**Our Fourth Amendment Privacy Is Not For Sale**

*Kyle C. Bailey*

**Introduction**

There is a spy in your pocket. The mobile applications on your smartphone continuously track your exact location, and the information is not kept secret.[[1]](#footnote-1) Instead, the apps send your location to numerous companies, up to 14,000 times a day.[[2]](#footnote-2) The companies then sell your information in massive databases containing data on millions of Americans.[[3]](#footnote-3) And the federal government is buying. Federal law enforcement agencies like Immigration and Customs Enforcement spend millions of dollars accessing commercial databases of mobile application location information (MALI) to assist in criminal investigations.[[4]](#footnote-4)

The federal government’s use of MALI implicates Fourth Amendment privacy rights. The Supreme Court recognized this extreme privacy risk, noting that “when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone’s user.”[[5]](#footnote-5) Accordingly, in *Carpenter v. United States*, the Court held that historical cell-site location information (CSLI) held by wireless carriers is protected by the Fourth Amendment.[[6]](#footnote-6) *Carpenter*brought the Fourth Amendment into the digital age by recognizing that cell phone location tracking “has afforded law enforcement a powerful new tool . . . [which] risks Government encroachment of the sort the Framers . . . drafted the Fourth Amendment to prevent.”[[7]](#footnote-7) Although the decision purported to be narrow, the majority’s reasoning applies to any geolocation tracking technology, including MALI.[[8]](#footnote-8)

**There is a Reasonable Expectation of Privacy in MALI**

In *Carpenter*, the Court held that “individuals have a reasonable expectation of privacy in the whole of their physical movements.”[[9]](#footnote-9) MALI meets this standard for the same reasons as CSLI: the information is “retrospective” and “deeply revealing.”[[10]](#footnote-10) MALI is retrospective because it provides a historical record of an individual’s location, allowing the government to “travel back in time” to follow a person without knowing in advance whom to track.[[11]](#footnote-11) Additionally, MALI is deeply revealing because it is precise and generated frequently. Mobile apps use geolocation technologies like GPS and WiFi positioning to accurately track a cell phone within 10–15 feet.[[12]](#footnote-12)

In contrast, the CSLI in *Carpenter* was only accurate within “one-eighth to four square miles.”[[13]](#footnote-13) Further, when a mobile app is being used, there is essentially no limit to how often it can record a cell phone’s location.[[14]](#footnote-14) Apps can even track location when a phone is not in use.[[15]](#footnote-15) One database of MALI contained 14,000 location records for a single individual in a day.[[16]](#footnote-16)

Despite the deeply revealing nature of MALI, the government claims that MALI does not violate individual privacy because personal identifiers are removed from the data.[[17]](#footnote-17) That contention is fundamentally flawed. Removing personal identifiers from data gives the illusion of privacy. However, the process ignores how data can be reidentified by linking it to outside information.[[18]](#footnote-18) For example, the government can identify a cellphone owner based on the home address where the phone is located each night.[[19]](#footnote-19) As little as four points of location data are sufficient to uniquely identify 95% of individuals.[[20]](#footnote-20) Considering that MALI databases contain dozens or thousands of data points per person per day, it is clear that MALI can be reidentified. Given the retrospective and deeply revealing nature of the information, individuals have a reasonable expectation of privacy in their physical movements as captured by MALI.

**The Third-Party Doctrine Does Not Extend to MALI**

Additionally, the Court “decline[d] to extend” the third-party doctrine to CSLI.[[21]](#footnote-21) The third-party doctrine holds that there is no reasonable expectation of privacy, and thus no Fourth Amendment protection, over information voluntarily given to a third party.[[22]](#footnote-22) The Court identified two rationales for the third-party doctrine—(1) “a reduced expectation of privacy in information knowingly shared with another” and (2) “voluntary exposure”—and held that neither rationale applied to CSLI.[[23]](#footnote-23) The justifications do not apply to MALI either. Considering the first rationale, the majority in *Carpenter* held that there is no reduced expectation of privacy in deeply revealing location information knowingly shared with a third party.[[24]](#footnote-24) Such pervasive tracking “implicates privacy concerns far beyond those considered” when the third-party doctrine was developed.[[25]](#footnote-25) Since MALI is a form of profoundly revealing location information, it is not subject to a reduced expectation of privacy.

For the second rationale, the Court offered two reasons why CSLI is not truly shared voluntarily. First, the Court reasoned that “cell phones and the services they provide . . . [are] indispensable to participation in modern society.”[[26]](#footnote-26) This reason applies directly to MALI. Mobile apps are the primary “service” provided by cell phones—the average smartphone user spends 90% of the total time on their phone using mobile apps.[[27]](#footnote-27) Second, the Court pointed to the “inescapable and automatic nature” that CSLI is collected.[[28]](#footnote-28) Likewise, the proliferation of location trackers in mobile apps makes it extremely difficult to avoid the creation of MALI. Over 55% of the top 160,000 Android apps contain location trackers.[[29]](#footnote-29) A study that investigated 110 iOS apps found that 47% shared geolocation information with third parties.[[30]](#footnote-30) And it is hard to know which apps to avoid since terms of service often omit or obfuscate whether an app collects and sells your location information.[[31]](#footnote-31) To prevent MALI from being created, cell phone users have to disable location services for essentially all mobile apps. Doing so removes a significant part of a cell phone’s usefulness and value. In *Carpenter*, the Court did not demand that people turn their cell phone off whenever they did not want to be tracked. Similarly, the onus should not fall on the public to disable location services to avoid intrusion from law enforcement.

