NOTES

LAUNDERING DATA: HOW THE GOVERNMENT'S PURCHASE OF COMMERCIAL LOCATION DATA VIOLATES *CARPENTER* AND EVADES THE FOURTH AMENDMENT

*Dori H. Rahbar**

In 2018, the Supreme Court decided in Carpenter v. United States *that the government requires a search warrant to access seven days or more of certain location data that comes from mobile devices. In 2020, however, news broke that different government agencies had purchased location data from data brokers and used them for law enforcement purposes. Because the Fourth Amendment does not regulate open market transactions, it is now an open question whether the government can lawfully buy location data from the open market like any private-sector entity. Courts have yet to address whether* Carpenter *restricts the government's ability to purchase location data rather than obtain it by a legal instrument—in other words, whether the government can nonetheless "buy" its way around Fourth Amendment requirements. This Note proposes that* Carpenter *restricts such practices when purchased data is functionally equivalent to the location data—cell-site location information—in which* Carpenter *found individuals have an expectation of privacy. It proposes that* Carpenter *restricts the government from purchasing location data for which it would otherwise require a warrant if obtained by demand.*

INTRODUCTION 714
I. THE CURRENT LANDSCAPE OF LOCATION DATA 718
A. An Overview of Location Data 718
B. The State of the Law Concerning Location Data 723
1. The Dearth of Current Law Governing Location Data 723
2. The Fourth Amendment's Current Treatment of Location Data Records 726

* J.D. Candidate 2022, Columbia Law School. Thank you to everyone who brought this Note together: first, to Professor Daniel Richman for his constant guidance, attention, and patience, and without whom this Note would not have been possible; second, to the staff of the *Columbia Law Review* for their thoughtful and diligent work; and finally to my family for their support—especially to Emily, who listened endlessly whenever I spoke about location data.

II. ANALYZING HOW *CARPENTER*'S EARLY PROGENY ADDRESSES THE FUNDAMENTAL CHARACTERISTICS OF COMMERCIAL LOCATION DATA 729
A. Debating Whether *Carpenter* Applies Beyond CSLI 730
B. Debating How *Carpenter* Applies to Aggregated, Pseudonymized Location Data 733
C. Questioning the Strength of User Consent to Location Collection at the OS and Application Level 736
III. REGULATING THE GOVERNMENT'S PURCHASE OF LOCATION DATA FOR AIDING LAW ENFORCEMENT 741
A. *Carpenter* Applies to Purchased Location Data That Is Involuntarily Shared 742
1. *Carpenter* Applies Beyond CSLI 743
2. Aggregated, Pseudonymized Data Still Risks Individuals' Privacy 745
3. Commercial Location Data Is Sourced From Involuntarily Shared Location Data From Users' Mobile Applications 747
B. The Difficulty of Ex Ante Application of Fourth Amendment Protections Against the Government's Warrantless Purchasing of Comprehensive Location Data 749
1. The Challenge of Parsing Out Genuine Affirmative Consent to Data Collection 749
2. A Statutory Solution: Applying the Stored Communications Act 750
CONCLUSION 753

INTRODUCTION

In May 2020, what began as a local protest against the murder of Minneapolis resident George Floyd turned into a global phenomenon.[1] The world watched as tens of thousands of people demanded racial justice: Rows of people walked together, anonymous individuals blending to form a single group unified in movement and message.[2]

But to data broker Mobilewalla, the masses of anonymous individuals were not so anonymous. Mobilewalla saw a different picture: a sea of mobile phones emitting data, including location data that was ripe to ingest,

1. See Derrick Bryson Taylor, George Floyd Protests: A Timeline, N.Y. Times (Nov. 5, 2021), https://www.nytimes.com/article/george-floyd-protests-timeline.html (on file with the *Columbia Law Review*).

2. Id.

aggregate, analyze, and sell.[3] Using location data harvested from protestors' cell phones, Mobilewalla published a report analyzing the protesters' demographics.[4] The analysis shared factors like race, ethnicity, gender, age, and protestors' hometowns—all sourced from mobile devices.[5]

Mobilewalla aggregates and sells insights based on consumer data by tapping into users' smartphone activity and online web browsing behavior.[6] Billing itself as a "consumer intelligence" platform,[7] the company accesses, stores, and analyzes mobile data across a stunning 1.3 billion devices.[8] In part, this mobile data includes location data used to track where consumers have been, based on where their cell phones have been.[9] Mobilewalla then leverages this powerful information to sell location data

---

3. See Caroline Haskins, Almost 17,000 Protesters Had No Idea a Tech Company Was Tracing Their Location, Buzzfeed News (June 25, 2020), https://www.buzzfeednews.com/article/carolinehaskins1/protests-tech-company-spying [https://perma.cc/B3F4-GGT6] (detailing a report released by Mobilewalla regarding protestors such as their age, gender, and race).

4. Id. Mobilewalla's CEO, Anindya Datta, also admitted that his company "didn't prepare the report for law enforcement or a public agency, but rather to satisfy its own employees' curiosity about what its vast trove of unregulated data could reveal about the demonstrators." Id.

5. The company has since taken down the previously publicly available report, but other sites maintain screenshots. See, e.g., New Report Reveals Demographics of Black Lives Matter Protesters Shows Vast Majority Are White, Marched Within Their Own Cities, PR Newswire (June 18, 2020), https://www.prnewswire.com/news-releases/new-report-reveals-demographics-of-black-lives-matter-protesters-shows-vast-majority-are-white-marched-within-their-own-cities-301079234.html [https://perma.cc/W9LK-GSEX]. Further, actual identities were likely not plainly shared, but deanonymizing a device's identity is fairly simple. See infra section III.A.2.

6. Consumer Data, Mobilewalla, https://www.mobilewalla.com/consumer-data [https://perma.cc/97EP-E7HH] (last visited Jan. 11, 2021); Guide to Third-Party Data, Mobilewalla, https://www.mobilewalla.com/third-party-data [https://perma.cc/T3B5-PZZF] [hereinafter Mobilewalla, Guide to Third-Party Data] (last visited Jan. 11, 2021) ("Much of the current third-party data activity centers around smartphones. . . . [E]very phone has a Mobile Advertiser ID (MAID) that effectively creates a persistent customer identity, uniting online activity (through app and web browser behavior) and offline activity (through device location).").

7. See Mobilewalla, Mobilewalla, https://www.mobilewalla.com [https://perma.cc/EU7E-BYRV] (last visited Jan. 11, 2021).

8. Mobile Data, Mobilewalla, https://www.mobilewalla.com/mobile-data [https://perma.cc/JG5X-4JPW] (last visited Jan. 11, 2021); see also Mobilewalla, Guide to Third-Party Data, supra note 6 (offering a broader discussion of the company's explanations of third-party data and location data specifically); Improve Advertising and Build Effective Consumer Profiles With Mobile Data, Mobilewalla (July 2, 2018), https://www.mobilewalla.com/blog/improve-advertising-build-effective-consumer-profiles-mobile-data [https://perma.cc/ZF67-NUEZ] (discussing mobile data to build consumer profiles, Mobilewalla asks, "Where are they located? Do they travel? What are patterns in their mobile behaviors?").

9. Location-Based Marketing, Mobilewalla, https://www.mobilewalla.com/location-based-marketing [https://perma.cc/9SS2-BYYZ] [hereinafter Mobilewalla, Location-Based Marketing] (last visited Jan. 11, 2021).

and services to private-sector companies looking to improve their marketing.[10]

Mobilewalla's practices echo the broader practices of data brokers—private-sector companies that regularly trade in vast volumes of consumers' location data, often sourced from mobile devices and spanning long periods, to buyers on the open market.[11] But in 2018, the Supreme Court decided in *Carpenter v. United States* that the government requires a search warrant to access seven days or more of certain location data that comes from mobile devices; the government could no longer rely on a mere court order that the Stored Communications Act (SCA) had previously statutorily permitted it to use.[12]

Carpenter, of course, does not impact data brokers' practices because the Fourth Amendment does not regulate open market transactions. But it is less apparent whether, under *Carpenter*, the government can now *buy* location data from the open market like any private actor. This Note addresses that question: whether the government can lawfully buy location data from the open market like any private-sector entity, notwithstanding *Carpenter*'s holding; in other words, whether the government—which now requires a warrant to acquire seven-plus days of location data from a wireless carrier—can nonetheless "buy" its way around Fourth Amendment requirements by going straight to the open market.[13]

Whether or not it can, it appears the government already has made such purchases: In early 2020, news outlets reported that different government agencies had purchased location data from a commercial data broker.[14] Federal agencies—including Customs and Border Patrol (CBP),[15]

---

10. See Mobilewalla, Guide to Third-Party Data, supra note 6 ("[T]hird-party data is a mainstay of marketing strategy and will become increasingly essential in maintaining a competitive advantage.").

11. See infra section I.A.

12. 138 S. Ct. 2206, 2212, 2217 (2018). Under section 2703(d) of the SCA, the government could require electronic communication services or remote computing services to disclose customer records if the government offered "specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d) (2018).

13. See Gilad Edelman, Can the Government Buy Its Way Around the Fourth Amendment?, WIRED (Feb. 11, 2020), https://www.wired.com/story/can-government-buy-way-around-fourth-amendment/ [https://perma.cc/XX8L-FDPE].

14. See, e.g., Byron Tau & Michelle Hackman, Federal Agencies Use Cellphone Location Data for Immigration Enforcement, Wall St. J. (Feb. 7, 2020), https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600 (on file with the *Columbia Law Review*).

15. DHS, Privacy Impact Assessment Update for the Border Surveillance Systems (BSS) 6–7 (2018), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp022-bss-september2018.pdf [https://perma.cc/Z533-F4FF] (noting CBP "may use commercial location data acquired from a data provider to detect the presence of individuals in areas between Ports of Entry where such a presence is indicative of potential illicit or illegal activity").

Immigration and Customs Enforcement (ICE), the Secret Service,[16] and the Criminal Investigation Unit of the Internal Revenue Service (IRS)—had reportedly purchased location data for law enforcement purposes.[17]

Courts have yet to address whether *Carpenter* restricts the government's ability to *purchase* location data rather than obtain it by a legal instrument. This Note argues that *Carpenter* restricts such practices when purchased data is functionally equivalent to the location data—cell-site location information (CSLI)—in which *Carpenter* found individuals have an expectation of privacy; in other words, *Carpenter* restricts the government from purchasing location data for which it would otherwise require a warrant.[18]

Part I begins by explaining the current landscape of location data. Section I.A provides an overview of location data, explaining its technical components and who wants it, how they get it, and why they sell it. Section I.B lays the foundation of how the law currently treats location data.

Part II argues that while courts have yet to hear cases specifically regarding the constitutionality of the government's use of commercial location data, commercial location data has certain characteristics that *Carpenter*'s early progeny is already grappling with—and the way lower courts are approaching these characteristics informs how courts in turn will eventually approach the constitutionality of government purchasing commercial location data. Courts, however, are conflicted on these characteristics, and Part II demonstrates these tensions. Section II.A illustrates the tension around the courts' treatment of non-CSLI location data; section II.B illustrates the tension around the courts' treatment of aggregated, pseudonymized location data; and section II.C illustrates the tension around the courts' treatment of involuntarily shared location data sourced from mobile applications and operating systems.

Finally, Part III proposes how *Carpenter* should apply to purchased location data. Section III.A argues that *Carpenter*'s principle indeed applies to restrict the government from purchasing seven-plus days of location data, proposing that the tension around how *Carpenter*'s early progeny treats proxy characteristics of commercial location data should be resolved to apply *Carpenter* to the government's use of commercial location data for

---

16. Tim Cushing, Secret Service Latest to Use Data Brokers to Dodge Warrant Requirements for Cell Site Location Data, Techdirt (Aug. 24, 2020), https://www.techdirt.com/articles/20200820/13395145155/secret-service-latest-to-use-data-brokers-to-dodge-warrant-requirements-cell-site-location-data.shtml [https://perma.cc/GAA4-PAA5] [hereinafter Cushing, Secret Service].

17. Tau & Hackman, supra note 14; see also Byron Tau, IRS Used Cellphone Location Data to Try to Find Suspects, Wall St. J., https://www.wsj.com/articles/irs-used-cellphone-location-data-to-try-to-find-suspects-11592587815 (on file with the *Columbia Law Review*) (last updated June 19, 2020).

18. See Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) ("[W]e hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI.").

law enforcement efforts. Section III.B raises challenges to this resolution and then offers a statutory solution.

I. THE CURRENT LANDSCAPE OF LOCATION DATA

Section I.A discusses important technical characteristics and considerations of location data, as well as suppliers that handle such data. Section I.B discusses the thin patchwork of laws currently regulating location data.

A. *An Overview of Location Data*

"Data exhaust" is data generated as a byproduct of one's digital or online activities.[19] An individual can hardly profit off their own data exhaust,[20] but data brokers certainly can and do so by collecting consumers' personal information from different sources, aggregating them to create profiles of individuals, and reselling or sharing that information with others.[21]

Aggregated data allows data brokers to unlock insights made possible only by scale.[22] Data brokers divide up individuals into thousands of advertising-friendly slices: The more data is available, the more exact such profiles become.[23] And of such data, location data is a prized asset: An oil that fuels a large, $21 billion location services industry,[24] the precision and

---

19. Data Exhaust, Techopedia, https://www.techopedia.com/definition/30319/data-exhaust [https://perma.cc/86S5-HMSZ] (last visited Jan. 15, 2021) (noting that data exhaust "consist[s] of storable choices, actions and preferences such as log files, cookies, temporary files and even information that is generated for every process or transaction done digitally").

20. See Gregory Barber, I Sold My Data for Crypto. Here's How Much I Made, WIRED (Dec. 17, 2018), https://www.wired.com/story/i-sold-my-data-for-crypto [https://perma.cc/F86R-JV23] (discussing a WIRED reporter's efforts to become his "own data broker" selling, among other things, his GPS location—and earning 0.3 cents).

