia. This Note is dedicated to my parents: my father, Peter Kelly, and mother, Ellen O'Brien Kelly. Without their enduring support and love, I would not have had the good fortune to pursue a career in the law. Their grace, compassion, sensibility, and heart are ideals that I strive to bring to everything that I do. I must add a final and immesaurable thank you to the staff of the Federal Communications Law Journal for their tireless and brilliant editorial work.

I. INTRODUCTION

Reacting to the Supreme Court's recent opinion in *Carpenter v. United States*, 138 S. Ct. 2206, 2210 (2018), Lior Strahilevitz, professor at the University of Chicago Law School, posed the following hypothetical:

> Witness sees [an] Uber black car speeding away from hit & run accident scene in [New York City] but doesn't see [the] plate or driver. [The government] wants Uber to give it names of Uber drivers [and possibly their passengers] who were near [the] scene at the time [of the accident]. After Carpenter, does the government now need a search warrant?[1]

This Note seeks to provide at least one way of thinking about–and possibly an answer to–that very question. It will address the Supreme Court's decision in *Carpenter v. United States*, in which the Court held that accessing personal location information stored by a service provider on an individual's cell phone constitutes a search under the Fourth Amendment, and the application of the principles announced and discussed in that opinion to the context of ride-hailing mobile applications, particularly Uber.[2] In so doing, it will argue that the Court has good reason in this context to read the *Carpenter* decision beyond the strict parameters of its facts. Specifically, in situations where the government seeks access to stored location information from third-party ride-hailing applications (e.g. Uber), courts should apply a multi-factor analysis, proceeding from the baseline principles articulated in *Carpenter*, looking to such factors as the type of record being collected, the pervasiveness of the data at issue, the sophistication of the technology, and the degree to which individuals are able to freely consent to the sharing of their personal location information in a digital setting.

Section I will begin by outlining the contours of the Fourth Amendment and exceptions to the warrant requirement. Section II will then seek to explain *Carpenter* in the context of Fourth Amendment case law and draw principles and future lessons from the decision itself. Section III will consider how ride-hailing apps function, how Americans think about privacy in the digital realm, and how these principles, both narrow and broad, might come into play in future cases. Finally in Section IV it will argue that courts should extend the rationale of *Carpenter* to require that in order for the government to access user location information gathered by ride-sharing applications in any situation it must first acquire a warrant. Doing so would be a doctrinally sound extension of *Carpenter*'s holding and would reflect a broader policy goal of ensuring that the law reflects evolving, modern expectations of privacy in an increasingly digitally interconnected social

---

1. Lior Strahilevitz, *The Path to Carpenter v. United States and Possible Paths Forward*, TECHNOLOY ACAD. POL'Y (July 23, 2018), https://www.techpolicy.com/Blog/July-2018/Path-to-Carpenter-v-United-States-and-Possible-Pa.aspx [https://perma.cc/PXT8-48H7].

2. Carpenter v. United States, 138 S. Ct. 2206, 2210 (2018).

sphere where intensely personal information is communicated in the furtherance of simple tasks.

II. BACKGROUND: THE FOURTH AMENDMENT AND EXCEPTIONS TO THE WARRANT REQUIREMENT

The Court's holding in *Carpenter* aligns with the Court's frequent assertion that "the most basic constitutional rule in this area is that 'searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable' under the Fourth Amendment – [and] subject only to a few specially established and well-delineated exceptions."[3] In *Carpenter*, police had made use of an already existing statutory scheme to gain access to a voluminous sum of personal data gathered by an individual's cell phone and stored by his service provider.[4] In the case of stored location information in the ride-hailing context, the potential route to accessing such data may well be more complicated, but no less insidious. As is well known, however, there are several exceptions to the warrant requirement that are "jealously and carefully drawn."[5]

Perhaps most importantly, Fourth Amendment rights, like several other constitutional rights, may be waived when one consents to search of his or her person or premises by officers who have not complied fully with the Fourth Amendment.[6] In the context of everyday, in-person citizen to police encounters, this plays out in what is perhaps a predictable and familiar manner. In a previous case explaining voluntary consent, for example, police had stopped a car and asked its occupants if they could search the vehicle–the defendant simply replied "Sure, go ahead."[7] The Court found no Fourth Amendment violation, noting that one of the defendants even attempted to aid in the search.[8] Given such facts, it may well seem apparent that such an exception reasonably furthers legitimate police interests.

The ever-increasing attenuation of the personal, immediate interaction between individual and law enforcement, however, adds a vexing complication to the familiar consent exception known as the third party doctrine: law enforcement can obtain consent from a person or entity other than the person who is being searched.[9] Traditionally, the Supreme Court held that third party consent was sufficient if that party "possessed common authority over or other sufficient relationship to the premises or effects sought

3. Coolidge v. New Hampshire, 403 U.S. 443, 454-55 (1971) (quoting Katz v. United States, 389 U.S. 347, 347 (1967)); G.M. Leasing Corp. v. United States, 429 U.S. 338, 352-53, 358 (1977).

4. 18 U.S.C. § 2703(d) (2012).

5. Jones v. United States, 357 U.S. 493, 499 (1958).

6. *See* Amos v. United States, 255 U.S. 313, 317 (1921).

7. Schneckloth v. Bustamonte, 412 U.S. 218, 221 (1973); *see also* Smith v. Maryland, 442 U.S. 735, 739 (1979).

8. *Schneckloth*, 412 U.S. at 221.

9. *See* Illinois v. Rodriguez, 497 U.S. 177, 183 (1990).

to be inspected."[10] Now, however, actual common authority is no longer required.[11] Prior to the advent of the digital age, the third-party consent question most often arose in the context of relatively immediate interpersonal interactions: a landlord agreeing to the search of an apartment, a hotel clerk allowing the search of a guest's room, or a babysitter who allows police to search the house .[12] Now, with private companies having access to a wealth of digital information about individuals' daily lives, the same question requires a different kind of thinking. This note in particular seeks to address how the Court might think about the third-party consent exception in an as-yet unaddressed area: user location information stored by ride-hailing companies.

III. *CARPENTER V. UNITED STATES*: WHAT SHOULD THE PROPER POST-CARPENTER TEST BE FOR NEW TECHNOLOGIES?

It is this issue that brings us to *Carpenter*, the Court's most recent and significant pronouncement on the third-party doctrine and on the application of the Fourth Amendment to new types of technology and stored information. What this Note argues is that the *Carpenter* Court, despite overtures to the contrary, provided a blueprint for how to address the question of whether police gaining access to other types of stored location information constitutes a search under the Fourth Amendment.[13] In the case itself, the Court professed to seeking a narrow solution, whereby a limitation to the third-party consent doctrine in the digital era was recognized when the type of record at issue was collected automatically and was comprehensive in its reach into the intimate details of an individual's life.[14] This section will turn first to the facts of *Carpenter* itself and its reasoning, before providing a more detailed consideration of its discussion of the third-party doctrine and recent cases, and then turning to contrasting evaluations of *Carpenter's* rationale.

Police in *Carpenter* had arrested four men suspected of committing a series of robberies.[15] One of the group provided officers with the cell phone numbers of the other alleged accomplices, including Carpenter's number.[16] Acting on this data, the FBI obtained court orders through the Stored Communications Act whereby law enforcement only had to put forward "specific and articulable facts" in order to gain access to Carpenter's location data from his service provider.[17] The collected information was voluminous–

10. United States v. Matlock, 415 U.S. 164, 171 (1974) (holding that valid consent existed where police searched the bedroom of defendant and woman with whom he was living agreed to the search).

11. *See, e.g.*, *Rodriguez*, 497 U.S. at 184 (1990).