**Conclusion**

Mobile application location information offers law enforcement unprecedented surveillance power of the type the Fourth Amendment was designed to protect against. If law enforcement agencies want to purchase MALI, the Fourth Amendment demands they get a warrant first.

1. Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. Times (Dec. 20, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html. [↑](#footnote-ref-1)
2. Jennifer Valentino-DeVries et al., *Your Apps Know Where You Were Last Night, and They’re Not Keeping It Secret*, N.Y. Times (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html?mod=article\_inline. [↑](#footnote-ref-2)
3. Thompson & Warzel, *supra* note 1. [↑](#footnote-ref-3)
4. 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; Byron Tau & Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, Wall Street J. (Feb. 7, 2020, 7:30 AM), https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600. [↑](#footnote-ref-4)
5. Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018). [↑](#footnote-ref-5)
6. The holding was limited to police access of seven or more days of CSLI. *Id.* at 2217, 2217 n.3. [↑](#footnote-ref-6)
7. *Id.* at 2223. [↑](#footnote-ref-7)
8. *See* Paul Ohm, *The Many Revolutions of Carpenter*, 32 Harv. J.L. & Tech. 357, 359, 364 (2019). [↑](#footnote-ref-8)
9. *Carpenter*, 138 S. Ct. at 2217 (citing United States v. Jones, 565 U.S. 400, 415, 430 (2012) (Sotomayor, J., concurring) (Alito, J., concurring)). The majority focused on the nature of historical cell phone tracking data in general, rather than the way CSLI was generated or collected by the government. Ohm, *supra* note 9, at 363. As a result, the commercial availability of the location information is not a factor in the reasonable expectation of privacy analysis. *See Carpenter*, 138 S. Ct. at 2217 (“Although such records are generated for commercial purposes, that distinction does not negate Carpenter’s anticipation of privacy in his physical location.”). [↑](#footnote-ref-9)
10. *See Carpenter*, 138 S. Ct. at 2217–18, 2223. [↑](#footnote-ref-10)
11. *See* *id*. at 2218 (describing the retrospective nature of historical location information). [↑](#footnote-ref-11)
12. *GPS Accuracy*, GPS.gov, https://www.gps.gov/systems/gps/performance/accuracy/; Ahmed Makki et al., *Survey of WiFi Positioning Using Time-Based Techniques*, 88 Computer Networks 218, 219 (2015). [↑](#footnote-ref-12)
13. *Carpenter*, 138 S. Ct. at 2218. [↑](#footnote-ref-13)
14. *See* Jennifer Valentino-DeVries et al., *supra* note 2 (investigating an app that tracked a user’s location “as often as every two seconds”). [↑](#footnote-ref-14)
15. *See, e.g.*, *Access Location in the Background*, Android Developers, https://developer.android.com/training/location/background. [↑](#footnote-ref-15)
16. Jennifer Valentino-DeVries et al., *supra* note 2. [↑](#footnote-ref-16)
17. Tau & Hackman, *supra* note 4. [↑](#footnote-ref-17)
18. Helen Nissenbaum, *The Meaning of Anonymity in an Information Age*, 15 Info. Soc’y 141, 142 (1999); *see generally* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701 (2010). [↑](#footnote-ref-18)
19. *See* Valentino-DeVries et al., *supra* note 2. [↑](#footnote-ref-19)
20. Yves-Alexandre de Montjoye et al., *Unique in the Crowd: The Privacy Bounds of Human Mobility*, Nature (Mar. 25, 2013), http://www.nature.com/articles/srep01376. [↑](#footnote-ref-20)
21. *Carpenter*, 138 S. Ct. at 2220. [↑](#footnote-ref-21)
22. *Id.* at 2216–19; Smith v. Maryland, 442 U.S. 735, 743–44 (1979). [↑](#footnote-ref-22)
23. *Carpenter*, 138 S. Ct. at 2219–20. [↑](#footnote-ref-23)
24. *Id.* at 2219. [↑](#footnote-ref-24)
25. *Id.* at 2220. [↑](#footnote-ref-25)
26. *Id.* (quoting Riley v. California, 573 U.S. 373, 385 (2014)). [↑](#footnote-ref-26)
27. Yoram Wurmser, *US Time Spent with Mobile 2019*, eMarketer (May 30, 2019), https://www.emarketer.com/content/us-time-spent-with-mobile-2019. [↑](#footnote-ref-27)
28. *Carpenter*, 138 S. Ct. at 2223. [↑](#footnote-ref-28)
29. SafeDK, *Mobile SDK Data Trends in the Android Market* (Mar. 2018), *available at* http://mobile-sdk-data-trends.safedk.com/full-report-Mar-2018. [↑](#footnote-ref-29)
30. Jinyan Zang et al., *Who Knows What About Me? A Survey of Behind the Scenes Personal Data Sharing to Third Parties by Mobile Apps*, Tech. Sci. (Oct. 30, 2015), https://techscience.org/a/2015103001/. [↑](#footnote-ref-30)
31. Nicole Nguyen, *A Lot Of Apps Sell Your Data. Here's What You Can Do About It.*, BuzzFeed News (May 1, 2018, 11:19 AM), https://www.buzzfeednews.com/article/nicolenguyen/how-apps-take-your-data-and-sell-it-without-you-even. [↑](#footnote-ref-31)