21. See FTC, Data Brokers: A Call for Transparency and Accountability, at i (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [https://perma.cc/R82F-JSR5] [hereinafter FTC, Data Brokers] (describing how data brokers rely on "a wide range of sources" to collect personal consumer information). The data broker industry is said to be worth approximately $200 billion. See David Lazarus, Column: Shadowy Data Brokers Make the Most of Their Invisibility Cloak, L.A. Times (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers (on file with the *Columbia Law Review*).

22. See FTC, Data Brokers, supra note 21, at iv ("While each data broker source may provide only a few data elements about a consumer's activities, data brokers can put all of these data elements together to form a more detailed composite of the consumer's life.").

23. See id. at 3 (noting that data brokers combine then analyze consumer data to make inferences about consumer interests, which, along with other information, place consumers in categories). Hardly anyone is immune: Data brokers collect and store data "on almost every U.S. household and commercial transaction," with one broker in the sample having "3000 data segments for nearly every U.S. consumer." Id. at iv.

24. Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller & Aaron Krolik, Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret, N.Y. Times

pervasiveness of commercial location data demonstrate its sensitivity.[25] Because cell phones are "almost a 'feature of human anatomy,'" historical location data effectively reveals everywhere cell phone owners have frequented—day and night.[26] The government itself has warned of the national security concerns of "Silicon Valley's practice of collecting and selling cellphone location information for advertising and marketing purposes," issuing guidance for military and intelligence personnel about the risks of location tracking through apps, wireless networks, and Bluetooth technology.[27] It is no surprise that an entire subset of the data broker industry deals in location data aiming to facilitate advertising.[28] To marketing teams, location data is a gold mine for improving customer profiles,[29] delivering timely ads,[30] and tracking ad conversions.[31]

(Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html (on file with the *Columbia Law Review*).

25. See Kirsten Martin & Helen Nissenbaum, What Is It About Location?, 35 Berkeley Tech. L.J. 251, 265 (2020) ("General Data Protection Regulation (GDPR), implemented in May 2018, singled out location data for special attention along with other types of data in the tightly regulated category of personally identifying information."); Paul Ohm, Sensitive Information, 88 S. Cal. L. Rev. 1125, 1180 (2015) ("Geolocation seems poised to be classified as sensitive.").

26. Carpenter v. United States, 138 S. Ct. 2206, 2211, 2218 (2018) (quoting Riley v. California, 573 U.S. 373, 385 (2014)) (noting also that "historical cell phone records . . . provide a comprehensive chronicle of the user's past movements").

27. Byron Tau & Dustin Volz, NSA Warns Cellphone Location Data Could Pose National-Security Threat, Wall St. J. (Aug. 4, 2020), https://www.wsj.com/articles/nsa-warns-cellphone-location-data-could-pose-national-security-threat-11596563156?cx_testId=3&cx_testVariant=cx_16&cx_artPos=4#cxrecs_s (on file with the *Columbia Law Review*) ("'Location data can be extremely valuable and must be protected. It can reveal details about the number of users in a location, user and supply movements, daily routines (user and organizational), and can expose otherwise unknown associations between users and locations,' the NSA bulletin warned."); see also Ohm, supra note 25, at 1131 (noting that "[t]hreat models suggest that precise geolocation should be considered sensitive").

28. See, e.g., Mobilewalla, Location-Based Marketing, supra note 9.

29. See Consumer Profiling: The Beginner's Guide, GWI, https://www.gwi.com/reports/beginners-guide-to-consumer-profiling [https://perma.cc/BX7Q-2EUQ] (last visited Oct. 6, 2021) (noting that marketers and advertisers are searching for "a more holistic portrayal of audience behaviors—across time, location, devices and platforms").

30. See Alfred Ng, Location Data Brokers Say They Can Help Contain COVID-19. Here's Why That's a Problem, CNET (Apr. 10, 2020), https://www.cnet.com/health/location-data-brokers-say-they-can-help-contain-covid-19-heres-why-thats-a-problem [https://perma.cc/Q9X4-87XU] [hereinafter Ng, Location Data Brokers Say They Can Help Contain COVID-19] ("The [mobile advertising] industry has collected location data on hundreds of millions of Americans for years to better target ads to people near certain stores.").

31. See Kochava and Cuebiq Partner to Measure the Impact of OOH Advertising in Driving App Downloads, PR Newswire (Sept. 30, 2019), https://www.prnewswire.com/news-releases/kochava-and-cuebiq-partner-to-measure-the-impact-of-ooh-advertising-in-driving-app-downloads-300927159.html [https://perma.cc/JTZ9-FQ6Z] (quoting the CEO of Kochava, a mobile app analytics company, claiming that, by connecting devices that physi-

Location data companies like Babel Street,[32] Cuebiq,[33] Gravy Analytics,[34] Mobilewalla,[35] Venntel Inc.,[36] and X-Mode[37] comprise a small slice of a market that competes to buy, sell, and analyze location data. Despite their household anonymity, these companies buy and sell significant volumes: Marketers spent an estimated forty percent, or $16 billion, of all mobile ad spending in 2017 on location-targeted ads served to mobile devices.[38]

Mobile devices are the first step of the location data supply chain. Data brokers and advertisers acquire location data by paying to place trackers in popular mobile applications.[39] Many applications collect location data whether or not it directly relates to application functionality.[40] Trackers are present in gas station finders, weather applications, and even a flashlight application.[41] And it is not always clear which applications send location

---

cally pass a billboard within a specific time range and comparing device locations with devices that installed within that time frame, Kochava "can fairly accredit an app install to an OOH [out-of-home] ad").

32. See Charles Levinson, Through Apps, Not Warrants, 'Locate X' Allows Federal Law Enforcement to Track Phones, Protocol (Mar. 5, 2020), https://www.protocol.com/government-buying-location-data [https://perma.cc/2JT3-4D8B] (discussing Babel Street's product, Locate X, used by federal law enforcement).

33. Cuebiq, a mobile advertising company, says "its data is accurate to 30 feet" and that it "tracks up to 15 million people in the US every day." Ng, Location Data Brokers Say They Can Help Contain COVID-19, supra note 30.

34. Gravy Analytics, Gravy Analytics, https://gravyanalytics.com [https://perma.cc/6LM9-UD4U] (last visited Oct. 17, 2020) (noting on the front page of its website that customers can "[b]uild a better customer experience with location intelligence[] [because] Gravy Analytics processes billions of pseudonymous, mobile location signals every day from millions of mobile devices to understand where people go and why").

35. See supra notes 3–11 and accompanying text.

36. See infra note 45 and accompanying text.

37. See Ng, Location Data Brokers Say They Can Help Contain COVID-19, supra note 30 ("'[Seventy percent] of our location is in a 20M (meter) accuracy and we also collect speed, bearing and altitude as well,' [X-Mode] said in an email." (first alteration in original)).

38. Christopher Mims, Your Location Data Is Being Sold—Often Without Your Knowledge, Wall St. J. (Mar. 4, 2018), https://www.wsj.com/articles/your-location-data-is-being-soldoften-without-your-knowledge-1520168400 (on file with the *Columbia Law Review*) (noting that research firm BIA/Kelsey estimates spending on these ads will double by 2021).

39. See Ng, Location Data Brokers Say They Can Help Contain COVID-19, supra note 30.

40. See Joseph Cox, Secret Service Bought Phone Location Data From Apps, Contract Confirms, Vice (Aug. 17, 2020), https://www.vice.com/en_us/article/jgxk3g/secret-service-phone-location-data-babel-street [https://perma.cc/VBL4-C7BM] (noting that sometimes location data "may provide some benefit to the app's operation itself" but intimating that the true benefit of collecting location data is to "sell that information as well to data brokers or other companies who incorporate it into their own products"); Charles Levinson, Through Apps, Not Warrants, 'Locate X' Allows Federal Law Enforcement to Track Phones, Protocol (Mar. 5, 2020), https://www.protocol.com/government-buying-location-data [https://perma.cc/63KL-GNXU] (discussing a tool that "tracks the location of devices anonymously, using data that popular cell phone apps collect").

41. Martin & Nissenbaum, supra note 25, at 260–61 ("[T]he popular Brightest Flashlight app was . . . tracking users' location and selling it to third parties, the Weather Channel

data to advertisers.[42] Indeed, "[e]very time you say 'yes' to an app that asks to know your location, you are also potentially authorizing that app to sell your data."[43]

After ordinary applications collect users' location data, the company aggregating that data sells it to advertisers and to others who wish to buy (and further sell) the data.[44] This buying and selling pushes commercial location data along a supply chain, within which exist companies that sell location data to private-sector advertisers but also to those who primarily contract to sell data to the government.[45]

Further, location data from mobile devices is not homogenous; rather, data is sourced from some combination of four different technologies every smartphone generally has: (1) the ability to connect to cell towers; (2) a Global Positioning System (GPS) chip; (3) a Bluetooth chip; and (4) the ability to connect to Wi-Fi networks.[46] These sources differ in their range and approximation of location; overall, however, the more precise location data is, the more likely it is that the data combines these four sources.[47]

---

was . . . passing its users' location data to other IBM-owned services as well as outside entities, and Accuweather . . . was recording and selling location data even after users had said no." (footnotes omitted)); Ng, Location Data Brokers Say They Can Help Contain COVID-19, supra note 30.

42. Ng, Location Data Brokers Say They Can Help Contain COVID-19, supra note 30 ("Unless you're analyzing every app you're using, it's hard to figure out which apps are sending your location to advertisers.").

43. Mims, supra note 38.

44. See, e.g., Audience Segments, Mobilewalla, https://www.mobilewalla.com/products/audience-segments [https://perma.cc/K6Z2-8WBL] [hereinafter Mobilewalla, Audience Segments] (last visited Oct. 17, 2020) (discussing a product offering called "Audience Segments" that uses "GPS latitude and longitude location data from billions of daily signals" to improve the "scale and accuracy" of its demographic insights attached to each device identity it develops).

45. Tau & Hackman, supra note 14 (discussing the company Venntel, which "[c]ontracting records show [sold] the federal government . . . location data . . . . Venntel, in turn, purchased the information from private marketing companies that sell the location data of millions of cellphones to advertisers").

46. See Harsha Panduranga, Laura Hecht-Felella & Raya Koreh, Government Access to Mobile Phone Data for Contact Tracing: A Statutory Primer, Brennan Ctr. For Just. 8 app. 1 (May 21, 2020), https://www.brennancenter.org/sites/default/files/2020-05/2020_05_21_ContactTracingPrimer_Final.pdf [https://perma.cc/66MY-65QP]; see also In re Search of: Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 733 (N.D. Ill. 2020) ("Google collects location information data from sources including GPS data, cell-site information, wi-fi access points, and Bluetooth beacons within range of a given mobile device.").

47. See *In re Search*, 481 F. Supp. 3d at 744 n.11 ("The location data points reflected in [Google Location History ('LH')] are estimates based on multiple inputs, and therefore a user's actual location does not necessarily align perfectly with any one isolated LH data point." (alteration in original)).

A cell phone's basic function is to connect to cell towers.[48] When cell phones ping nearby towers, wireless companies record each "ping" and the corresponding specific cell tower to which the phone connected.[49] Because cell phones regularly ping cell towers, a record of where a cell phone pings de facto reveals that phone's location history.[50] Location data sourced this way is called cell-site location information (CSLI): the same data at issue in *Carpenter*.[51]

GPS also generates location information (by connecting to satellites, not cell towers) and can be accurate to within sixteen feet.[52] Bluetooth and Wi-Fi do not connect to satellites, but both can generate location information by connecting to beacons or nearby Wi-Fi networks.[53]

Companies that provide mobile phone operating systems (OSes) are the technical bridges between users' location data and the applications that then collect and feed that data into the supply chain.[54] Almost all mobile phones run either Google's Android or Apple's iOS.[55] Given the pervasiveness of Google, which collects data through its own Android OS and Google-owned mobile applications on Apple's iOS, virtually anyone with a cell phone likely transmits location data to Google.[56]

The mobile OS itself records location data and then shares it with the applications that users have given permission to access such data.[57] In

48. Carpenter v. United States, 138 S. Ct. 2206, 2211–12 (2018).

49. Id.

50. Id.

51. Id.

52. See Panduranga et al., supra note 46, at app. 1; GPS Accuracy, GPS.gov, https://www.gps.gov/systems/gps/performance/accuracy [https://perma.cc/42XN-TYQS] (last visited Jan. 13, 2021).

53. See Panduranga et al., supra note 46, at app. 1.

54. Martin & Nissenbaum, supra note 25, at 260–61 (noting that Apple and Google give developers tools to leverage data naturally generated on their systems, and that for location, the OS provides GPS and markers like "position in relation to nearby Wi-Fi routers and the closest cellular service towers" (footnote omitted)).

55. See Mobile Operating System Market Share Worldwide, Statcounter, https://gs.statcounter.com/os-market-share/mobile/worldwide [https://perma.cc/G2RT-JHVJ] (last visited Jan. 13, 2021) (reporting that, as of December 2020, Android had a 72.5% market share and iOS a 26.9% market share, leaving only 0.6% for other mobile OSes).

56. In re Search of: Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 734 n.1 (N.D. Ill. 2020) (noting the government's representation that, given both Google's Android market share and "that many Apple devices nonetheless communicate with Google" via Google's mobile applications like "Gmail, Google Maps, Google Chrome, and YouTube[,] . . . a person possessing a smartphone likely transmits data to Google").