12. *See* Chapman v. United States, 365 U.S. 610, 612 (1961); Stoner v. California, 376 U.S. 483, 485 (1964); United States v. Sanchez, 608 F.3d 685, 689 (10th Cir. 2010).

13. *See Carpenter*, 138 S. Ct. at 2220 (noting that "[the Court's] decision today is a narrow one . . . .").

14. *See id.* at 2217.

15. *Id.* at 2212.

16. *Id.*

17. *Id.* (quoting 18 U.S.C. § 2703(d)).

it showed a comprehensive pattern of Carpenter's personal movement over a period of weeks, tracked based on his phone automatically sending signals to cell towers (a process colloquially referred to as "pings.").[18] As suspected, for the crimes in question the data showed Carpenter to be in the immediate vicinity of the robbed locations for each of the alleged incidents.[19] The data took center stage at his trial and, despite numerous attempts to suppress, its introduction led to his conviction.[20]

Presented with the question of whether the police search of the stored location information, collected by the service provider, constituted a search under the Fourth Amendment, the Court answered in the affirmative. It began its analysis by reflecting on the centrality of cell phones in modern American life, noting that "[c]ell phone location information is detailed, encyclopedic, and effortlessly compiled."[21] In the digital age, this would seem a necessary preface to the basic conception of the Fourth Amendment as protecting the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[22] While the opinion itself disavows any affirmative implications for other types of technology, its suggestion at various points that future analyses will be highly fact-specific is worth noting.[23] The Court's emphasis on the intimacy of personal digital data, even when held or (in theory) owned by third-party companies, belies a more fundamental aversion to modes of police surveillance that simply co-opt existing third-party technology. Much of the Court's opinion actually appears to rely on the fact that while the cell-site location information ("CSLI") at issue in the case might not have been extremely pervasive, the technology itself is headed in an incredibly sophisticated and pervasive direction.[24] The introduction of new technologies, new devices, and new tracking technologies only serve to reinforce the basic point that this new digital environment constitutes an essential aspect of Americans' personal lives.

A. The Third-Party Doctrine and Carpenter

To an outside observer, the Supreme Court's Fourth Amendment jurisprudence certainly seems convoluted. Even in *Carpenter* itself, members of the Court could not avoid quibbling over whether it might be best to return to a property-based conception of the Amendment's protections.[25] But in the main the Court has remained true to the fundamental precept that "[T]he Fourth Amendment protects people, not places," if not without some

18. Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018).
19. *See id.*
20. *See id.* (the government had claimed that the records in question had "clinched the case.").
21. Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018).
22. *Id.* at 2213 (quoting U.S. CONST. amend. IV, § 1).
23. *See id.* at 2221-22.
24. *See Carpenter*, 138 S. Ct. at 2218 (citing *Kyllo v. United State*s, 533 U.S. 27, 36 (2001)).
25. *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018) (Kennedy, J., dissenting); *see also Carpenter*, 138 S. Ct. at 2268 (Gorsuch, J., dissenting) (urging a return to a property-based conception of the Fourth Amendment's protections).

detractors from both sides of the legal spectrum.[26] While *Carpenter* might have presented a novel question, it relied in good part on history and tradition, holding clearly that Fourth Amendment analysis "is informed by historical understandings 'of what was deemed an unreasonable search and seizure when the Fourth Amendment' was adopted."[27] The amendment's protections work to "secure 'the privacies of life' against 'arbitrary power."[28] Perhaps more importantly, the Court reiterated that "a central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance."[29] Summarizing the Court's development of Fourth Amendment jurisprudence in *Carpenter*, Chief Justice Roberts explained that the Court has, since its decision in *Katz v. United States*, "expanded [its] conception of the Amendment to protect certain expectations of privacy."[30] In so doing, the Court began to develop a balancing scheme designed at least in part to respond to emerging societal privacy concerns in an increasingly digital and interconnected world, where personal information is collected and shared as a necessary part of everyday life.[31]

In seeking to solve questions involving "personal location information maintained by a third party," the Court stated that its analysis will be informed by two related "lines of cases."[32] The first, perhaps predictably, concerns what the Court has said about what an individual's expectation of privacy is in his physical location and movements.[33] Most recently, in *United States v. Jones*, "five Justices agreed that . . . privacy concerns would be raised by . . . [the government] conducting GPS tracking of [Jones'] cell phone."[34] The Court in *Carpenter* held that an individual has a reasonable expectation of privacy in one's physical location and movements.[35] The "second set of decisions" refers to the so-called third-party (consent) doctrine, which attempts to define the distinction between "what a person keeps to himself and what he shares with others."[36] In essence, the third-party doctrine holds that there is no "legitimate expectation of privacy" in information voluntarily given to a third-party vendor.[37] In *United States v. Miller*, the Court made clear that this also applies "even if the information is revealed on the assumption that it will be used only for a limited purpose."[38] The doctrine's analysis necessarily includes "the nature of the particular documents

26. Katz v. United States, 389 U.S. 347, 351 (1967). *But see* Kyllo v. United States, 533 U.S. 27, 42 (2002) (Stevens, J. dissenting).
27. *Carpenter*, 138 S. Ct. at 2214 (quoting *Carroll v. United States*, 267 U.S. 132, 149 (1925)).
28. *Id.* (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)).
29. *Id.* at 2214 (quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)).
30. *Id.* at 2210.
31. *See id.* at 2210-11.
32. *Id.* at 2215.
33. *Id.*
34. *Id.* (citing *United States v. Jones*, 565 U.S. 400, 430 (2012)).
35. *Id.* at 2212.
36. *Id.* at 2216.
37. *See* Smith v. Maryland, 442 U.S. 735, 743-44 (1979).
38. United States v. Miller, 425 U.S. 435, 443 (1976)

sought."[39] In *Smith*, for example, the Court considered the use of a "pen register," a type of wiretapping device used to record outgoing calls from a landline phone.[40] There the Court declined to extend the Fourth Amendment's protections, finding instead that the device had "limited capabilities" and that individuals don't really maintain a "reasonable expectation of privacy in the numbers they dial."[41]

In a modern world defined more by the ubiquity of cellphones than rotary phones and pen registers, however, Americans may well view the same question differently. Indeed, Justice Marshall in dissent in *Smith* presaged many of the concerns with the third-party doctrine that the Court later touched on in *Carpenter*, stating forcefully that he "remain[ed] convinced that constitutional protections are not abrogated whenever a person apprises another of facts valuable in criminal investigations."[42] Notably, Justice Marshall pointed out that "inherent in the concept of assumption of risk is some notion of choice."[43] In order to be thought of as taking on the chance that one's personal information might ultimately be accessed by the government, one must have an actual, even-handed choice in the matter; and yet "unless a person is prepared to forgo the use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance."[44]

In *Carpenter*, the Court seems to have sought a middle ground. While not jettisoning the idea of consent entirely, the Court endeavors to develop a way in which consent can be thought of in a useful way in the digital context. In this effort, the Court offers the notion of "affirmative act" as a plausible way of determining consent in an increasingly convoluted technological environment.[45] The Court mentions this idea of an "affirmative act" in attempting to explain why it did not make sense to think of Carpenter as somehow consenting to the sharing of his personal location information given the fact that at no point did he have to expressly agree to said sharing.[46] A person carries his cell phone simply as a fact of life, the Court reasoned, and as such it cannot be said that an individual engages in an "affirmative act"

39. *Id.* at 442.

40. *See Smith*, 442 U.S. at 742. It is worth noting, further, that a pen-register tracks only outgoing phone numbers. As such, while it remains a wire-tapping device in the technical sense, this meaning may not accord with modern perceptions of what wiretapping might entail.

41. *Id.* at 742-43; *see also Carpenter*, 138 S. Ct. at 2215 (quoting *Smith*, 442 U.S. at 742).

42. *Smith*, 442 U.S. at 748 (Marshall, J., dissenting).

43. *Id.*

44. *Id.*

45. Carpenter v. United States, 138 S. Ct. 2206, 2210 (2018).

46. *See id.* at 2211.

consenting to the sharing of highly personal data.[47] The Court in *Carpenter* then began its reasoning for declining to extend the third-party doctrine to cell-site location information ("CSLI") by noting that the technology of CSLI itself was "qualitatively different" and "unique."[48] In assessing whether the "logic" of the third-party doctrine should apply to CSLI, the Court holds out a slightly refined notion of consent as a basis for determining when and where to apply the third-party doctrine to evolving, modern technologies.[49] This necessarily involves an assessment of the ways in which the nature of the technology at issue affects the consent question. One can see this in the way that the Court cites the "qualitatively different" nature of CSLI, where it appears to suggest that the analysis is more-or-less case-by-case.[50] While in doing so the Court refrains from engaging in the sweeping type of constitutional pronouncement which might stir the hearts of privacy advocates, it at least purports to be attentive to the various and perhaps uncontemplated ways in which new technologies (each with their own applications) may fall within or outside of the third-party doctrine depending on their precise characteristics.[51]

What is more, the Court's discussion of the question of when to apply the third-party doctrine centers on the issue of increased technological sophistication: the wireless carriers at issue in the case are "ever alert" and possess "nearly infallible" memories.[52] And yet "an individual's reduced expectation of privacy in information knowingly shared with another 'does not mean that the Fourth Amendment falls out of the picture entirely."[53] Paramount, the Court intimated, is the pervasiveness of the technology itself and whether there are any inherent limitations on how far the technology in question might reach.[54] This multi-factor approach has the advantage of allowing the Court to mold its analysis to the circumstances as required; indeed, it is the same type of approach that allowed a majority of the Court to find that a "longer term GPS monitoring of . . . a vehicle traveling on public streets constitutes a search" in *United States v. Jones*.[55]

Underneath the surface in the Court's discussion of the third-party doctrine and its refusal to extend the doctrine to the "qualitatively different"

---

47. *See id*. It is worth noting, in this light, that the Court's opinion does not emphasize nor even make reference to Carpenter's act of signing a cell phone contract with his service provider as perhaps constituting an "affirmative act" sufficient to qualify as consent to location sharing. This might tend to suggest that the similar act of signing a privacy policy or analogous document in the ride-hailing context is not itself dispositive on the question of consent. This is in contrast to the dissents of both Justice Kennedy and Justice Thomas, who make a point of emphasizing Carpenter's act of signing a cell-phone contract as critical. *See id.* at 2225 (Kennedy, J., dissenting); *id.* at 2235 (Thomas, J., dissenting) ("Neither the terms of his contracts nor any provision of law makes the records his.").

48. *Id.* at 2212.

49. *Id.*

50. *Id.*

51. *See id.* at 2220.

52. *Id.* at 2221.

53. *Id.* (quoting *Riley v. California*, 134 S. Ct. 2473, 2488 (2014)).

54. *See id.* at 2222.

55. *Id.* at 2220 (Alito, J., concurring in the judgment) (citing *United States v. Jones*, 565 U.S. 400, 430 (2012)).

category of CSLI is the notion that the doctrine itself may have made sense at a time when tracking technology was far less sophisticated but perhaps cannot stand with the same force in the modern, digital age. Indeed, the notion that modern GPS tracking or other surveillance technologies might have sufficient "limiting capabilities" so as to justify application of the doctrine (as the pen register did in *Smith*) seems rather quaint given the proliferation of these technologies.[56] The Court's consideration of the subject raises a point originally made by Justice Marshall in dissent in *Smith*–namely the idea that no matter the extent of the invasion, one may well think that the breach itself cannot be thought of as the product of free and voluntarily provided consent where the technology in question constitutes a personal or professional necessity.[57]

As such, the Court's analysis of the "second rationale" behind the third-party doctrine–voluntary exposure–is necessarily tied to its consideration of the pervasiveness and sophistication of the technology at issue.[58] Noting the unique qualities of CSLI, the Court posited that the concept of voluntary exposure simply does not make complete sense when applied to CSLI.[59] For a start, the Court noted that "[c]ell phone location information is not truly 'shared' as one normally understands the term."[60] The Court then relied on its decision in *Riley* to argue that because cell phones are so ubiquitous, such an "insistent part of daily life," they are "indispensable to participation in modern society."[61] Simply put, it cannot be categorically asserted that an individual has "voluntarily exposed" himself to surveillance by virtue of his carrying a cell phone in public–as doing so is no different from his waking up in the morning and walking out the door. It is in this context that the Chief Justice explains that because Carpenter had not engaged in any "affirmative act" consenting to exposure of his personal location information but had instead simply existed in public with his phone on his person–as everyone does–he cannot be thought of as having agreed to invasive sharing of his personal location.[62]

The precise issue of whether an individual engages in an affirmative act consenting to the conveyance of his personal location information stored by a ride-hailing company, therefore, seems to pose a more difficult, closer question. The Court's explication of the "affirmative act" concept in *Carpenter* is, admittedly, rather terse and perfunctory; the term itself appears only once in the opinion, where the Court explains that 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 [the phone]."[63] As such, the Court reasons, one does not "truly share" cell phone location information in the ordinary

56. *Id.* at 2215 (citing *Smith v. Maryland*, 442 U.S. 735, 742 (1979)).
57. *See Smith*, 442 U.S. at 748 (Marshall, J., dissenting).
58. *Carpenter*, 138 S. Ct. at 2215.
59. *Id.*
60. *Id.* at 2220.
61. *Id.* (citing *Riley v. California*, 134 S. Ct. 2473, 2476 (2014)).
62. *Id.* at 2220.
63. *Id.*

sense.[64] The Court adds that this notion of one not truly sharing CSLI is bolstered by the fact that cell phones as a technology are incredibly "pervasive" to the point that having one is "indispensable to participation in modern society," negating the idea that free choice might have been possible.[65] Nonetheless, the Court admits that its use of the term "affirmative act" is meant to nod at the Court's discussion of assumption of risk in *Smith*, noting that "virtually any activity" on one's cell phone creates CSLI and that, "apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily 'assume[] the risk' of turning over a comprehensive dossier of his physical movements."[66]

B. How Lower Courts Have Been Implementing Carpenter: Teasing Out Lessons from Recent Interpretations

In *Carpenter*'s wake, lower courts have not had a terribly fulsome opportunity to consider its potential implications. Many recent decisions have sought simply to delineate situations where *Carpenter* clearly does not apply; consider a recent district court opinion in *People v. Torres*, which simply noted that *Carpenter* does not "address the constitutionality of search conditions imposed pursuant to probation or parole."[67] In *Torres* and similar cases, lower courts seem to be paying a good deal of attention to the nexus between the place where the search is conducted (as being somewhere where a law enforcement officer could otherwise lawfully be) and the sophistication of the technology being employed to obtain the evidence in question.[68] This seems to be in line with the principles distilled from *Carpenter*, where the Court devoted much of its discussion to the sophistication of CSLI technology and to whether the concept of voluntary exposure is tenable in the context of providing location information to third parties. The defendant in *United States v. Kubasiak*, for example, sought to use *Carpenter's* reasoning to assert that using a video camera to record a person's backyard 24 hours a day over several months violates reasonable expectations of privacy–but the Court there held that this argument ignores a critical element of the Court's reasoning in both *Jones* and *Carpenter*: because the surveillance camera was fixed, it could observe the defendant in only one location (i.e. his backyard).[69] This same argument has also been rejected in the case of pole cameras.[70]