57. See infra section II.C. Though Apple's recent feature, App Tracking Transparency, might do more to alert the average consumer about the applications tracking them, that does not mean consumers will always opt out of sharing data with their mobile applications. See Shani Rosenfelder, Initial Data Indicates ATT Opt-In Rates Are Much Higher Than Anticipated—At Least 39% [Updated], AppsFlyer (Apr. 8, 2021), https://www.appsflyer.com/blog/att-opt-in-rates-higher/ [https://perma.cc/ZCD3-TF8G] (reporting that consumers opt in to share data at rates higher than expected in real-world estimates, opting in at a weighted average of thirty-nine percent of the time).

other words, if the OS is like running water, then the permission users grant to applications to collect data acts as the faucet: Once users grant permission, application developers can access the information that the OS collects.[58]

B. *The State of the Law Concerning Location Data*

This Note focuses on the constitutional treatment of location data records. Section I.B.1 explains the justification of the constitutional focus. Section I.B.2 then discusses the Fourth Amendment's current approach to location data, tracing the third-party doctrine and the Supreme Court's decision to refrain from extending the third-party doctrine to some instances of acquired location data in *Carpenter v. United States*.

1. *The Dearth of Current Law Governing Location Data.* — The private sector collects and uses more location data than the average consumer realizes.[59] The thin patchwork of laws regulating location data allows data brokers to collect, buy, and sell location data subject largely only to general market constraints.[60] Indeed, the information technology industry—and the companies busy buying and selling location data—function in large part through self-regulation.[61] Unlike in Europe, where the General Data Protection Regulation governs, the United States lacks a comprehensive regime to regulate data.[62] Because there is no comprehensive federal data

---

58. Lauren Goode, App Permissions Don't Tell Us Nearly Enough About Our Apps, WIRED (Apr. 14, 2018), https://www.wired.com/story/app-permissions/ [https://perma.cc/4F83-BNES] (noting that "once you grant location access, app makers are able to pull in" location information).

59. See Valentino-DeVries et al., supra note 24 (noting how easy it is "to share information without realizing it" and that "[o]f the 17 apps that The Times saw sending precise location data, just three on iOS and one on Android told users in a prompt during the permission process that the information could be used for advertising").

60. See What Information Do Data Brokers Have on Consumers, and How Do They Use It?: Hearing Before the S. Comm. on Com., Sci. & Transp., 113th Cong. 63 (2013) [hereinafter What Information Do Data Brokers Have on Consumers, and How Do They Use It?] (noting the dearth of federal privacy laws covering location data and disagreement over whether self-regulation of data privacy is sufficient); Robert Gellman & Pam Dixon, Data Brokers and the Federal Government: A New Front in the Battle for Privacy Opens, World Privacy F. 10 (Oct. 30, 2013), http://www.worldprivacyforum.org/wp-content/uploads/2013/10/WPF_DataBrokersPart3_fs.pdf [https://perma.cc/BHH3-EXVF] ("Commercial database owners are largely unregulated for privacy, and they are generally free to sell information as they please with little regard for accuracy, currency, completeness, or fairness.").

61. Martin & Nissenbaum, supra note 25, at 263. Some technology companies are calling for more regulation of location data, however. See, e.g., Jeff Glueck, Opinion, How to Stop the Abuse of Location Data, N.Y. Times (Oct. 16, 2019), https://www.nytimes.com/2019/10/16/opinion/foursquare-privacy-internet.html (on file with the *Columbia Law Review*) (noting the CEO of Foursquare's opinion that "[i]t's time for Congress to regulate the [location data] industry").

62. Chris Jay Hoofnagle, Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement, 29 N.C. J.

privacy statute, no single law governs how corporations share collected user data.[63] And any privacy protections that do exist attach not based on characteristics inherent to the data but rather on how the data was collected.[64] This applies to location data as well, despite its sensitivity; in fact, only one federal law—the Children's Online Privacy Protection Act—expressly addresses location data, location-based technology, and consumer privacy.[65]

The federal statutory and regulatory regimes that could regulate the use of consumers' locations are limited. Sometimes, statutory regimes are industry specific: Section 222 of the Communications Act of 1934, for example, addresses how telecommunications carriers must protect the confidentiality of customers' proprietary information.[66] With respect to customers' location data, it specifies that nothing short of a customer's "express prior authorization" shall be considered to approve disclosure of call location information.[67] But section 222 is limited both in its target (telecommunications companies) and in its scope (*call* location data). In turn, while the SCA limits certain entities from voluntarily disclosing consumer data to the government,[68] the SCA does not prevent providers from disclosing customer data to *private* entities.[69] Nothing then, in turn, prevents private entities from sharing customer data back to the government.[70]

Int'l L. & Com. Regul. 595, 618–19 (2004); see also Martin & Nissenbaum, supra note 25, at 265–66.

63. Wall St. J., How the U.S. Government Obtains and Uses Cellphone Location Data, YouTube, at 07:45 (Feb. 7, 2020), https://youtu.be/SXAShotdFZo (on file with the *Columbia Law Review*) [hereinafter Wall St. J., How the U.S. Government Obtains and Uses Cellphone Location Data].

64. Hoofnagle, supra note 62, at 618–19 ("Privacy law in the United States is riddled with similar deficits in protection."). For example, the Health Insurance Portability and Accountability Act of 1996 protects medical information shared with a health provider, but if a consumer completes a product warranty card that requests details about ailments, anyone can freely sell that information for any purpose. Id. Another example: Cable companies "face strict rules limiting the use of data on viewers' behaviors, but the law does not extend to intermediate devices, such as a Tivo personal video recorder. Tivo, Inc. can sell the same information that the cable company cannot." Id.

65. What Information Do Data Brokers Have on Consumers, and How Do They Use It?, supra note 60, at 63. There are, however, brewing state laws that are data broker–specific (Vermont's) or have data broker–specific or data-selling provisions (California's and Illinois's). See Christopher W. Savage, Managing the Ambient Trust Commons: The Economics of Online Consumer Information Privacy, 22 Stan. Tech. L. Rev. 95, 105 n.36 (2019).

66. 47 U.S.C. § 222 (2018).

67. Id. § 222(f).

68. See 18 U.S.C. § 2702(a)(3) (2018) (prohibiting entities providing a remote computing service or electronic communication service to the public from knowingly divulging certain customer information to the government); Panduranga et al., supra note 46, at 5.

69. 18 U.S.C. § 2702(c)(6) (permitting entities to disclose data to "any person other than a governmental entity").

70. Joshua L. Simmons, Buying You: The Government's Use of Fourth-Parties to Launder Data About "The People", 2009 Colum. Bus. L. Rev. 950, 977–78 (noting that the SCA

On the regulatory side, the FCC requires wireless carriers to take reasonable measures to discover and protect against attempts to gain unauthorized access to certain data, including customer location data.[71] In 2020, the FCC fined the nation's four largest wireless carriers $200 million for improperly selling access to customers' location data.[72] This too, however, is limited by the FCC's scope. The FTC, alternatively, could regulate the selling of location data but only indirectly because the Commission works to prevent anticompetitive, deceptive, and unfair business practices,[73] so companies open about collecting and sharing location data may be conducting unethical—but not deceptive—practices.[74]

This paucity of statutes and regulations governing location data leaves the Fourth Amendment as the last threshold regulating the government's use of location data in law enforcement. There is little else regulating the government's relationship with data brokers.[75] The federal government is itself a regular customer of commercial data brokers, acquiring data for various activities.[76] This includes regularly tapping the private sector, especially since 9/11, to purchase location data for law enforcement.[77] And recently, federal agencies like CBP, ICE, the Secret Service, and the Criminal Investigation unit of the IRS have reportedly purchased location data for

---

"allows service providers to disclose consumer records to 'any person other than a governmental entity,' such as a fourth-party, and there is no provision preventing the fourth-party from giving that information to the government in turn" (footnote omitted)).

71. Ernesto Mendieta, FCC Proposes Over $200 Million in Fines to AT&T, Verizon, T-Mobile and Sprint for Not Protecting Customers' Location Data, Nat'l L. Rev. (Mar. 10, 2020), https://www.natlawreview.com/article/fcc-proposes-over-200-million-fines-to-att-verizon-t-mobile-and-sprint-not [https://perma.cc/TEE9-BCC5].

72. Press Release, FCC, FCC Proposes Over $200 Million in Fines Against Four Largest Wireless Carriers for Apparently Failing to Adequately Protect Consumer Location Data 1 (Feb. 28, 2020), https://docs.fcc.gov/public/attachments/DOC-362754A1.pdf [https://perma.cc/RCP6-Q46W]. For a broader account of the location-data-selling scandal, see Valentino-DeVries et al., supra note 24.

73. About the FTC, FTC, https://www.ftc.gov/about-ftc (on file with the *Columbia Law Review*) (last visited Jan. 19, 2021).

74. See infra notes 149–150 and accompanying text (discussing the forthcomingness of Google's location-tracking policy of "continu[ing] to track users even if they've disabled the setting").

75. See Hoofnagle, supra note 62, at 619 (noting that "analysis of existing law shows that there are, in fact, few legal constraints on government access to commercial databases").

76. See id. at 595–96 (describing law enforcement's use of commercial data brokers to obtain information about individuals); Simmons, supra note 70, at 954 (detailing the federal government's relationship with private-sector data aggregators like ChoicePoint).

77. See Gellman & Dixon, supra note 60, at 8. Indeed, in fiscal year 2005, the DOJ, DHS, State, and SSA all reported they planned to spend $30 million "to purchase personal information from resellers. The vast majority—approximately 91 percent—of the planned spending was for purposes of law enforcement (69 percent) or counterterrorism (22 percent)." U.S. Gov't Accountability Off., GAO-08-543T, Government Use of Data from Information Resellers Could Include Better Protections: Testimony Before the Subcomm. on Info. Pol'y, Census & Nat'l Archives, Comm. on Oversight & Gov't Reform 2 (2008), https://www.gao.gov/assets/120/119298.pdf [https://perma.cc/LAS7-TCJU].

law enforcement purposes.[78] Indeed, the databases that agencies within the Department of Homeland Security (DHS) have acquired are one of the biggest surveillance tools that have been revealed to the public in recent years.[79]

Notwithstanding *Carpenter*'s holding that individuals have an expectation of privacy in the whole of their movements (more than seven days' worth), federal law enforcement agencies have purchased location data from commercial data brokers without warrants. As the government begins to access commercial location data for law enforcement purposes, it becomes even more pressing to focus on how the Fourth Amendment treats the government's access to location data—commercially available or otherwise—for criminal investigative purposes in light of *Carpenter*. The government's access impacts individuals more gravely than does data brokers trading on consumers' buying habits; the former is more likely to curb an individual's liberty than is the latter.[80]

2. *The Fourth Amendment's Current Treatment of Location Data Records.* — The test from *Katz v. United States* has been the Fourth Amendment's North Star in balancing law enforcement needs with individuals' expectations of privacy: The test finds that the Fourth Amendment applies—and thus the government requires probable cause and a warrant—only when an individual has a subjective expectation of privacy that society is prepared to recognize as reasonable.[81] But the Fourth Amendment's staple third-party doctrine, developed by the seminal cases of *United States v. Miller* and *Smith v. Maryland*, states that an individual lacks an expectation of privacy in information they share with third parties.[82]

Decided in the analog decade of the 1970s, *Miller* and *Smith* both dealt with individuals who had shared what they argued to be private data with third parties. Miller's bank had a copy of his bank records, and Smith had shared the numbers he dialed on his telephone with his telephone company. The Supreme Court ruled against them both. *Miller* and *Smith* thus laid the foundation for the third-party doctrine's core, simple principle

---

78. See supra notes 15–17 and accompanying text.

79. Wall St. J., How the U.S. Government Obtains and Uses Cellphone Location Data, supra note 63, at 0:30.

80. See, e.g., Jon Schuppe, Google Tracked His Bike Ride Past a Burglarized Home. That Made Him a Suspect, NBC News (Mar. 7, 2020), https://www.nbcnews.com/news/us-news/google-tracked-his-bike-ride-past-burglarized-home-made-him-n1151761 [https://perma.cc/PE5X-UMNF].

81. 389 U.S. 347, 361 (1967) (Harlan, J., concurring); see also Laura K. Donohue, The Fourth Amendment in a Digital World, 71 N.Y.U. Ann. Surv. Am. L. 553, 581 (2017) ("In his [*Katz*] concurrence, Justice Harlan spelled out the two-part test that would henceforward be applied.").

82. See Smith v. Maryland, 442 U.S. 735, 744 (1979) (quoting United States v. Miller, 425 U.S. 435, 443 (1976)) (noting the Court has repeatedly held the Fourth Amendment does not prohibit obtaining information revealed to a third party even if the information is revealed "only for a limited purpose and the confidence placed in the third party will not be betrayed").

that one lacks an expectation of privacy in information one shares with others.[83] The logic: by voluntarily sharing information, one chooses to forfeit the right to consider that same information private.[84] But applied to information shared by modern technology, the doctrine suddenly excludes a lot of information from Fourth Amendment protection, as virtually everything users do on smartphones is shared with some other entity.[85]

In her 2012 concurrence in *United States v. Jones*, Justice Sonia Sotomayor questioned the doctrine's applicability in the context of location data gathering specifically.[86] *Jones* concerned law enforcement attaching a GPS tracker to a vehicle to collect location data to monitor a defendant's movements for twenty-eight days.[87] In contrast to the majority's trespass-focused reasoning finding a search occurred, Justice Sotomayor reached the same conclusion but relied instead on *Katz*'s notion of an expectation of privacy: Even though the vehicle had been driving on public roads, revealing its location for all to see, she reasoned that it "may be necessary" to reconsider the premise that individuals lack reasonable expectations of privacy in information voluntarily disclosed to third parties, as such approach is "ill suited to the digital age" where people reveal much information about themselves to third parties while "carrying out mundane tasks."[88] The concurrence laid the foundation for the possibility that *Katz*'s expectation of privacy could persist notwithstanding that an individual shared data with a third party.

Exactly this principle took center stage in *Carpenter v. United States*, when the Court built on Justice Sotomayor's *Jones* concurrence. In 2011, police officers arrested Timothy Carpenter for robbing a series of T-Mobile stores.[89] Police identified him after an accomplice confessed to the crime and provided the cell phone numbers of his accomplices, leading the police to Carpenter's number.[90] Having the cell phone number, law enforcement then sought Carpenter's CSLI records via section 2703(d) of the

---

83. *Smith*, 442 U.S. at 744 ("[The third-party doctrine] analysis dictates that petitioner can claim no legitimate expectation of privacy here."); *Miller*, 425 U.S. at 442 ("[W]e perceive no legitimate 'expectation of privacy' [where] . . . [a]ll 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.").

84. *Smith*, 442 U.S. at 744 (explaining that someone who volunteers information "takes the risk, in revealing his affairs to another, that the information will be conveyed . . . to the Government" (quoting *Miller*, 425 U.S. at 442)).

85. See Donohue, supra note 81, at 555 ("[O]ur reliance on industry and third-party providers to service the needs of daily life has made much more of our personal information, as well as new kinds of personal data, vulnerable to government collection.").

86. 565 U.S. 400, 415–17 (2012) (Sotomayor, J., concurring).

87. See id. at 402–03.

88. Id. at 417 (Sotomayor, J., concurring).

89. Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018).

90. Id.

SCA, under which law enforcement enjoyed the statutory ability to seek Carpenter's records with a showing of less than probable cause.[91]

The government argued that Carpenter, like anyone with a cell phone, was constantly revealing his location to his wireless carrier, thus triggering the third-party doctrine and denying Carpenter an expectation of privacy in his location that he voluntarily shared with his wireless provider.[92] But the Court disagreed, declining to extend the third-party doctrine to the facts and instead holding that the government's access to more than seven days of Carpenter's CSLI constituted a search.[93] While CSLI records are business records based on data Carpenter shared with his wireless carrier, they were nonetheless "unique" and of a "qualitatively different category" of business records than what the third-party doctrine typically excludes from Fourth Amendment protection.[94] And "[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere," wrote Chief Justice John Roberts, but rather has "a reasonable expectation of privacy in the whole of their physical movements."[95] Importantly, the Court also rejected the argument that Carpenter had *voluntarily* shared his location with his wireless provider, further justifying rejecting the third-party doctrine's application to the facts.[96]

But *Carpenter* was a self-described narrow decision: Only the government's acquisition of seven days or more of historical CSLI from a wireless carrier constituted a search.[97] The Court explicitly noted that its decision did not express a view on "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)" or other business records that could "incidentally reveal location information."[98] The Court also noted the opinion did not "consider other collection techniques involving foreign affairs or national security," "disturb the application of *Smith* and *Miller*," or "question conventional surveillance techniques and tools, such as security cameras."[99]

---

91. Id.; see also 18 U.S.C. § 2703(d) (2018); supra note 13 and accompanying text.

92. *Carpenter*, 138 S. Ct. at 2218 ("[A] cell phone . . . tracks nearly exactly the movements of its owner. . . . [Individuals] compulsively carry cell phones with them all the time. A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales.").

93. Id. at 2217.

94. Id. at 2216–17.

95. Id. at 2217.

96. Id. at 2220 ("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." (quoting Riley v. California, 573 U.S. 373, 385 (2014))).

97. Id. (noting the decision is "a narrow one").

98. Id.

99. Id.

So far, this Note has asked whether *Carpenter*'s Fourth Amendment hurdles for acquiring CSLI from a wireless carrier apply to the government's *purchase* of commercial location data. *Carpenter* recognized the unique sensitivity location data poses and required the government to meet its constitutional obligations upon searching an individual's CSLI. But, at the same time, the Fourth Amendment does not cover market transactions. It is then an open question for how to treat, constitutionally, the government's purchase of commercial location data for law enforcement purposes. Part II expands on the tensions and early judicial guidance on this open question.

II. ANALYZING HOW *CARPENTER*'S EARLY PROGENY ADDRESSES THE FUNDAMENTAL CHARACTERISTICS OF COMMERCIAL LOCATION DATA

No court has explicitly considered whether *Carpenter*'s warrant requirement covers the government's purchase of location data from data brokers on the open market, but emerging case law from *Carpenter*'s early progeny is currently grappling with three areas that comprise the fundamental characteristics of commercial location data. First, courts are debating whether *Carpenter* may apply in cases with non-CSLI location data like GPS, which makes up much of commercial location data; second, courts are currently debating the constitutionality of geofence warrants, which concern aggregated and pseudonymized[100] location data analogous to location data sets that data brokers like Venntel sold to the government;[101] and third, courts are considering how user consent to their location data collection—at both the OS and the application level—impacts Fourth Amendment application.[102]

This Note proposes that principles extrapolated from debates about how *Carpenter* applies in these three areas will necessarily inform how courts might then approach the constitutionality of the government purchasing commercial location data. These three areas currently are all debates that courts must necessarily have in analyzing whether *Carpenter*

---

100. Pseudonymized data is data where users are labeled with unique identifiers, not their real names. Pseudonymization, Trend Micro, https://www.trendmicro.com/vinfo/us/security/definition/pseudonymization [https://perma.cc/UY2G-2C5G] (last visited Jan. 12, 2021) ("When data is pseudonymized, the information that can point to the identity of a subject is replaced by 'pseudonyms' or identifiers. This prevents the data from specifically pinpointing the user.").

101. Strictly speaking, Timothy Carpenter's identity would have been made available to law enforcement under the same court order used to compel disclosure of his location records. See *Carpenter*, 138 S. Ct. at 2212 ("[T]he prosecutors applied for court orders under the Stored Communications Act to obtain cell phone records for petitioner Timothy Carpenter and several other suspects."). In contrast to *Carpenter*, however, commercial location data that is pseudonymized masks a device owner's identity with a randomized string of numbers and letters that, in theory, do not readily reveal the device owner's identity. See supra note 100. But see infra section III.A.2 discussing the ease of deanonymizing device identities (IDs).

102. See infra section II.C.

covers the government's purchase of commercial location data: Commercial location data is not homogenous but rather composed of both CSLI and non-CSLI data;[103] it is aggregated and pseudonymized;[104] and, since location data is often sourced from mobile applications, users tend to affirmatively consent to its collection (even if the scope of collection may be broader than expected).[105]

The next sections explore the debate in these three areas: Section II.A illustrates cases both agreeing and disagreeing over whether *Carpenter* requires finding an expectation of privacy in non-CSLI location data. Section II.B illustrates cases where courts agree and disagree with the notion that *Carpenter* could apply to aggregated, pseudonymized location data—not merely an individual's data. Section II.C illustrates the debate over whether affirmative consent is truly given or whether, alternatively, users involuntarily share their location data such that it is appropriate to decline to apply the third-party doctrine to such collected location data. Although these areas do not focus on case law specifically involving commercial location data, understanding the tensions around how *Carpenter* might apply in these areas is significant to the broader question of how courts might treat the government's purchase of commercial location data.

A. *Debating Whether* Carpenter *Applies Beyond CSLI*

A key characteristic of commercial location data from data brokers is that such data comprises more than just CSLI. Indeed, CBP's statement justifying its use of commercial location data tries to distinguish the technical composition of the agency's data from the CSLI in *Carpenter*: "While CBP is being provided access to location information, it is important to note that such information *does not include cellular phone tower data*, is not ingested in bulk, and does not include the individual user's identity . . . ."[106]

But not all courts have applied *Carpenter* so narrowly, instead expanding its reach to apply beyond CSLI. Some courts have applied *Carpenter* to

---

103. See Ng, Location Data Brokers Say They Can Help Contain COVID-19, supra note 30 (quoting Angel Diaz, counsel at the Brennan Center for Justice, claiming that "this data comes from users that choose to share their location information with particular mobile apps."); see also Cushing, Secret Service, supra note 16 ("This location data isn't pulled from cell towers. Perhaps this is why agencies feel comfortable ignoring the *Carpenter* decision. . . . Multiple apps collect location data. Some of them sell this data to data brokers who then sell this to marketing firms and/or the US government.").

104. See Valentino-DeVries et al., supra note 24 (reporting that "the information apps collect is tied not to someone's name or phone number but to a unique ID. But those with access to the raw data . . . could still identify a person without consent").

105. See id.; see also Nili Steinfeld, "I Agree to the Terms and Conditions": (How) Do Users Read Privacy Policies Online? An Eye-Tracking Experiment, 55 Comput. Hum. Behav. 992, 998 (2016) ("[W]hen users have the option of accepting website terms and conditions without reading a policy, they will generally forgo reading the document.").

106. Wall St. J., How the U.S. Government Obtains and Uses Cellphone Location Data, supra note 63, at 02:22 (emphasis added).

find an individual enjoys an expectation of privacy in non-CSLI location data or, in some cases, data that is not even location-based at all. In *United States v. Diggs*, for example, a judge in the Northern District of Illinois held that *Carpenter* applied to the search of a defendant's GPS data sourced from the GPS tracking device built into his Lexus.[107] The court noted that the GPS data at issue fit "squarely within the scope of the reasonable expectation of privacy identified by the *Jones* concurrences and reaffirmed in *Carpenter*."[108] The judge reasoned that *Carpenter* defeats the government's third-party doctrine argument claiming that Tobias Diggs's location data escapes Fourth Amendment protection because it was shared with Lexus.[109] The judge further reasoned that applying the third-party doctrine to the GPS data in this case would require the very same application of the doctrine that *Carpenter* rejected in context of location data shared with a wireless carrier, and thus *Carpenter* "compels the conclusion that, given the privacy concerns implicated by the 'detailed and comprehensive record of [Diggs's] movements' captured by the Lexus's GPS tracker, 'the fact that the [police] obtained the information from a third party does not overcome [Diggs's] claim to Fourth Amendment protection.'"[110]

Importantly, courts appear actively aware of the technical distinction between location data sourced from CSLI and sourced otherwise. In *Demo v. Kirksey*, a District Court of Maryland judge noted that broadly, *Carpenter* "plainly reaffirmed an individual's reasonable expectation of privacy in the continuous gathering of geolocation data" no matter the technical underpinning of the location data. [111] More specifically, "*Carpenter* . . . established that an individual maintains an expectation of privacy in location data, whether via GPS on a vehicle traveling through public roads, or location data from cell site towers connecting to the cell phone in one's pocket."[112]

A Northern District of Illinois magistrate judge went even further, albeit in dicta, to note there was "much to suggest" that *Carpenter* applied even when the location data at issue was distinct from *Carpenter*'s CSLI and instead comprised a mix of "GPS data, cell-site information, wi-fi access

107. 385 F. Supp. 3d 648, 652, 655 (N.D. Ill. 2019) (explicitly rejecting the property-based logic in *United States v. Jones* and accepting the concurrence's logic).

108. Id. at 652.

109. Id. at 652–53.

110. Id. at 653–54 (alterations in original) (quoting Carpenter v. United States, 138 S. Ct. 2206, 2217, 2220 (2018)). The court recognized that *Carpenter* understood CSLI to present "many of the qualities of . . . GPS monitoring . . . . [B]oth are 'detailed, encyclopedic, and effortlessly compiled'; both 'provide[] an intimate window into a person's life'; and, in the context of historical information, both provide a 'tracking capacity . . . against everyone' without any need for the police to 'know in advance whether they want to follow a particular individual, or when.'" Id. at 653 (quoting *Carpenter*, 138 S. Ct. at 2216–18).

111. No. 8:18-CV-00716-PX, 2018 WL 5994995, at *5–6 (D. Md. Nov. 15, 2018).

112. Id. at *6 (citation omitted).

points, and Bluetooth" that Google used to track location data.[113] Other courts have noted willingness to extend *Carpenter* to other sets of facts if principles behind the decision applied.[114]

But not all courts are eager to reason this way. Indeed, *Carpenter* assumed that it is the sharing of over seven days' worth of CSLI, revealing an individual's location at close intervals, that violates an individual's expectations of privacy in the whole of her physical movements.[115] Some courts have then reasoned that fact patterns involving location data technologically distinct from CSLI disqualify *Carpenter*'s application. In *United States v. Santos-Matos*, a District Court of Delaware judge held that *Carpenter* could not apply to support a defendant's motion to suppress location data from a cell phone because "any location data obtained from the phone was not derived from a cell-site."[116] In a similar vein, a judge in the Southern District of New York declined to extend *Carpenter* to nonlocation data in *United States v. Kidd* when the defendant argued he had an expectation of privacy in his IP address.[117] Even CBP emphasized that the location data the agency purchased did not comprise CSLI.[118]

These cases show that while some courts do cabin *Carpenter*'s application to facts tightly analogous to the original case, other courts have applied *Carpenter* both to non-CSLI location data and data unrelated to location. Applications of *Carpenter* beyond pure CSLI make it more likely that a future court will hold that *Carpenter* covers the government's purchase of commercial location data, since such data is composed of more heterogeneous location data.

---

113. In re Search of: Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 733, 737 (N.D. Ill. 2020).

114. For example, a judge in the Western District of Washington in *Zietzke v. United States* explained that while he did not extend *Carpenter* to cryptocurrency records in this case, the court "will extend *Carpenter* to new circumstances only if they directly implicate the privacy concerns that animated the majority." 426 F. Supp. 3d 758, 768 (W.D. Wash. 2019). A judge in the Northern District of Georgia reasoned similarly in *United States v. Coleman* when she rejected *Carpenter*'s application to IP addresses, not because IP addresses are not CSLI but because the IP addresses in this case did not engender the same worries that CSLI did in *Carpenter*. No. 01:18-CR-00484, 2020 WL 5229042, at *15–16 (N.D. Ga. Jan. 14, 2020), report and recommendation adopted, No. 01:18-CR-00484, 2020 WL 2538931 (N.D. Ga. May 18, 2020).

115. *Carpenter*, 138 S. Ct. at 2217 n.3 ("It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search.").