It should be noted that the analysis, as the Court urged in *Carpenter*, centers here on the perceived pervasiveness of the technology, looking to what area is being intruded upon and what if any steps individuals have taken

---

64. *Id.*
65. *Id.*
66. *Id.* (quoting *Smith v. Maryland*, 442 U.S. 735, 745 (1979)).
67. People v. Torres, Super. Ct. No. SCN362581, 2018 WL 5004764, at *26 (Cal. Ct. App. Oct. 16, 2018)
68. *See* United States v. Kubasiak, No. 18-cr-120-pp, 2018 WL 4846761, at *3 (E.D. Wis. Oct. 05, 2018).
69. *Id.* at *4.
70. *See* United States v. Houston, 813 F.3d 282, 285 (6th Cir. 2016).

to prevent such intrusion. These recent cases seem consistent with the growing perception that tracking or surveillance technology that follows an individual constantly is sufficiently concerning so as to be constitutionally significant.[71] Static surveillance, as was at issue in the previously mentioned cases, seems to be something that people find inherently less invasive; when surveillance follows you, and the government can potentially gain access to a type of technology that keeps track of one's physical location over several places, such as one's destinations of travel, route of travel, among others, individuals seem more prepared to consider that invasion as infringing upon their basic rights and personal dignity.[72]

Some of these very recent considerations of *Carpenter* should offer a clue for the future. Lower courts have thus far had relative success in undertaking the type of multi-factor analysis urged in *Carpenter*, focusing on how much of an aggregate account of a person's life the technology in question seems to capture and whether it is similar in sophistication to that described in *Carpenter*–i.e. the "intimate details of everyday movement."[73] Lower courts in the wake of *Carpenter* seem to be suggesting a constitutionally significant nexus between the place where the information is being collected, whether such place is somewhere a law enforcement officer could otherwise be lawfully, the sophistication of the technology used to acquire the information (including whether that technology will grow more invasive), and just how aggregate of a picture the technology captures of a person's daily life.[74] The greater the nexus, the reasoning appears to be, the more likely a person can be considered to have a reasonable expectation of privacy in such information that is "voluntarily" conveyed to a third party.[75] This approach is in line with the multi-factor, fact-specific approach of *Carpenter*. As such, courts in the post-*Carpenter* world should endeavor to take into account the implications of technological growth for purposes of assessing expectations of privacy and consent.

If thought of this way, this string of factors offers a principled way of determining where the Court should apply sensible exceptions to the third-party doctrine in light of developing technology, weighing such factors as pervasiveness and advancing technological sophistication against the issue of whether an individual can be considered as engaging in an "affirmative act" consenting to the sharing of one's location information.[76] This argument applies with force to the ride-sharing context. Based on the Court's rationale in *Carpenter*, a warrant should be required to access individuals' location information when the technology at issue is both pervasive enough to reveal

---

71. *See Carpenter*, 138 S. Ct. at 2216; *cf.* United States v. Jones, 565 U.S. 400, 430 (2012).

72. *See* Aaron Smith, *Shared, Collaborative, and On Demand: The New Digital Economy*, PEW RES. CTR.: INTERNET AND TECH. (May 19, 2016), http://www.pewinternet.org/2016/05/19/the-new-digital-economy/ [https://perma.cc/AQ5N-XBAX].

73. *See Carpenter*, 138 S. Ct. at 2217.

74. *See* United States v. Kubasiak, No. 18-cr-120-pp, 2018 WL 4846761 at *3-4 (E.D. Wis. Oct. 05, 2018); *cf.* United States v. Jones, 565 U.S. 400, 406 (2012).

75. *Carpenter*, 138 S. Ct. at 2216.

76. *Id.* at 2214.

intimate details of one's life (and promises to grow more sophisticated) and when circumstances strongly suggest that an individual could not be thought of as providing genuine consent to the sharing of that information.

C. Varying Assessments of Carpenter and its Implications

The *Carpenter* decision's muddling of the third-party doctrine gained immediate attention. Orin Kerr, a noted Fourth Amendment scholar, has noted that the *Carpenter* opinion seems to go so far as to introduce what he calls an "equilibrium-adjustment cap" on the third party doctrine.[77] By this, it is meant that the decision aims to adjust the scope of the amendment's protections in light of new facts and technology in order to maintain a baseline level of liberty against unjustified intrusions of government power.[78] As Kerr aptly suggests, *Carpenter* appears to say that where the third-party doctrine would seem to give the government unduly expansive powers, the doctrine itself should not apply; this distinction, he notes, is borne out by the text of the opinion itself, where the Court notes that there is "a world of difference between the limited types of personal information addressed in Smith and Miller and the exhaustive chronicle of location information casually collected . . . today."[79] It is a distinction worth noting, for the future debate on this issue may well center on how "exhaustiveness"–or, to put it another way, technology's pervasiveness–is to be defined.

Much discussion in the wake of the Court's pronouncement has attended to what, if any, other types of location information might be implicated either by the ruling itself or by suggestions that one might reasonably draw from the Court's reasoning.[80] Kerr himself, in a draft chapter of a new book on the Fourth Amendment in the digital age, has recently put forth the argument that the user-location records of ride-hailing services do not constitute examples of data collection that should trigger a search.[81] Kerr argues, in the main, that *Carpenter* should apply to Internet (digital) records once three requirements are satisfied: the records must "exist because of the digital age," they must be "created without meaningful voluntary choice," and they must "tend to reveal the privacies of life."[82] He proceeds to argue, albeit briefly, that Uber location records do not satisfy this test at least under the

---

77. Orin S. Kerr, *Understanding the Supreme Court's Carpenter Decision*, LAWFARE BLOG (June 22, 2018, 1:18 PM), https://www.lawfareblog.com/understanding-supreme-courts-carpenter-decision [https://perma.cc/P7W6-6UPG] [hereinafter Kerr, LAWFARE BLOG]; *see also* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 490-91 (2011).

78. *See* Kerr, LAWFARE BLOG, *supra* note 77.

79. *Id.* (quoting *Carpenter*, 138 S. Ct. at 2216).

80. *See, e.g.*, Andrew Guthrie Ferguson, *Future Proofing the Fourth Amendment*, HARV. L. REV. BLOG (June 25, 2018), https://blog.harvardlawreview.org/future-proofing-the-fourth-amendment/ [http://perma.cc/W8B4-7CTR].

81. Orin S. Kerr, Implementing Carpenter, THE DIGITAL FOURTH AMENDMENT (Oxford University Press, forthcoming) (2019), USC Law Legal Studies Paper No. 18-29, https://ssrn.com/abstract=3301257 [https://perma.cc/5GUF-FE8F] [hereinafter Kerr, THE DIGITAL FOURTH AMENDMENT].

82. *See id.*

second prong and potentially under all three.[83] The remainder of this Note, accordingly, will seek to demonstrate why that view does not constitute the best reading of *Carpenter* as applied to ride-hailing location data records. To begin with, it will argue that the proper post-*Carpenter* test is not as narrow as Kerr suggests. It will first explicate the functioning of ride-hailing apps and look to prevailing attitudes concerning such apps' collection of data. Having done so, it will turn to what this Note considers the proper test for *Carpenter* searches and argue why ride-hailing location data meets that test. In particular, it will endeavor to explain why Carpenter's affirmative act distinction proves unhelpful in this context and why looking for meaningful voluntary choice is not fully satisfactory when many individuals in fact rely on ride-hailing services for freedom of movement.[84] In order to consider how a broader reading of *Carpenter* would apply to the ride-hailing context, it will first be necessary to consider the precise functioning of these services.