116. No. CR 17-61-LPS, 2018 WL 5294509, at *2 (D. Del. Oct. 25, 2018).

117. 394 F. Supp. 3d 357, 362 (S.D.N.Y. 2019) (noting that "[e]very court to consider the application of *Carpenter* . . . has declined to extend its reasoning to IP address information").

118. See Wall St. J., How the U.S. Government Obtains and Uses Cellphone Location Data, supra note 63, at 02:22 (describing the CBP's statement in response to reporting of its location data purchasing, the agency highlights that the data it bought does "not include cellular phone tower data, is not ingested in bulk, and does not include the individual user's identity").

B. *Debating How* Carpenter *Applies to Aggregated, Pseudonymized Location Data*

Another key characteristic of commercial location data is that such data is aggregated, pseudonymized information—that is, commercial location data comprises data compiled over a period of time from multiple users whose identities are masked by unique identifiers, not their real names.

How courts currently approach the constitutionality of geofence warrants will inform how courts might eventually apply *Carpenter* to aggregated, pseudonymized location data. The nature of location data used by geofence warrants and the nature of commercial location data the government may purchase for law enforcement are extremely similar. Both provide the government pseudonymized location data to sift through and aid law enforcement in identifying individual device IDs that appear relevant to an investigation.[119]

Specifically, geofence warrants (also known as "reverse warrants"[120]) are warrant requests that ask a service provider—like Google, for example—to "cast a virtual net" around a certain location for a set time period.[121] Geofence warrants gather information not about prespecified individuals but instead about numerous persons within one specific area; anyone with a cell phone with geolocation capabilities can be included in a dragnet of location data sent to law enforcement.[122] The service provider discloses "a list of unique device identifiers" for any cell phones the provider knows were within the virtual net during the described time frame.[123]

Scholars have already questioned the constitutionality of geofence warrants as being too broad.[124] But courts are also getting involved. One

---

119. See id. at 03:12 ("The goal is to utilize this data to detect the presence of—but not identify—individuals in an area which CBP has identified as an area of interest, consistent with CBP statutory authorities, federal law, and DHS policy."); see also Tim Cushing, Feds Also Using 'Reverse Warrants' to Gather Location/Identifying Info on Thousands of Non-Suspects, Techdirt (Oct. 31, 2018), https://www.techdirt.com/articles/20181027/08301740920/feds-also-using-reverse-warrants-to-gather-location-identifying-info-thousands-non-suspects.shtml [https://perma.cc/4SST-NWRB] (explaining that reverse warrants allow law enforcement to serve "warrants to Google in hopes of figuring out who to suspect of committing crimes, rather than having a suspect in mind and working forward from there") [hereinafter Cushing, Feds Also Using 'Reverse Warrants'].

120. Cushing, Feds Also Using 'Reverse Warrants,' supra note 119.

121. In re Search of: Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 732 (N.D. Ill. 2020); see also Alfred Ng, Geofence Warrants: How Police Can Use Protesters' Phones Against Them, CNET (June 16, 2020), https://www.cnet.com/tech/services-and-software/geofence-warrants-how-police-can-use-protesters-phones-against-them/ [https://perma.cc/32TM-U5V8] (showing scanned image of a geofence warrant).

122. Katelyn Ringrose & Divya Ramjee, Watch Where You Walk: Law Enforcement Surveillance and Protester Privacy, 11 Calif. L. Rev. Online 349, 355 (2020).

123. *In re Search*, 481 F. Supp. 3d at 732.

124. See Wendy Davis, Law Enforcement Is Using Location Tracking on Mobile Devices to Identify Suspects, but Is It Unconstitutional?, ABA J. (Dec. 1, 2020),

case has recently been decided in the Eastern District of Virginia, where the defendant challenged the constitutionality of local police's use of a geofence warrant.[125] While the district court judge ultimately denied the defendant's motion to suppress, finding that the good-faith exception to exclusionary rule applied, the judge still found that geofence warrant from Google "plainly violates the rights enshrined in" the Fourth Amendment and lacked particularized probable cause.[126] In Illinois, a Northern District of Illinois magistrate judge in *In re Search of: Information Stored at Premises Controlled by Google* found a proposed geofence warrant requesting disclosure of pseudonymized[127] information of devices to be overly broad.[128] Although the judge did not need to rule on *Carpenter*'s applicability to the situation,[129] the judge still felt compelled to discuss *Carpenter*'s applicability in dicta, noting "there is much to suggest that *Carpenter*'s holding, on the question of whether the privacy interests in CSLI over at least seven days, should be extended to the use of geofences involving intrusions of much shorter duration."[130]

---

https://www.abajournal.com/magazine/article/law-enforcement-is-using-location-tracking-on-mobile-devices-to-identify-suspects-geofence [https://perma.cc/4NFL-63L7] (describing the constitutional question with respect to geofence warrants as whether they are sufficiently particular); Jennifer Lynch & Nathaniel Sobel, New Federal Court Rulings Find Geofence Warrants Unconstitutional, EFF (Aug. 31, 2020), https://www.eff.org/deeplinks/2020/08/new-federal-court-rulings-find-geofence-warrants-unconstitutional-0 [https://perma.cc/5KU8-9YLS] (last updated May 17, 2021) ("Two federal magistrate judges . . . have ruled that a geofence warrant violates the Fourth Amendment's probable cause and particularity requirements."); see also Ringrose & Ramjee, supra note 122, at 355–57 (discussing "warrantless geolocation searches" that can identify protesters and other individuals in a general vicinity, de facto subjecting a large number of civilians to governmental surveillance).

125. United States v. Chatrie, No. 3:19CR130, 2022 WL 628905, at *1 (E.D. Va. Mar. 3, 2022).

126. Id.

127. While the opinion uses the word "anonymized" to describe the information that Google would provide to the government, the author believes that the correct technical term is "pseudonymized." See *In re Search*, 481 F. Supp. 3d at 747. The description of the data the geofence warrant would compel Google to provide fits the definition of pseudonymized data—data where "pseudonyms" or identifiers replace the identity of a subject. See supra note 100. The opinion uses language such as "the 'anonymized' list of *unique device identifiers*" and "the anonymized list of device IDs." *In re Search*, 481 F. Supp. 3d at 747 (emphasis added).

128. *In re Search*, 481 F. Supp. 3d at 753–54.

129. In this case, although the government applied for a geofence warrant, it also noted "in a footnote to its brief" that *Carpenter* in fact did not control the government's actions—in other words, that it did not really need to apply for such a warrant. Id. at 736. The court, however, found that the government—by applying for a warrant and failing to develop any argument that the Fourth Amendment (and thus *Carpenter*) did *not* apply to the government's request for a geofence warrant—had forfeited such an argument, and thus the court did not need to rule on *Carpenter*'s applicability to the situation. Id. at 736–37.

130. Id. at 737, 756–57. The geofence warrant had requested data amounting to 2.25 hours of information—a far cry from *Carpenter*'s line in the sand of seven-plus days. See id. at 736.

Further, in ruling on the language of the proposed warrant itself, the judge saw no practical difference between a warrant that harnesses the technology of the geofence, easily and cheaply, to generate a list of device IDs that the government may easily use to learn the subscriber identities and a warrant granting the government unbridled discretion to compel Google to disclose some or all of those identities.[131]

The judge believed the discretion the government would enjoy by searching through multiple people's pseudonymized location data was equivalent to the government simply compelling Google to provide the identities of all the devices present within a certain place and time.[132] Despite acknowledging the "tempting" potential for the government to use Google's capabilities in such a manner, the judge noted that "a federal court in the United States of America should not permit the intrusion" where "the government can identify that wrongdoer only by sifting through the identities of unknown innocent persons without probable cause and in a manner that allows officials to 'rummage where they please in order to see what turns up,' even if they have reason to believe something will turn up."[133]

In *United States v. Walker*, an Eastern District of North Carolina judge alternatively found that *Carpenter* does not apply when law enforcement seeks aggregated location data from a "tower dump" of CSLI.[134] Here, the court upheld the government's use of an order under section 2703(d) of the SCA to acquire CSLI from a tower dump, despite the order "undisputed[ly]" requiring a showing of less than probable cause.[135] The judge reasoned that orders for the location data captured "not for one targeted individual for an extended time, chronicling that individual's private life for days, but rather capture[d] CLSI [sic] for a particular *place* at a *limited time*."[136] This distinction, in turn, *did not* invite the privacy concerns underpinning *Carpenter*, "where the search for data focuses not on 'the whole of [an individual's] physical movements' but rather on the data that was left

131. Id. at 749.

132. Id. at 756 (finding the proposed warrant flawed for granting "the government far greater discretion, namely, to sort through the location information and derivative identifying information of multiple people to identify the suspect by process of elimination" and that "[t]his amount of discretion is too great to comply with the particularity requirement").

133. Id. at 757 (citation omitted).

134. No. 2:18-CR-37-FL-1, 2020 WL 4065980, at *7 (E.D.N.C. July 20, 2020) ("The holding of *Carpenter* does not apply with equal force 'in the context of a tower dump request.'" (quoting Second Motion to Suppress at 7, *Walker*, 2020 WL 4065980, at *7)). Tower dumps—a request served on a cell phone service provider for all data from a cell tower within a specific time frame—are a "cousin" of geofence requests. Mark Rasch, Don't (Geo)Fence Me In: Courts Order Google to Give Up Location Data, Sec. Boulevard (Dec. 3, 2019), https://securityboulevard.com/2019/12/dont-geofence-me-in-courts-order-google-to-give-up-location-data/ [https://perma.cc/5SR8-YZEB].

135. *Walker*, 2020 WL 4065980, at *6 ("[T]he orders did not constitute warrants satisfying Fourth Amendment Requirements.").

136. Id. at *8 (citations omitted).

behind at a particular time and place by virtue of cell phone tower locations."[137]

These cases demonstrate that courts have not yet settled how *Carpenter* applies to the government's access to a database of pseudonymized, aggregated location data. That makes a case like *In re Search of: Information Stored at Premises Controlled by Google* an even more important barometer of how courts may eventually treat the government's purchase of commercial location data, which is functionally identical to data sought in a geofence warrant: If geofence warrants tread too closely to an unconstitutional general warrant, then the government's purchase of location data might evoke similar worries.

The similar nature of data in geofence warrants and commercial location data may make courts wary of the breadth of data the government can purchase, but wariness alone does not beget unconstitutionality. Analyzing the constitutionality of the government purchasing location data under *Carpenter* requires considering the third-party dynamics at play: that data brokers selling location data to the government likely acquire their data from other third-party acquirers who, at the earliest point in the supply chain, likely obtained the data from consenting users. The next section explores user consent to location data collection.

C. *Questioning the Strength of User Consent to Location Collection at the OS and Application Level*

The third key characteristic of commercial location data is the likelihood that users initially consented to the collection of such data. That consensually collected location data then fuels the supply chain where third parties buy and sell it and where the government may purchase it.

Consent happens at the smartphone's OS or application level, whether upon downloading an application or later by adjusting relevant settings.[138] Using popular rideshare applications or Google Maps, for example, requires users to affirmatively toggle settings to consent to location

137. Id. (alteration in original) (quoting Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018)) ("CLSI [sic] tower dump information gathered here is more akin to 'conventional surveillance techniques' and tools, such as security cameras and fingerprint collections, which capture data from *every* individual who came into contact with the crime scene in the manner revealed by the technology at issue." (quoting *Carpenter*, 138 S. Ct. at 2220)).

138. See Goode, supra note 58 (showing images of application location permission bubbles and settings).

data collection; otherwise, applications might not properly provide services.[139]

However, some have raised serious questions about the voluntariness of user consent to the collection of location data.[140] Some critique application permissions as "oversimplified." For example, it is hardly clear to what users are consenting, though they affirmatively agree.[141] When users consent to location data collection through user agreements (say, by "reflexively" toggling their "location services" on) they often have desperately insufficient notice that such consent might set in motion a buying-and-selling chain reaction—a reaction where their data enters the open market, reaches the government, and is used by law enforcement.[142] In a recent report detailing users' anecdotal reactions to learning how much their applications shared their location data, the *New York Times* reported that out of seventeen mobile applications sending precise location data, "just three on iOS and one on Android told users in a prompt during the permission process that the information could be used for advertising. Only one app, GasBuddy, which identifies nearby gas stations, indicated that data could also be shared to 'analyze industry trends.'"[143] Indeed, users' affirmative consent to location data collection does not track cleanly with users' *control* over data collection.[144] Once data enters the data broker supply chain, users have even less control over what happens to the information sourced from their mobile phone activities.[145]

---

139. See id. ("[A] ride-hailing app like Uber doesn't work without location information. Reject those permissions, and you'll break functionality.").

140. See infra note 149.

141. See Goode, supra note 58 ("Some app makers just tack 'and more' onto its permissions explanations. Facebook's explanation for location says 'Facebook uses this to make some features work, help people find places, and more,' while Snapchat's explanation for using your microphone is 'to record audio for Snaps, video chat, and more.'").

142. Michael D. Ricciuti, Privacy in the Cell Phone Age: New Restrictions on Police Activity, 52 Suffolk U. L. Rev. 393, 411 (2019) (noting that what user agreements with the likes of Facebook, Snapchat, Instagram, and others "say about waivers of privacy rights" in the context of the third-party doctrine may "become far more meaningful" if "the issue becomes the reasonableness of an expectation of privacy"); see also The Mobilewalla Business Services Privacy Policy, Mobilewalla (May 15, 2020), https://www.mobilewalla.com/business-services-privacy-policy [https://perma.cc/89Q6-EMDJ] [hereinafter Mobilewalla, Mobilewalla Business Services Privacy Policy] ("Mobilewalla will use information to enforce Mobilewalla's terms, policies and legal agreements, to comply with court orders and warrants, and assist law enforcement agencies . . . .").