IV. THE PROLIFERATION OF RIDE-HAILING APPLICATIONS IN AMERICAN LIFE AND IMPLICATIONS FOR POLICE SURVEILLANCE

Because the precise legal questions involved appear to turn on application of the third-party doctrine and specifically on an analysis of how *Carpenter's* affirmative act distinction holds up in the ride-hailing context, it will first be necessary to consider the precise manner in which ride-hailing applications operate, and the degree to which individuals understand how ride-hailing companies function and their expectations of privacy in information collected by those companies in the course of soliciting their services. Having done so, Section IV will argue that in light of the relative sophistication and pervasiveness of ride-hailing services, the way in which individuals interact with said services, and the complications attendant to consent in the digital realm, a person does not truly consent to the sharing of their personal location information when using a ride-hailing service.

Ride-hailing apps have transformed from a relatively novel concept to an increasingly present role in American life within a span of less than a decade, particularly for young urban Americans.[85] Uber is now a 15-billion-dollar company with over 750,000 drivers in the United States alone.[86] What is more, these apps offer and provide something that taxi companies cannot: individualized, location-based services with a pre-set charge.[87] Indeed, this rise to prominence has been so rapid as to generate relatively little litigation involving direct police action.[88] And yet one-in-five Americans have used a

83. *See id.*
84. *See* Smith, *supra* note 72.
85. *See id.*
86. Sara Ashley O'Brien, *Uber Has More Work to Do Winning Over Drivers*, CNN BUSINESS (Dec. 18, 2017), https://money.cnn.com/2017/12/18/technology/uber-drivers-180-days-of-change/index.html [https://perma.cc/EKT3-4YB6].
87. *See* Smith, *supra* note 84.
88. *Id.*

ride-sharing app.[89] Coverage is highly concentrated in cities and relatively sparse in rural areas–only three percent of rural residents have used such an app.[90] And while the tracking technology used by these companies to gather users' locations has only grown more sophisticated, until the Court's decision in *Carpenter* this past term, a potential constitutional problem with obtaining access to this information may well have seemed remote.[91] Such expansion makes it all the more likely that courts will have to address difficult legal questions related to the privacy of information shared with and processed by such companies, just as courts have had to address a variety of questions surrounding the privacy of information stored by cell phone companies as those companies have grown more technologically sophisticated and put out increasingly high-tech products.[92]

In principle, the technology at issue in *Carpenter*–CSLI–and the type of GPS technology used by ride-hailing companies such as Uber are remarkably similar. Indeed, insofar as GPS tracking provides the same type of data–i.e. an individual's location over time–it parallels the type of GPS device at issue in *United States v. Jones*.[93] Whenever an individual walks or otherwise exists in public, that person's cell phone routinely sends or "pings" location signals to nearby cell towers; using the information gathered from several cell towers, it is possible to "triangulate" a phone's location (and thereby, almost invariably, a person's).[94] In this basic respect, the precision of the respective technologies is almost exactly parallel. Uber, as a typical example:

> [C]ollects location information when the Uber app is running in the foreground. In certain regions, Uber also collects this information when the Uber app is running in the background of your device if this collection is enabled through your app settings or device permissions.[95]

This is distinct from the "ping" function of almost all modern cell phones. Location tracking in the ride-hailing context arises when that particular service is solicited by the phone user–not so with ordinary "pings" to cell towers; put in simpler terms: if someone has started running the Uber app on a phone in order to solicit a car, that person's location will be tracked.[96]

---

89. *Id.*

90. *Id.*

91. *See, e.g.*, Andrew Hawkins, *How Uber Moves the 'Blue Dot' to Improve GPS Accuracy in Big Cities*, THE VERGE (Apr. 19, 2018), https://www.theverge.com/2018/4/19/17252680/uber-gps-blind-spot-shadow-maps [https://perma.cc/7A9B-YNZ5].

92. *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2476 (2014) (holding that police must obtain a warrant before conducting a search of an individual's phone and its contents).

93. *See* United States v. Jones, 565 U.S. 400, 415 (2012) (where the Court concluded that the placing of a physical tracker on a car constituted a search).

94. *See* Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018).

95. *See Privacy Policy*, Uber Technologies, Inc. (May 25, 2018), https://privacy.uber.com/policy [http://perma.cc/RW94-HYDR].

96. *See id.* (noting that "if you are a rider and have provided permission for the processing of location data, Uber collects location information when the Uber app is running in the foreground. In certain regions, Uber also collects this data when the Uber app is running in the background of your device if this collection is enabled through your app settings or device permissions.").

Moreover, unless that individual has not deliberately disabled the tracking function through accessing the app settings, the app will continue to track a user's location "in background," even though the person may be doing other things on the phone such as texting or calling.[97] This means that so long as the user has not specifically closed that app, one's location will be tracked for a brief period; for Uber, until as recently as 2017 this meant that users continued to be tracked for a short window after they left vehicles and entered buildings.[98]

Uber, to its credit, seeks to provide law enforcement authorities with guidance regarding what procedure the company will follow in the event that police contact the company for information. Its guidelines, however, are unsettlingly permissive. According to Uber's "Guidelines for Law Enforcement Authorities," police must create an online account through the "Uber Law Enforcement Response Team" and submit any requests for information through an online portal.[99] In one subsection, Uber states the following:

We require a subpoena issued in connection with an official criminal investigation to compel the disclosure of basic information. A search warrant issued under the procedures described in the Federal Rules of Criminal Procedure or equivalent state warrant procedures upon a showing of probable cause is required to compel our disclosure of certain communications between people using Uber or GPS location information.[100]

The policy goes on to state that:

> Exceptions to these requirements may be available for emergency and exigent requests, where a user has provided consent, or–for requests that do not require a warrant–where other legal or regulatory standards apply.[101]

This vague reference to "consent" without express definition of the term makes Uber's policy ripe for abuse, threatening to swallow the company's self-imposed requirements.[102] By its own terms, Uber's policy does clearly delineate the circumstances in which a user would be understood as having provided consent. Must the user expressly agree? Is his or her use of the app enough? These would seem to be important questions but their resolutions are left unclear. The lack of a clear definition of what is meant by consent in this

97. *See id.*

98. *See* Laurel Wamsley, *Uber Ends Its Controversial Post-Ride Tracking of Users' Location*, NAT'L PUB. RADIO (Aug. 29, 2017, 05:41 PM), https://www.npr.org/sections/thetwo-way/2017/08/29/547113818/uber-ends-its-controversial-post-ride-tracking-of-users-location [https://perma.cc/SRV9-QYQE].

99. *Uber Guidelines for Law Enforcement Authorities – United States*, Uber Technologies, Inc. (last visited Feb. 28, 2019), https://www.uber.com/legal/en/document/?country=united-states&lang=en&name=guidelines-for-law-enforcement.

100. *Id.*

101. *Id.*

102. *Id.*

context necessarily raises the issue of how that very concept is to be understood in the digital age.

If a user does not exercise the option to disable the tracking function of the Uber app, the resulting location data can provide an extensive window into a person's physical movements over a prolonged period, similar to the CSLI data profile at issue in *Carpenter*.[103] Uber keeps location data about past rides stored off-site.[104] During each ride, Uber stores a number of data points, the most salient of which are: a user's pickup location, drop-off location, precise route path, and duration of trip.[105] Interestingly, available data tends to show that a majority of adults say they are either not too confident or not at all confident that records of their activity maintained by their own cellular telephone company would remain private and secure.[106] While Americans understand that "modern life won't allow them to be 'left alone' and untracked, they do want to have a say in how their personal information is used."[107] 74 percent say it is "very important" to be in control of who can get personal information and 65 percent say it is "very important" to control what personal information is collected.[108] In terms of how aware people are of how their information will be used once shared, 47 percent of people said they were unsure of how their personal information would be used by companies; 91 percent of adults either agree or strongly agree that consumers have lost control of how personal information is collected and used by companies.[109] Indeed, this would seem to undercut the notion that individuals have true choice in the digital realm; if individuals see that they are provided the option of allowing or disallowing location tracking but already believe that they do not have free control over that choice, it undermines the concept of consent in this context.

In terms of the sensitivity of personal location information, 50 percent of people state that the details of one's physical location over time are "very sensitive," and another 32 percent agree that such information is "somewhat sensitive."[110] These attitudes involve implicit assumptions about "privacy tradeoffs," including the "likelihood of getting spam, the risk of data breaches, [and] the special intimacy tied to location data."[111] The most strongly negative reactions in this poll came in the context of scenarios involving the sharing of personal location data. One respondent even went so

---

103. *See* Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018) (explaining how CSLI tracks personal movements over a prolonged period).

104. *See Privacy Policy*, *supra* note 95 (discussing information created when individuals use the service, including "location, usage, and device information.").

105. *See id.*

106. *See The State of Privacy in America*, PEW RES. CTR. (Jan. 20, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/ [https://perma.cc/9CAN-UYUW].

107. *Id.*

108. *Id.*

109. *Id.*

110. *Id.*

111. Lee Rainie & Maeve Duggan, *Privacy and Information Sharing*, PEW RES. CTR.: INTERNET AND TECH. (Jan. 14, 2016), http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/ [https://perma.cc/Z9F9-SVT9].

far as to say that he "continually den[ies] location services" on his smartphone out of a desire to block ads.[112] It would be concerning indeed, in this light, for location data to be collected ostensibly so that a ride-hailing company can improve its service or lower rates, but then also employed for police to have a more efficient tracking system for people without expressly violating privacy rights.

V. APPLICATION OF CARPENTER'S RATIONALE TO RIDE-HAILING LOCATION DATA

A. Technological Sophistication and Pervasiveness: Records of the Digital Age and Privacies of Life

Under the proper post-*Carpenter* framework, the Court should turn first to a consideration of how pervasive and sophisticated a particular tracking technology is. This is borne out by the Court's fact-heavy discussion in *Carpenter* itself, detailing the precise functioning of CSLI and how much data it captures.[113] It is also borne out by the Court's attention to the fact that the CSLI technology at issue in the case was then just beginning to grow in sophistication and capability: only getting better, more sophisticated, and better able to see exactly where an individual has travelled.[114] As such, the Court need not be tied to the exact mechanics of the technology with which it is faced and can instead take notice of the abstract, big picture: to what degree of sophistication a technology can reasonably be thought of as heading. This type of broader approach takes account of increasing technological sophistication in a way that is inherently more pragmatic, treating new forms of technology and tracking for what they actually are: substantively different settings entirely, where old modes of thinking may not necessarily translate neatly. Now, Prof. Kerr says that the first consideration in post-*Carpenter* cases in the digital sphere should be whether the records at issue exist "because of the digital age."[115] Although his framework takes account of such issues as sophistication and pervasiveness later on, this specific formulation risks making the analysis overly narrow. Moreover, the very answer to that question requires a definition of the "digital age" and its consequences.

Opponents such as Kerr also point out that because cab companies have compiled records of trips in the past, courts now need not be concerned about Uber location records as a new type of data record.[116] Yet this misses the forest for the trees. In pulling back to a broad level of abstraction, this argument seeks to indicate that this type of record, in its most basic form, in fact has a long history. But in so doing it clouds the nature of the technological revolution that enabled Uber to track and collect user data. Uber in fact collects extremely precise information: where an individual called for a ride,

112. *Id.*
113. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).
114. *Id.* at 2215.
115. Kerr, THE DIGITAL FOURTH AMENDMENT, *supra* note 81.
116. *Id.*

where that individual was picked up, how long the ride to the destination took, and what exact route that individual used.[117] That precision and sophistication is itself possible because of the advent of GPS technology and the feasibility of recording that information digitally. It would certainly be unrealistic to expect a cab company as recently as the 1980s to be capable of compiling such extensive information.

When one takes full stock of the nature of the information that ride-hailing services collect, moreover, it seems doubly unrealistic to think that records of one's comings and goings will not "tend to reveal the privacies of life" in the same way as CSLI data that shows one's location over a period of weeks.[118] Having access to the details of an individual's trips to and from specific locations, at specific times and along exact routes may indeed provide a window into that person's intimate associations and affiliations. In this respect, it would seem a vapid distinction to say that CSLI data is pervasive enough to risk revealing one's personal associations and yet the records of where an individual chooses to travel is not at least similarly revealing. If, as the *Carpenter* Court held, the "mapping [of] a cell phone's location over the course of 127 days provides . . . an intimate window into a person's life," and if further it is true that this window reveals "familial, political, professional, religious, and sexual associations," then it is difficult to imagine how a comprehensive record of one's Uber trips over the course of even one or two weeks would not also tend to reveal an individual's political, professional, and personal associations.[119] This may well include, as Justice Sotomayor aptly points out in her concurrence in *Jones*: "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club . . . the gay bar and on and on."[120] One would be hard pressed indeed to find that ride-hailing location records don't tend to reveal intimate associations in the same way as GPS data did in *Jones*.

B. The Affirmative Act Distinction in the Ride-Hailing Context: How to Assess the Consent Issue as Applied to Ride-Hailing Location Data

Given the similarities outlined earlier between CSLI and the GPS location information stored by Uber and similar ride-hailing applications, the remaining question of whether a user of a ride-hailing app can be thought of as consenting to the sharing of his or her physical location information comes to the fore. Under the *Carpenter* framework, the question in the digital, ride-hailing records context turns on the Court's usage of the phrase "affirmative acts" and its analysis thereof.[121] The crux of the Court's argument was that

---

117. *See Privacy Policy*, *supra* note 95 (discussing information created when individuals use the service, including "location, usage, and device information.").

118. *See* Kerr, THE DIGITAL FOURTH AMENDMENT, *supra* note 81.

119. Carpenter v. United States,138 S. Ct. 2206, 2217 (2018); *see also* United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

120. *Jones*, 132 S. Ct. 565 U.S. at 415 (2012) (Sotomayor, J., concurring) (quoting *People v. Weaver*, 12 N.Y.3d 433, 441-42 (2009)).

121. *Carpenter*, 138 S. Ct. at 2214.

Carpenter did not engage in any "affirmative act" consenting to his constant tracking by his phone company but instead simply carried his phone on his person, as most people do; as such, he cannot be thought to have "agreed" or "consented" to his tracking in any traditional or even ordinary sense.[122] As mentioned, Orin Kerr interprets the Court's discussion of the same subject to contend that a user of a ride-hailing app does in fact engage in "meaningful voluntary choice" when using the service so as to lose Fourth Amendment protection.[123] Among the reasons he offers for why a user does in fact provide meaningful consent in this setting is the notion that users remain free to exercise other, less invasive travel options such as taxi cabs, buses, subways, or personal vehicles.[124]

Such questions necessarily raise the issue of what the very notion of "being free" means in the context of digital interactions. The concept of voluntary exposure in the ride-hailing context poses new questions and several factual distinctions from the CSLI-*Carpenter* context. Whereas individuals owning a cell phone carry their phones with them in public as a fact of life, all individuals need not download a ride-hailing app or otherwise engage in that service as a part of existing in society in the same way. A user of a ride-hailing service, moreover, might be thought of as engaging in several "affirmative acts" consenting to exposure of location information, including the act of downloading the app itself and failure to exercise the option of disabling automatic GPS tracking. It certainly is also true to an extent that in at least some instances users will remain free to solicit other travel options. What these and other distinctions fail to take stock of, however, is the fact that many individuals in fact rely or may in time rely on such services for personal freedom.[125] As the Court mentioned in *Carpenter*, and as Justice Marshall suggested in dissent in *Smith*, in considering whether a particular type of location information is "truly shared as one normally understands the term," attention must be given to whether an individual had actual, free choice in exercising the affirmative acts previously described.[126]

Assessing consent in this context requires a wide-angle lens. The percentage of people actively employing the use of a ride-hailing app is far from ubiquitous.[127] While ride-sharing applications function in a distinct way to the ordinary carrying of a cellphone, lower courts do not seem to have analyzed thus far whether that distinction is enough of a difference to warrant a different constitutional outcome.[128] Comparing any particular technology or

122. *Id.* at 2219-20.