143. Valentino-DeVries et al., supra note 24.

144. Yael Grauer, What Are 'Data Brokers,' and Why Are They Scooping Up Information About You?, Vice (Mar. 27, 2018), https://www.vice.com/en/article/bjpx3w/what-are-data-brokers-and-how-to-stop-my-private-data-collection [https://perma.cc/E59K-KH3X] ("Even when consumers are aware of both the existence of data brokers and the extent of data collected, it's difficult to determine which data they can control.").

145. Id. ("[S]ome data brokers might allow users to remove raw data, but not the inferences derived from it, making it difficult for consumers to know how they have been categorized. Some . . . store all data indefinitely, even if it is later amended. The industry is incredibly opaque . . . .").

To understand and anticipate how courts might eventually apply *Carpenter* to the government purchasing commercial location data for law enforcement, it is imperative to look at how current cases handle or comment on these open questions of consent at the mobile device or application level and whether sharing is truly voluntary. *Carpenter* itself assumed cell phone users did *not* voluntarily share location data with wireless carriers and that they in turn lacked agency to prevent wireless carriers from collecting their location data short of refusing to own a cell phone.[146] Consequently, the more courts appear willing to find that mobile users *involuntarily* share location data when that data comes from mobile applications, the more likely it will be that courts would find *Carpenter* applies to government purchasing location data, notwithstanding that users likely granted consent to its collection.

And courts have indeed expressed concern about mobile applications and mobile operating systems sharing users' data involuntarily. For example, in *United States v. Chatrie*, the Eastern District of Virginia district judge—after an extensive discussion on Google's collection and production of location data—was "unconvinced that the third-party doctrine would render hollow [the defendant's] expectation of privacy in his data, even for 'just' two hours" covered by the geofence warrant.[147] The judge went on to write that, although "the messiness of the current record as to how and when" the defendant gave consent made the Court unable to "reach a firm decision on the issue" that "Google Location History information—perhaps even more so than the cell-site location information at issue in *Carpenter*—is 'detailed, encyclopedic, and effortlessly compiled'" and that while the defendant "apparently took some affirmative steps to enable location history, those steps likely do not constitute a full assumption of the attendant risk of permanently disclosing one's whereabouts during almost every minute of every hour of every day."[148] In *In re Search*, the magistrate judge took note that "[p]ublished reports have indicated that many Google services on Android and Apple devices store the device users' location data even if the users seek to opt out of being tracked by activating a privacy setting that says it will prevent Google from storing the location data."[149] The presumption is that Google uses the unconsented-

146. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) ("Cell phone location information is not truly 'shared' . . . . Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. . . . [I]n no meaningful sense does the user voluntarily 'assume[] the risk' of turning over . . . his physical movements." (second alteration in original)).

147. United States v. Chatrie, No. 3:19CR130, 2022 WL 628905, at *26 (E.D. Va. Mar. 3, 2022).

148. Id.

149. In re Search of: Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 737 n.3 (N.D. Ill. 2020) (citing Ryan Nakashima, AP Exclusive: Google Tracks Your Movements, Like It or Not, Associated Press (Aug. 13, 2018), https://apnews.com/828aefab64d4411bac257a07c1af0ecb/AP-Exclusive:-Google-tracks-your-movements,-like-it-or-not [https://perma.cc/N4T3-LVMG] [hereinafter Nakashima, Google Tracks Your

to collection of location data to continue to refine its advertisement delivery.[150]

The judge, in turn, cited *Carpenter*'s reasoning in the specific context of smartphone users; he considered whether smartphone users face similar de facto involuntariness in sharing their location data as Carpenter did in sharing his CSLI with his wireless carrier. The court found it

> difficult to imagine that users of electronic devices would affirmatively realize, at the time they begin using the device, that they are providing their location information to Google in a way that will result in the government's ability to obtain—easily, quickly and cheaply—their precise geographical location at virtually any point in the history of their use of the device.[151]

Worry over a user's meaningful consent to data collection post-*Carpenter* has also reached the Seventh Circuit. In *Naperville Smart Meter Awareness v. City of Naperville*, the Seventh Circuit declined to extend the third-party doctrine to the collection of smart-meter data collected from homes, citing *Carpenter*.[152] As in *Carpenter*, the court found unpersuasive that sharing data with a third party completely disables Fourth Amendment protections; it instead discussed how

> a choice to share data imposed by fiat is no choice at all. If a person does not—in any meaningful sense—"voluntarily 'assume the risk' of turning over a comprehensive dossier of physical movements" by choosing to use a cell phone, it also goes that a

---

Movements] ("Even with Location History paused, some Google apps automatically store time-stamped location data without asking. (It's possible, although laborious, to delete it.)"); Ryan Nakashima, APNewsBreak: Google Clarifies Location-Tracking Policy, Associated Press (Aug. 16, 2018), https://apnews.com/ef95c6a91eeb4d8e9dda9cad887bf211/APNewsBreak:-Google-clarifies-location-tracking-policy [https://perma.cc/HAP7-CKS8] [hereinafter Nakashima, Google Clarifies Location-Tracking Policy] (reporting that days after the Associated Press reported Google stored location information for users who have opted not to have that information stored, Google clarified its practices and acknowledged that "some location data may be saved as part of your activity on other services, like Search and Maps").

150. See Nakashima, Google Clarifies Location-Tracking Policy, supra note 149 (noting Google "continues to track users even if they've disabled the setting" and "[c]ritics say Google's insistence on tracking its users' locations stems from its drive to boost advertising revenue"). Several state attorneys general have started to take notice, too: a bipartisan group of attorneys general from District of Columbia, Texas, Indiana, and Washington have sued Google, alleging the company has "deceptive practices to track users' physical location even when those users have made efforts to block Google from doing so." Brian Fung, Four Attorneys General Sue Google for 'Deceptive' Location Tracking, CNN (Jan. 24, 2022), https://www.cnn.com/2022/01/24/tech/google-lawsuit-location-tracking/index.html [https://perma.cc/SED2-762M].

151. *In re Search*, 481 F. Supp. 3d at 736–37 (emphasis added) ("In *Carpenter*, the Supreme Court concluded that this same line of reasoning, i.e., that persons voluntarily convey the information about their physical location (based on their devices' contact with cell towers) . . . did not apply because of the indispensable role mobile technology plays in modern society.").

152. See 900 F.3d 521, 527 (7th Cir. 2018).

> home occupant does not assume the risk of near constant monitoring by choosing to have electricity in her home.[153]

This case illustrates an appellate court reasoning that in situations of involuntary data sharing that invite "constant monitoring"—even with non-location data—*Carpenter* should govern.[154]

But other courts are not so keen to discount the affirmative consent that users may provide to location data collection from mobile applications and devices, finding it difficult to say users enjoy an expectation of privacy in the very data to whose collection they consented that companies subsequently buy and sell. In *United States v. Robinson*, a magistrate judge in the Eastern District of North Carolina considered a defendant's motion to suppress the government's acquisition of his real-time and historical CSLI with an invalid warrant.[155] The *Carpenter* court had specifically decided not to express a view on the government's acquisition of real-time CSLI.[156] Ultimately, the judge in *Robinson* found the defendant "fare[d] poorly" under *Katz*.[157] Because *Katz* is based on the premise that individuals wish to keep certain information private, the judge noted the difficulty in answering "how much sharing of location information a user can engage in before it can be said that they are no longer exhibiting an expectation of privacy in that information . . . ."[158] The judge found that users granting permission to share location data "from ordinary cellphone apps, including those for games, weather and e-commerce" weakened a *Katz* argument for expectation of privacy in location data—even when government purchases that data without a warrant and uses it for law enforcement purposes.[159]

The current dearth of judicial opinions concerning *Carpenter*'s application to purchased location data may make cases like *United States v. Robinson* a potential harbinger of the challenges advocates might face in

---

153. Id. (quoting *Carpenter*, 138 S. Ct. at 2220 (quoting Smith v. Maryland, 442 U.S. 735, 745 (1979))).

154. Id. While the Seventh Circuit ultimately found that the search of the smart meter data was reasonable, the case is important as applied because the Seventh Circuit, citing *Carpenter*, declined to apply the third-party doctrine to non-CSLI data, notwithstanding the fact that the data was shared with third parties. Further, the Seventh Circuit added for good measure: "We caution . . . that our holding depends on the particular circumstances of this case. Were a city to collect the data at shorter intervals, our conclusion could change. Likewise, our conclusion might change if the data was more easily accessible to law enforcement or other city officials outside the utility." Id. at 529.

155. No. 7:18-CR-00103-FL-1, 2020 WL 1648480, at *4 (E.D.N.C. Mar. 5, 2020), report and recommendation adopted, No. 7:18-CR-103-FL-1, 2020 WL 1641283 (E.D.N.C. Apr. 2, 2020).

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

157. *Robinson*, 2020 WL 1648480, at *7.

158. Id. at *7–8.

159. Id. at *7 ("[R]ecent news reports claim that, in the aftermath of *Carpenter*, 'the federal government has essentially found a workaround by purchasing location data used by marketing firms rather than going to court on a case-by-case basis.'" (citing Tau & Hackman, supra note 14)).

convincing courts that the government cannot purchase information that users appear to readily share with the open market.[160] But it also may not. There is uncertainty on how courts might treat the government's purchasing of commercial location data for law enforcement purposes. Part II shows it is still possible to anticipate how a court might approach the question by looking at the three characteristics of commercial location data currently influencing debates in courts. Comparing *Robinson* and *In re Search* shows, for example, the emerging different thinking on the extent to which location data is voluntarily shared. Similarly, there is conflicting authority on whether *Carpenter* can be applied to non-CSLI and to aggregated, pseudonymized location data. The sum of these tensions in areas with parallel characteristics of purchased location data will inform how courts might debate the direct application of *Carpenter* to purchased location data.

III. REGULATING THE GOVERNMENT'S PURCHASE OF LOCATION DATA FOR AIDING LAW ENFORCEMENT

Part II highlighted three areas characteristic of commercial location data that the government might purchase. It showed the tension in how lower courts are thinking through *Carpenter*'s application to three areas: non-CSLI location data; aggregated, pseudonymized data; and involuntarily shared data. Because courts have yet to address the constitutionality of the government's use of purchased location data for law enforcement post-*Carpenter*, understanding courts' approaches to the characteristics that comprise commercial location data is essential.

Given this, Part III proposes that *Carpenter* applies to the government's practice of purchasing location data. Part III argues that courts' approaches to non-CSLI location data, aggregated and pseudonymized data, and involuntarily shared data compel the application of the Fourth Amendment to the government's use of purchased location data for law enforcement purposes. This proposal resolves a present uncertainty rooted in the lack of case law; importantly, however, some nonjudicial portions of the government—separate from the agencies and units that purchased location data—are aligned with this application of *Carpenter*. In mid-February 2021, the Treasury Inspector General for Tax Administration issued a letter in response to inquiring senators regarding the use of Venntel licenses to drive law enforcement efforts.[161] In offering its own brief analysis, the letter expressed the possibility that *Carpenter* might ultimately preclude the government from purchasing location data for law

160. Indeed, this is the only case the author could find explicitly mentioning the fact that the government has purchased and used location data for law enforcement purposes.

161. See Letter from J. Russell George, Inspector Gen., Tax Admin., to Sens. Ron Wyden and Elizabeth Warren 1 (Feb. 18, 2021) (on file with the *Columbia Law Review*).

enforcement.[162] While the letter is significant in its own right (as the first known government analysis raising doubts about the constitutionality of the government purchasing location data for law enforcement), it also reinforces the need for a stronger understanding of the constitutionality of law enforcement using purchased location data and of possible statutory resolutions.[163] Part III does exactly this.

Section III.A argues that *Carpenter* logically applies to governmental purchases of location data, notwithstanding distinguishing characteristics of purchased location data versus the CSLI at issue in *Carpenter*. Such an application would preclude the government from purchasing its way around the Fourth Amendment and constitutionally regulate federal law enforcement agencies' use of commercial location data.[164] Section III.B discusses the main challenge to this proposition and a possible solution. Section III.B.1 discusses the challenge that commercial location data likely contains data from at least some users who do truly consent to share their location data (thus inviting the third-party doctrine to exclude application of the Fourth Amendment) as well as users who involuntarily share location data (thus, following *Carpenter*, rejecting the third-party doctrine's application). Section III.B.2 then offers a statutory answer to this challenge.

A. Carpenter *Applies to Purchased Location Data That Is Involuntarily Shared*

Carpenter should apply to governmental purchase of location data—and not just acquisition by legal instruments—because location data purchased from the open market invites the same worries that did data acquired directly from wireless carriers in *Carpenter*. Such worries should be remedied the same as in *Carpenter*: by precluding warrantless governmental access to seven-plus days of location data.[165]

Three principles around the data at issue in *Carpenter* make clear its holding should also cover law-enforcement-purchased location data if such data covers more than seven days:[166] first, the content of the data

---

162. See id. ("The Court's rationale [in *Carpenter*] was that phone users do not truly voluntarily agree to share the information given the necessity of phones in our society. Courts may apply similar logic to GPS data sold by marketers, particularly if the Government . . . [can] identify the phone's owner . . . .").

163. Byron Tau, Treasury Watchdog Warns of Government's Use of Cellphone Data Without Warrants, Wall St. J. (Feb. 22, 2021), https://www.wsj.com/articles/treasury-watchdog-warns-of-governments-use-of-cellphone-data-without-warrants-11614003868 (on file with the *Columbia Law Review*).

164. See Edelman, supra note 13.

165. See Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

166. The seven-day threshold might change. See In re Search of: Info. Stored at Premises Controlled by Google, 481 F. Supp 730, 737 (N.D. Ill. 2020) (noting, in dicta, that "there is much to suggest that *Carpenter*'s holding, on the question of whether the privacy interests in CSLI over at least seven days, should be extended to the use of geofences involving intrusions of much shorter duration").