123. *See* Kerr, THE DIGITAL FOURTH AMENDMENT, *supra* note 81.

124. *See id.*

125. *See* Smith, *supra* note 72 (explaining that 80% of users feel than ride-hailing apps offer good job options for those wanting flexible work schedules, as well as a routinely cheaper method of transport that traditional cab services).

126. Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018); *see also* Smith v. Maryland, 442 U.S. 735, 748 (1979) (Marshall, J., dissenting).

127. *See* Smith, *supra* note 72 (noting that 15 percent of American adults have used a ride-hailing service).

128. *See* United States v. Kubasiak, No. 18-cr-120-pp, 2018 WL 4846761, at *3-4 (E.D. Wis. Oct. 05, 2018) (finding no reason to extend protection to minimally invasive technologies).

service to the cell phone, however, is not in an especially useful distinction given the uniquely ubiquitous status of that technology. A broader view is necessary to inform the discussion and to reveal how the interactions and perceptions of Americans in the digital realm color the analysis of consent.

It might be useful for a court to use the kind of analysis undertaken in *Kubasiak* to inform its consideration of whether the third-party doctrine should apply.[129] The *Carpenter* Court certainly seems to be saying that in determining whether to apply the third party doctrine, a number of factors matter, including: sophistication of technology, the breadth of information collected, the personal and intimate detail of one's physical movements, among others.[130] By focusing on these factors, the *Carpenter* Court was able to make clear the stakes involved: access to technology that keeps an exacting track of an individual's precise location over several days (and weeks) implicates privacy concerns in a way that society is apt to regard as unreasonable.[131] This is quite similar to the nexus idea suggested earlier. That is to say, the most sensible post-*Carpenter* approach would seem to be undertaking an intense analysis of the mechanisms of the technology in question and making a determination of just how intrusive it might be.[132]

As argued, in the ride-sharing context each factor seems to tip the balance in favor of privacy and protection. The standout contravening factor, then, would appear to be the fact that users must download and thereby seemingly consent to a ride-hailing service's tracking system. The question, as such, seems to become whether an individual's failure to disable location information tracking constitutes an "affirmative act" that can be seen as constituting consent to ride-hailing location tracking.[133] Failing to do so, or failure to exercise other potential affirmative acts (such as choosing to take the bus), however, should not constitute an affirmative act under the *Carpenter* framework because it is both inconsistent with the way the Court discusses privacy expectations in that case and because doing so would constitute a misguided way of thinking about the interaction between individuals and modern digital technology.

While perhaps no technology may rise to the level of ubiquity and personal significance as that achieved by the cell phone, ride-hailing apps have become a key element of the American digital landscape and in in the lives of their users; by overwhelming margins, users of such services agree that the services themselves save users time and stress, provide decent work for those who desire flexible hours, and serve as a critically important option for older adults with limited mobility.[134] Ride-hailing services for many individuals serve vital interests of personal autonomy, work freedom,

---

129. *See id.*

130. *Carpenter*, 138 S. Ct. at 2220-21 (detailing the ways in which CSLI offers a deeply personal look into an individual's physical movements).

131. *See id.*

132. *See* Ferguson, *supra* note 80 (suggesting an ad-hoc approach might be best suited to modern developments).

133. *Carpenter*, 138 S. Ct. at 2220.

134. *See* Smith, *supra* note 72.

mobility, and personal safety.[135] Interestingly enough, however, the same study previously cited found that the issue of privacy concerns "largely fails to register with ride-hailing users," with users rejecting "by a five-to-one margin" the "notion that these services collect too much personal information."[136] Those who use such services on a less-than-weekly basis are largely unsure on the same question.[137] Indeed, this might be read as reflecting broader public skepticism at being able to realistically preserve privacy upon entering and engaging with the digital realm.

Another relevant consideration in this context is the way in which Americans writ large think about their interaction with new ride-hailing services. An inherent assumption of the third party doctrine as announced in both *Smith* and *Miller* is that, as the *Carpenter* Court surmised, individuals have reduced expectations of privacy in information conveyed to third parties.[138] As Justice Marshall's dissent in *Smith* seems to have presaged, it is becoming increasingly apparent that Americans are in fact becoming more closely guarded in terms of information that they provide to third parties; Pew Research shows that a majority of Americans remain wary of the growth of surveillance: a majority (57 percent) consider it unacceptable for the government to monitor the communications of U.S. citizens.[139]

With this context in appropriate focus, it would seem that the very concept of consent in the context of the digital interaction is a somewhat shaky one. Indeed, given the way in which people interact with modern technology, the affirmative act distinction fails to serve as a completely satisfactory effort at line-drawing. Individuals are rarely if ever asked, and yet are apparently expected, to consent to constant location tracking as a fact of life. The notion that individuals forfeit Fourth Amendment protection by somehow choosing to solicit a ride-hailing service that utilizes location tracking fails to take proper cognizance of individuals' relation to the digital realm. Because ride-hailing services for many individuals broaden the ability and access to travel so as to enable increased mobility and thereby greater personal autonomy, can it truly be said that such an individual engages in a genuine choice to reveal one's location data through the use of a ride-hailing service?[140] Is that choice not thrust upon them as a result of circumstances outside of any one individual's control? One may indeed counter that an individual retains the option of not soliciting the service at all, as Kerr contends, but for individuals who rely on such services for basic autonomy that would seem to ring hollow.[141]

Consider also the sheer volume of interaction that individuals undertake with digital applications and the attendant wealth of user-agreements that a user must encounter: one study in particular indicates that for the average

---

135. *See id.*
136. *Id.*
137. *Id.*
138. *Carpenter*, 138 S. Ct. at 2215.
139. *See* Smith v. Maryland, 442 U.S. 735, 748 (1979) (Marshall, J., dissenting); *see also The State of Privacy in America*, *supra* note 106.
140. *See* Smith, *supra* note 72.
141. *See* Kerr, THE DIGITAL FOURTH AMENDMENT, *supra* note 81.

American interacting in the digital realm, it would take 76 eight-hour work days to read all the privacy polices one encounters in a year.[142] Would it not be reasonable to say, therefore, that meaningful consent in this area is a hollow term so long as Americans do not have another feasible option but to participate in the digital sphere? Richard Epstein, along these lines, argues that "[t]he automated nature of ubiquitous and involuntary [digital] connection undercuts the consensual nature of the exposure."[143] This goes to the same point: the digital world, with all of its connections, requires individuals, to engage both instantly and fully in order to function in the same fashion as everyone else. If the initial decision to engage is itself not truly voluntary, then the idea that someone can somehow provide meaningful consent in each minute interaction, especially when such an interaction involves location tracking, seems to fail.