(location) and its comprehensiveness (constant monitoring);[167] second, that the data can reasonably describe individuals' movements;[168] and third, that individuals do not truly voluntarily share comprehensive location data.[169] When the government purchases datasets in which these factors are present, *Carpenter* must necessarily govern the purchase.

Consequently, section III.A.1 argues that, in light of its initial purpose and trajectory of early progeny, *Carpenter* applies to the government's purchase of seven-plus days of non-CSLI location data used for law enforcement. Section III.A.2 argues that when the government purchases location data, that data is functionally de-anonymized and thus mirrors the original worry in *Carpenter* that warrantless access to seven-plus days of location history violates an *individual's* expectation of privacy. Section III.A.3 argues that the same consent and de facto involuntary data sharing issues in *Carpenter* are present when smartphones and applications collect location data.

1. Carpenter *Applies Beyond CSLI*. — Bulk, commercial location data provides analogous location information as to what CSLI can reveal, evoking the same worries at issue in *Carpenter*, even when commercial location data is not pure CSLI.[170] *Carpenter*'s initial purpose—and the trajectory of early progeny—demands that its holding applies when data meets two criteria: the right type of data (an individual's location) and the right volume of data (a level of comprehensiveness).

First, on data type: While *Carpenter* focused on CSLI, neither its reasoning nor holding found dispositive the technical composition of CSLI but rather found that the use of CSLI committed a broader harm.[171] Because government warrantlessly using comprehensive location data it purchased evokes the same worries, the same expectation of privacy found valid and violated in *Carpenter* necessarily is valid and violated when the government chooses to "buy its way around the Fourth Amendment," even

---

167. See *Carpenter*, 138 S. Ct. at 2220 ("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." (alteration in original) (quoting Smith v. Maryland, 442 U.S. 735, 745 (1979))).

168. See id. ("[T]his case is not about 'using a phone' or a person's movement at a particular time. It is about a detailed chronicle of a person's physical presence compiled every day, every moment, over several years. Such a chronicle implicates privacy concerns far beyond those considered in *Smith* and *Miller*.").

169. See supra note 167 and accompanying text.

170. See Edelman, supra note 13 ("The location tracking made possible by app data in 2020 is more precise and potentially even more comprehensive than the cell tower data that the FBI used back in 2011 [in *Carpenter*].").

171. *Carpenter*, 138 S. Ct. at 2217 ("Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection. . . . The location information obtained from Carpenter's wireless carriers was the product of a search.").

where location data is not pure CSLI.[172]

But it is the combination of location data *and* its comprehensiveness that dictates *Carpenter*'s application. If the government merely obtaining data revealing an individual's location was indicative of Fourth Amendment protections, without controlling for comprehensiveness (say, seven days of data—the court's current temporal yardstick of comprehensiveness), then *Carpenter* would apply to data collected from a single license plate passing through an EZ-Pass or a computer user's IP address visiting a single website.[173] This broad application would risk falling outside *Carpenter*'s underlying worry of law enforcement's access to location data with "depth, breadth, and comprehensive[ness]."[174] Indeed, it was not merely that law enforcement in *Carpenter* sought location data via the SCA's lower-than-probable cause standard but rather that the data sought was "an all-encompassing record of the holder's whereabouts."[175]

Echoes of what is known as the Mosaic Theory suggest that it is data revealing not just an individual's location but their comprehensive location *history* that invites constitutional protection.[176] The Mosaic Theory asks courts to consider whether a set of "nonsearches," aggregated together, constitute a search.[177] The theory's principle played a role in the opinions that five Justices wrote or joined in *United States v. Jones*, which can be read together as openness to the notion that monitoring an individual in a comprehensive, round-the-clock manner violates *Katz*—even where snippets of an individual's location (like location information sourced from a license plate reader) may itself not be a search.[178] *Carpenter* affirmed this principle.[179]

---

172. Edelman, supra note 13.

173. See Mariko Hirose, Newly Obtained Records Reveal Extensive Monitoring of E-ZPass Tags Throughout New York, ACLU (Apr. 24, 2015), https://www.aclu.org/blog/privacy-technology/location-tracking/newly-obtained-records-reveal-extensive-monitoring-e-zpass [https://perma.cc/A5SE-MPEC]; Dave Johnson, What You Can Do With an IP Address, and How to Protect Yours From Hackers, Bus. Insider (June 2, 2020), https://www.businessinsider.com/what-can-you-do-with-an-ip-address [https://perma.cc/6N2Y-NU4K] (showing IP address can reveal users' locations).

174. *Carpenter*, 138 S. Ct. at 2223 (noting the opinion does not "address other business records that might incidentally reveal location information").

175. Id. at 2217.

176. See Orin S. Kerr, The Mosaic Theory of the Fourth Amendment, 111 Mich. L. Rev. 311, 320 (2012) (noting "[t]he mosaic theory requires courts to apply the Fourth Amendment search doctrine to government conduct as a collective whole rather than in isolated steps" and that it "asks whether a *series of acts* that are not searches in isolation amount to a search when considered as a group" (emphasis added)).

177. Id.

178. Id. at 326, 328 ("[T]he concurring opinions in *Jones* analyze the collective sum of government action, rather than individual sequential steps, to determine what counts as a Fourth Amendment search.").

179. *Carpenter*, 138 S. Ct. at 2218 (discussing how location data's "retrospective quality" allows law enforcement to reconstruct a person's movements and how tracking an individual

Courts currently finding *Carpenter* applies beyond CSLI already appear to follow this logic. For example, lower courts are applying *Carpenter* when data comprehensively shows an individual's location—even in cases of non-CSLI data, like GPS or smart meters.[180] In the same vein, agencies like CBP are then wrong to imply that *Carpenter* does not govern its practices of using purchased location data because the location data they purchased from the open market is not, technically speaking, pure CSLI.[181] If the data the agencies purchased showed more than seven days of location data, then the agencies cannot avoid *Carpenter* merely based on the data's technical composition.

2. *Aggregated, Pseudonymized Data Still Risks Individuals' Privacy.* — *Carpenter*'s application to the government purchasing commercial location data covering an individual's location does not exclude aggregated, pseudonymized data. In other words, *Carpenter* applies even when the government purchases location data where data sets comprise aggregated movements of numerous, unnamed cell phone users. This is because the ease of deanonymizing location data means even aggregated, pseudonymized location data can de facto violate an individual's privacy. The ability to deanonymize location data is not difficult; location data services company Mobilewalla, for example, reserves the right to do so directly in its privacy policies[182] and explains in a technology whitepaper that "[t]he depth and breadth of Mobilewalla . . . allows us to build a portrait around each device ID."[183] It has also admitted to doing so in practice (to advance the GOP 2016 get-out-the-vote efforts).[184]

Reporting has shown just how easily aggregated, pseudonymized lo-

---

via the location of their cell phone "achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user").

180. See Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 527 (7th Cir. 2018) (noting that *Carpenter* applied to find that a search occurred of non-CSLI smart meter electricity readings from people's homes, even if that search was reasonable); United States v. Diggs, 385 F. Supp. 3d 648, 653–54 (N.D. Ill. 2019) (finding *Carpenter* applied to GPS data taken from a vehicle).

181. Wall St. J., How the U.S. Government Obtains and Uses Cellphone Location Data, supra note 63, at 02:22 ("While CBP is being provided access to location information, it is important to note that *such information does not include cellular phone tower data*, is not ingested in bulk, and does not include the individual user's identity . . . ." (emphasis added)).

182. Mobilewalla, Mobilewalla Business Services Privacy Policy, supra note 142 ("We may use business data, personal information and other information about individuals to create de-identified and aggregated information, such as de-identified demographic information, de-identified location information, information about the computer or device from which individuals access our Business Services, or other analyses we create.").

183. See Mobilewalla, Audience Segments, supra note 44.

184. Lorenzo Franceschi-Bicchierai, Firm That Tracked Protesters Targeted Evangelicals During 2016 Election, Vice (June 26, 2020), https://www.vice.com/en/article/9353qv/mobilewalla-tracked-protesters-targeted-evangelicals-during-2016-election [https://perma.cc/UN2W-EMYN].

cation data can be de-anonymized.[185] In late 2018, a New York Times interactive piece demonstrated with stunning visuals what research has already proven: that location data that mobile applications collect—despite not being "tied . . . to someone's name or phone number"—can be quickly de-anonymized and individuals' entire lives revealed with extreme ease.[186]

The *New York Times* reviewed a database of information gathered in 2017 by a company that receives precise location data from apps whose users enable location services to get local news, weather, or other information (the company was one of seventy-five companies the *New York Times* found, several of which "claim to track up to 200 million mobile devices in the United States").[187] The data reveals people's day-to-day movements "in startling detail, accurate to within a few yards and in some cases updated more than 14,000 times a day."[188] After acquiring the data, de-anonymization is fairly straightforward: People with access to the raw data could identify a person they already know by following whatever unique pseudonymized identifier regularly spent time at that person's home. Working in reverse, those with access to the data can just as easily "attach a name to an anonymous dot" and see "where the device spent nights and us[e] public records to figure out who lived there."[189] Incidentally, this is exactly how law enforcement agents would de-anonymize aggregated data received from a geofence warrant.[190]

In the same vein, the distinctions that agencies like CBP make, that commercial location data does not identify individuals, are substantively misleading. CBP reports that its location data does not include individuals'

---

185. See Dan Calacci, Alex Berke, Kent Larson & Alex 'Sandy' Pentland, The Tradeoff Between the Utility and Risk of Location Data and Implications for Public Good, arXiv.org 3 (2019), https://arxiv.org/pdf/1905.09350.pdf [https://perma.cc/4M9U-B7FW] (noting a 2013 study of 1.5 million users whose data was "scrubbed of their identities ('de-identified') showed the ease with which users could be re-identified, . . . [because of] individual 'mobility traces'" and that "[j]ust four randomly selected spatio-temporal points were enough to uniquely identify 95% of users in the dataset" (footnote omitted)); see also McKay Cunningham, Exposed, 2019 Mich. St. L. Rev. 375, 409–10 ("Anonymization, for the same reason, fails to inoculate data. Merely stripping the name off locational data, for example, does not prevent that locational data from identifying the user. Advances in computer science increase the likelihood of re-identifying supposedly 'anonymized' data, rendering futile many attempts to protect privacy with anonymity." (footnotes omitted)); Stuart A. Thompson & Charlie Warzel, Opinion, Twelve Million Phones, One Dataset, Zero Privacy, N.Y. Times (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html (on file with the *Columbia Law Review*); Wall St. J., How the U.S. Government Obtains and Uses Cellphone Location Data, supra note 63, at 04:15 (noting the ease of figuring out to whom a cell phone belongs).

186. Valentino-DeVries et al., supra note 24.

187. Id.

188. Id.

189. Id.

190. See supra section II.B.

identities, but its own privacy assessment shows how individualized commercial location data can be: The agency's own privacy assessment of its border surveillance technologies, which explicitly includes "the use of commercial[] . . . location data," says such technology is in use to "monitor individuals in a particular border location as part of a law enforcement investigation, and may be used as evidence if the apprehension of the individual results in criminal or administrative proceedings."[191] As the *Wall Street Journal* reported in early 2020, for example, CBP and ICE, both divisions of DHS, used purchased access to a commercial database "that maps the movements of millions of cellphones" to advance immigration work: CBP used the data to search for cell phone activity in unusual places; ICE used the data to carry out deportations.[192] In one reported incident, ICE detected cell phones moving through a previously undiscovered tunnel between the United States and Mexico that ended in a closed Kentucky Fried Chicken on U.S. land.[193] Yet even though the purchased location data contributed to the restaurant's owner's arrest, police records of the incident did not mention the use of cell phone location data, instead attributing the case "to a routine traffic stop."[194]

The ease with which pseudonymized location data can be deanonymized—coupled with the knowledge that federal agencies currently use commercially available, facially pseudonymized location data to "monitor individuals"—is sufficient to show that the same worry of infringement of an individual's privacy at issue and protected in *Carpenter* applies when the government buys aggregated, bulk location data from the private sector.

3. *Commercial Location Data Is Sourced From Involuntarily Shared Location Data From Users' Mobile Applications.* — The same de facto involuntariness of location data sharing explicitly recognized in *Carpenter* exists for cell phone users with smartphone OSes and mobile applications.[195] This de facto involuntariness necessitates *Carpenter*'s application to government purchases of location data: De facto involuntariness implies that users do not truly consent—as in, choose—to share location data with their OSes and mobile applications. Without consent, distinctions between government purchasing location data and government acquiring it directly from wireless carriers—and thus requiring a warrant—break down considerably.

That users either consent to ambiguous permissions or that their lack of consent may be patently ignored is especially meaningful in the context

191. DHS, supra note 15, at 1.

192. Tau & Hackman, supra note 14.

193. Id.

194. Id.

195. See Cristina Del Rosso & Carol M. Bast, Protecting Online Privacy in the Digital Age: *Carpenter v. United States* and the Fourth Amendment's Third-Party Doctrine, 28 Cath. U. J.L. & Tech. 89, 120–21 (2020) ("[M]any device users do not voluntarily relinquish information; rather, when the devices are powered on, information is sent on behalf of the individual to third parties.").

of modern smartphone usage. The Supreme Court has now recognized the special place that cell phones and their data hold in Fourth Amendment doctrine.[196] In *Carpenter*, the Court was clear: "[C]ell 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."[197] Given this pervasiveness, *Carpenter* recognized that users had little agency when, "by dint of [a cell phone's] operation, without any affirmative act on the part of the user beyond powering up," wireless carriers recorded users' locations around the clock.[198] Today, use of location-data-gathering applications is part and parcel of smartphone usage; thus, the permission structure to consent to such applications' data gathering practices, if so impenetrable as to preclude meaningful consent, invites the same worries that *Carpenter* discussed around the involuntary collection of CSLI.[199]

With respect to purchased data, accounts of location data collected not only without consent but in the face of explicit denial of consent demonstrates that at least some data feeding the commercial location data supply chain is not consented-to data.[200] The only difference between Google storing users' location data even after requests to prevent such sharing and the scenario at issue in *Carpenter* is that Google—and not MetroPCS and Sprint, Carpenter's wireless carriers—collected the data.[201]

In sum, the proper way to apply *Carpenter* is to find its holding governs seven-plus days of location data (commercially available or not) even when the data at issue is not purely CSLI; even when the data is aggregated to depict a group of people and not a single individual; and even when there appears to be consent to the collection if that consent is de facto involuntary.