To argue that an individual somehow consents to revealing personal information simply through using a ride-hailing service when he or she has other options available also does not accord with many of the Court's prior statements on this issue. At least one amicus brief in *Carpenter*, for example, emphasized a point made by Justice Sotomayor in her concurrence in *Jones* that "[t]he third-party doctrine's central tenet . . . does not . . . accord with the expectations most people have when transmitting information for a specific purpose."[144] One might readily think of a ride-hailing app in a similar fashion; a user of such an app expects to convey location information specifically so as to enable the trip in question and in all likelihood does not expect to have his or her whereabouts become, by virtue of the limited trip, public knowledge.

Even prior to the Court's recent expression of doubt towards the third-party doctrine, at least some commentators were beginning to recognize the growing failure of the doctrine to accord with developing, modern expectations of privacy. With regard to stored location information, one scholar at least has pointed out that it is "unreasonable to consider data somehow 'not private' if the information, like CSLI, is generally exposed only to automated systems rather than human employees."[145] Indeed, in the ride-sharing context–location data is similarly stored in an off-site automated program, tending to diminish the notion that the location data is not private by virtue of its sharing with a third party.[146] That thinking extends to the idea

142. Lorrie Faith Cranor & Aleecia McDonald, *The Cost of Reading Privacy Policies*, 4:3 I/S: A JOURNAL OF L. & POL'Y FOR THE INFO. SOC'Y 546, 554-58 (2008); *see also* Alexis C. Madrigal, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*, THE ATLANTIC (Mar. 1, 2012), https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/ [https://perma.cc/JJ8A-6KVU].

143. *See* Richard A. Epstein, *Privacy And The Third Hand: Lessons From The Common Law Of Reasonable Expectations*, 24 BERKELEY TECH. L.J. 1199, 1206 (2009).

144. *See* Brief of Scholars of Criminal Procedure and Privacy in Support of Petitioner, p. 16, Carpenter v. United States, 138 S. Ct. 2210 (2018) (quoting *United States v. Jones*, 565 U.S. at 417 (2012) (Sotomayor, J., concurring)).

145. *Id.* at 17 (quoting Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 611-27).

146. *See Privacy Policy*, *supra* note 95.

that the doctrine even properly applies in situations where the government simply seeks to compel the production of evidence rather than conduct a search.[147] Here, the implications of holding that the government does not always need a warrant in order to collect stored location information obtained through third parties would be grave indeed. In effect, the government could simply outsource a highly sophisticated system of surveillance created and deployed by ride-hailing companies with thousands of employees, all while avoiding the costs of developing new tracking technology and being subject to exactly none of the privacy rights that citizens have come to expect; it is a concern that tracks with the Court's recent expression of skepticism of broadly invasive surveillance techniques.[148]

This would seem to be supported by data detailing how few people actually understand how ride-sharing apps collect user data; statistics cited above show that few if any users of Uber actually are aware of how the app stores their location data and few if any are aware that there is an option for disabling the tracking function.[149] It is reasonable to think that individuals might be unaware of such options precisely because they understand that in order to participate in the modern digital public environment on an even plane with others, they cannot simply detach themselves from its pervasive interconnectedness; this is especially true for individuals who actually need ride-hailing services to enable work freedom.[150]

And yet this very point seems to admit of something of a sliding scale of voluntary exposure and expectations of privacy. Should the notion that an individual at least has somewhat practical access to alternate forms of transportation, for example, matter in how a court conducts its analysis? Admittedly, an individual might easily find alternative forms of transport–be they public (subway, public bus) or semi-private. Indeed, this forms a key part of Kerr's argument for why Uber-location records would not be protected.[151] While individuals who may actually rely on private ride-hailing apps for freedom and mobility might have a stronger claim to be considered as not engaging in voluntary exposure by virtue of their use of such apps, can the same truly be said for individuals not reliant on such apps for personal travel? In the case of such individuals, the fallback necessarily seems to be the foundational expectation that one has a reasonable expectation of privacy in the intimate details of physical location and movement, as articulated in *Carpenter*.[152] Indeed, if the nature of the physical movement in itself is indistinguishable between the two classes of individuals, whereas the reasons

147. *See, e.g.*, Sherry Colb, *What Is a Search: Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 121 (2002).

148. *See* Riley v. California, 134 S. Ct. 2473, 2478 (2014) (holding that the government must obtain a warrant to search the contents of an individual's cell-phone); *see also* United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) (stating that the third-party doctrine does not make sense in a world of rapidly expanding technologies and shifting privacy expectations).

149. *See* Smith, *supra* note 72.

150. *See id.*

151. *See* Kerr, THE DIGITAL FOURTH AMENDMENT, *supra* note 81.

152. *See* Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018).

for engaging in such transport may be different, perhaps there can be no tenable difference between the two.

When thinking of the issue principally in terms of consenting to the tracking itself, much of the reasoning of *Carpenter* translates to this new context. The concept of affirmative acts may yet be a principled distinction for some types of technology, where it might be possible to hold individuals to a clearer, more express standard of consenting to tracking. In the context of personal travel, however, where physical location is implicated, the affirmative act distinction fails to capture the full breadth of how people interact with modern technology and what their expectations are. To say that a user retains other, less personally invasive options does not capture the breadth of the problem and fails to take stock of the challenges and realities consumers face in the digital world.

VI. CONCLUSION: RE-CONCEPTUALIZING PRIVACY IN STORED LOCATION INFORMATION IN THE DIGITAL AGE

This Note is not meant to suggest or urge that the same conclusion should follow in the context of other types of stored location information. Instead it argues in sum that in the future analyzing questions of this sort not only depends upon a detailed analysis of the type of technology at issue and just how personal the information collected through it is, but also on a fundamental rethinking of the idea of consent itself in the context of new technologies in light of the way that the modern citizen engages with an ever-expanding grid of collected information. To his credit, Kerr seems to agree that measured analysis of a given technology's pervasiveness and sophistication is critical in this context. What his analysis seems to miss, however, is a framing of the consent question that makes intuitive sense in light of modern, personal interactions in the digital sphere. The affirmative act framework may yet prove to be a useful basis for distinguishing when a particular user of a technology can be thought of as having consented to tracking or other revealing of personal information in such a way as to provide an exception to the Fourth Amendment's requirements. In the context of the ride-hailing app, however, it fails to provide a fully satisfactory way of framing the issue.

Carpenter itself was a narrow decision, and while this Note argues it can be read more broadly there may yet be room for principled distinctions where the Court allows for limited, required disclosures.[153] Arguments limiting *Carpenter* to its facts risk overlooking the ways in which tracking methods used by ride-hailing services intrude into the personal sphere; CSLI was often indicative of the "general area" someone was in, but rarely ever indicative of the exact places someone had been and exact routes of travel.[154] As courts continue to grapple with the question of just how sophisticated and pervasive a particular technology must be before protection can be extended,

153. *See id.* at 2214-15.
154. *Id.* at 2211.

a more ready solution might perhaps be found within the halls of Congress. The House of Representatives is in the process of conducting hearings on the subject of the need for a new comprehensive federal privacy and consumer protection law.[155] Putting aside for the moment the question of what precise form any bill should take, and perhaps the larger questions swirling in consumer protection circles, a law of this form would be a welcome addition to the legal landscape. Testimony provided this February has already emphasized that individuals are often compelled to engage with the current digital environment in a way that does not suggest the presence of genuine choice.[156] The lack of a sufficiently clear legal answer to the problem suggests that it is time for the people at large to express their will, so as to clearly define consent in this new context.

155. *See Protecting Consumer Privacy in the Era of Big Data: Hearing Before the Subcomm. on Consumer Protection and Commerce of the H. Comm. on Energy and Commerce*, 116th Cong. (2019).

156. *See id.* (statement of Nuala O'Connor, President and CEO, Center for Democracy and Technology).