---

196. See Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018) ("The Court has in fact already shown special solicitude for location information in the third-party context."); Riley v. California, 573 U.S. 373, 393 (2014) ("Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse. . . . Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on [one's] person.").

197. *Carpenter*, 138 S. Ct. at 2220 (quoting *Riley*, 573 U.S. at 385).

198. Id.

199. Id. ("[C]ell 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." (quoting *Riley*, 573 U.S. at 385)).

200. Nakashima, Google Tracks Your Movements, supra note 149 (reporting that many Google services on Android devices and iPhones store location data even if users selected privacy settings meant to prevent Google from doing so).

201. *Carpenter*, 138 S. Ct. at 2212.

B. *The Difficulty of Ex Ante Application of Fourth Amendment Protections Against the Government's Warrantless Purchasing of Comprehensive Location Data*

Section III.A argues that *Carpenter* necessitates finding that the government violates an individual's expectation of privacy when using commercially available, comprehensive location data to advance law enforcement. There are, however, challenges in applying only constitutional protections against the government buying its way around the Fourth Amendment. Section III.B.1 briefly describes this challenge; section III.B.2 offers a statutory solution.

1. *The Challenge of Parsing Out Genuine Affirmative Consent to Data Collection.* — There are two challenges to effectively applying the Fourth Amendment ex ante to protect against the government's warrantless purchase of location data. First, even if *Carpenter* were to counsel protection for location data *before* it enters the supply chain, that protection might extinguish if data is sold to third parties on the open market who then in turn sell to the government. Second, for *Carpenter*'s ability to govern over commercial location data at all, user consent to applications and OSes collecting their location data would itself have to be analogously problematic enough such that the government cannot benefit from such consent.

Indeed, the reasoning that led *Carpenter*'s refusal to extend the third-party doctrine to seven-plus days of location data from wireless carriers—the worry of *involuntariness*—may not necessarily shut out the third-party doctrine when consent to data collection is voluntary, even if not fully informed.[202] Not all applications that collect and then sell or share location data are necessarily analogous to Carpenter's involuntary data sharing experience; it is possible for users to affirmatively and genuinely consent to share data with certain applications which cannot as easily be analogized to Carpenter's involuntary data sharing with his wireless carrier.[203]

Consequently, where uninformed users voluntarily consent to share data with mobile applications, the third-party doctrine may permit federal agencies to purchase commercial location data composed of that consented-to data: Consent at the OS or application level would be sufficient, as the third-party doctrine does not require users to consent to the *government's* use of their data but merely allows the government to

---

202. Id. at 2220 ("Cell phone location information is not truly 'shared' as one normally understands the term. In the first place, 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." (quoting *Riley*, 573 U.S. at 385)); see also Michelle Tomkovicz, Comment, If You're Reading This, It's Too Late: The Unconstitutionality of Notice Effectuating Implied Consent, 70 Emory L.J. 153, 190 (2020) ("Under the consent exception to the Fourth Amendment warrant requirement, in determining whether officers obtained valid consent to search, courts look to indication, authority, voluntariness, and scope.").

203. While applications like Google Maps could be considered part and parcel of using a smartphone, the argument is harder to make, perhaps, for a flashlight.

benefit from the users' sharing with the data collector.[204] But the third-party doctrine would simultaneously preclude government from purchasing commercial location data sourced from applications where users involuntarily consent to data collection, à la *Carpenter*.[205]

One answer to this challenge is placing the burden on the government to prove users voluntarily consented to location data collection when the government uses the data for law enforcement purposes. With this approach, a challenger who voluntarily consented to location data collection would lose, but one who did not voluntarily consent would win, with the government bearing the risk ex ante of not knowing whether the purchased data came from voluntarily consenting users. Ultimately, though, this outcome is inefficient; it makes ex ante guidance difficult around the constitutionality of law enforcement agencies purchasing commercial location data, and it also would likely incentivize government to be more discerning of the sources from which agencies purchased location data and would ultimately allow agencies to continue buying their way around the Fourth Amendment.

2. *A Statutory Solution: Applying the Stored Communications Act.* — A statutory approach would remedy this ex ante difficulty by building on the constitutional floor, focusing privacy protection on those the government acquires location data from in bulk—regardless of whether user consent to share data was voluntary or involuntary.

Early discussions of statutory approaches to regulate government purchasing location data are already in play: Senator Ron Wyden of Oregon, for example, has publicly called for legislation to curb federal agencies' practices of buying location data.[206] In other contexts, the Network Advertising Initiative, a national trade group representing the digital advertising industry, has recommended member companies put stricter controls on

---

204. See Smith v. Maryland, 442 U.S. 735, 743–44 (1979) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").

205. Compare Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 527 (7th Cir. 2018) ("If a person does not—in any meaningful sense—voluntarily assume the risk of turning over a comprehensive dossier of physical movements by choosing to use a cell phone then a home occupant does not assume the risk of near constant monitoring by choosing to have electricity in her home" (internal quotation marks omitted) (quoting *Carpenter*, 138 S. Ct. at 2220 (quoting *Smith*, 442 U.S. at 745))), with Christo Lassiter, Consent to Search by Ignorant People, 39 Tex. Tech L. Rev. 1171, 1174 (2007) ("[C]onsent to search renders the otherwise unreasonable intrusion onto Fourth Amendment privacy reasonable.").

206. Katie Canales, Sen. Ron Wyden Is Introducing a Privacy Bill That Would Ban Government Agencies From Buying Personal Information From Data Brokers, Bus. Insider (Aug. 4, 2020), https://www.businessinsider.com/ron-wyden-fourth-amendment-is-not-for-sale-privacy-2020-8 [https://perma.cc/9ZTK-DGYV]; Cushing, Secret Service, supra note 16 (noting Senator Wyden's statement that "[i]t is clear that multiple federal agencies have turned to purchasing Americans' data to buy their way around Americans' Fourth Amendment Rights" and that he is "drafting legislation to close this loophole, and ensure the Fourth Amendment isn't for sale").

the consumer mobile-phone location data they provide to government.[207] Even Silicon Valley has called to better regulate location data.[208]

But existing statutory structures—interpreted in slightly different ways—could also protect individuals' expectations of privacy in commercial location data. The SCA, already *Carpenter*'s background statutory context, offers a prime opportunity to regulate location data such that the government has limited ability to purchase bulk location records (whether or not a warrant would otherwise be required) without impacting sales between private companies.

The SCA already attempts to stop consumer data from reaching the government without any friction. Section 2702(a)(3) reads that a "provider of remote computing service or electronic communication service to the public shall not *knowingly* divulge a record or other information pertaining to a subscriber to or customer of such service . . . to any governmental entity."[209] But this prohibition has two problems. First, it excludes companies that are not remote computing services or electronic communication services (like data brokers).[210] Second, even for SCA-covered entities, it only restricts companies *directly* divulging records or other customer information; nothing in the SCA in turn prevents location data, for example, from leaving an SCA-covered entity, traveling through private-sector companies in the supply chain, and then being purchased by government.[211]

Both these problems are remediable: Section 2702(a)(3) should be interpreted such that SCA-covered entities violate the section not only when *directly* divulging customer records, like location data, to a governmental entity but also when *indirectly* divulging such records—in other words, when they divulge records that they know or reasonably should know will eventually be shared or re-sold to law enforcement by a *non*-governmental entity.[212] Applying an expanded interpretation of

---

207. Byron Tau, Digital Group Urges Controls on Flow of Cellphone Data to Government, Wall St. J. (June 23, 2020), https://www.wsj.com/articles/digital-group-urges-controls-on-flow-of-cellphone-data-to-government-11592946810?mod=searchresults&page=1&pos=12 (on file with the *Columbia Law Review*).

208. See Zack Whittaker, Foursquare CEO Calls on Congress to Regulate the Location Data Industry, TechCrunch (Oct. 16, 2019), https://techcrunch.com/2019/10/16/foursquare-congress-regulate-location-data [https://perma.cc/3BER-CFSM].

209. 18 U.S.C. § 2702(a)(3) (2018) (emphasis added).

210. See Edelman, supra note 13 (warning that the SCA "probably doesn't apply to a broker like Venntel that doesn't deal with consumers directly").

211. See Simmons, supra note 70, at 977–78 (noting that the SCA "allows service providers to disclose consumer records to 'any person other than a governmental entity,' such as a fourth-party, and there is no provision preventing the fourth-party from giving that information to the government in turn").

212. SCA-covered entities are well in their statutory rights to share data, generally, with entities other than the government. See 18 U.S.C. § 2702(c)(6) (permitting entities to disclose data to "any person other than a governmental entity"); see also Edelman, supra note

"knowingly" helps remedy the second problem and de facto remedy the first by preventing SCA-covered entities from both directly *and* indirectly divulging customer records to the government. This interpretation prevents SCA-covered entities from inadvertently "laundering"[213] location data through a non-governmental, non-SCA-covered entity that then could sell such data directly to the government.[214]

Interpreting section 2702(a)(3) in this manner provides a statutory band-aid over wounds the third-party doctrine's logic inflicts.[215] The volume of public reporting on federal agencies' use of purchased location data is now sufficiently widespread that it would be reasonable to impute such knowledge to an SCA-covered entity who sells location data to an aggregator or other third-party data broker that is a de facto middleman in the location data supply chain, like Venntel, between the private sector and government.[216]

This interpretation also gets at the heart of the SCA's broader goal: to prevent inappropriate disclosures of consumers' digital information to the government.[217] Further, it would also incentivize SCA-covered entities to be more scrupulous of the data brokers with whom they share bulk location data so as to avoid violating the SCA's provision themselves. This interpretation, importantly, also does not concern itself with whether users voluntarily or involuntarily consent to share their location data in the first instance. This interpretation also would not unintentionally restrict location data from flowing within the private-sector supply chain; it merely concerns itself with preventing data from crossing without a warrant to the

---

13 (noting that under the SCA, prohibitions of knowingly sharing data "probably" do not apply to data brokers that do not "deal with consumers directly" but "could apply to the app makers . . . passing data along to companies like Venntel, if they know it will eventually end up in the government's hands").

213. Simmons, supra note 70.

214. See § 2702(c)(6).

215. Congress similarly passed the Right to Financial Privacy Act in direct response to United States v. Miller, 425 U.S. 435 (1976) finding that, due to the third-party doctrine, individuals lack an expectation of privacy in their bank records. See Orin S. Kerr, The Case for the Third-Party Doctrine, 107 Mich. L. Rev. 561, 596 (2009).

216. Edelman, supra note 13. Indeed, the ACLU lawyer who himself argued *Carpenter* explicitly asks:

> What happens if the weather app is selling it to some location aggregator, but they know that one or two or three steps down the chain of contract, DHS is buying it? Are they knowingly divulging it to a government entity? After today's Journal story, if I was a lawyer at one of those companies, I would be sweating. It's a really substantial question. Id.

217. See 18 U.S.C. § 2702(a); see also Christopher J. Borchert, Fernando M. Pinguelo & David Thaw, Reasonable Expectations of Privacy Settings: Social Media and the Stored Communications Act, 13 Duke L. & Tech. Rev. 36, 39 (2015) ("Congress enacted the SCA in 1986 to provide a set of Fourth Amendment-like privacy protections for communications made online because it was, and still remains, largely unclear whether traditional Fourth Amendment protections extend to the online context.").

government. Consequently, there would be no limiting impact on the benefits of location data being collected to run mobile applications and services, which could all continue to collect location data with no interruptions.

Section 2702(a)(3) is ripe for interpretation in this manner and would allow, with already existing language, a mechanism to stem the tide of companies selling location data to the government for which otherwise a warrant would be needed. Admittedly, *Katz* does not typically protect individuals' expectations of privacy in their location data traveling on the open market.[218] But neither is it typical for the government to be able to purchase data from the open market for which it would otherwise need a warrant. It is antithetical to one of the goals of the SCA—preventing the government from voluntarily receiving records about individuals from service providers—to have the introduction of a data broker as a middleman between an SCA-covered entity and the government extinguish any protection the SCA would otherwise provide consumers and their data. While this requires treating the government differently on the open market than private entities untouched by the Fourth Amendment, it is a necessary treatment: *Carpenter* and its progeny should push courts to rethink the notion that the government is a purchaser like anyone else.[219]

CONCLUSION

Carpenter v. United States entered the annals of case law at a time of great and rapid technological change. Despite the Court's efforts to keep *Carpenter*'s scope narrow so as not to "embarrass the future,"[220] lower courts have already started a tug-of-war calibrating just how far *Carpenter* may reasonably stretch as they face growing technological stressors on longstanding legal doctrine. Though courts will undoubtedly continue to debate *Carpenter*'s scope, its application to commercial location data is both doctrinally sound and normatively necessary: The similarities between the commercial location data that the government purchases and the location data that the government gets from wireless carriers—only with a warrant—far outweigh any distinctions between the two. Focusing arbitrarily on the distinctions improperly allows a backdoor for the government to inadvertently launder purchased location data; focusing instead on the similarities properly applies the Fourth Amendment for its intended purpose: "to secure 'the privacies of life' against 'arbitrary power.'"[221]

---

218. See supra note 81 and accompanying text.

219. See Panduranga et al., supra note 46, at 2 (noting that it may be the case that government "may be able to buy [location data] from a data broker who is legally able to purchase similar information from a smartphone application developer who collects it").

220. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

221. Id. at 2214 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).