Saint Louis University School of Law
Scholarship Commons

SLU Law Journal Online

4-25-2019

Evolving Societal Norms and the Fourth Amendment: Government Tracking of Cellphone Locations in an Era of Commercial Tracking

Paul Tahan

Follow this and additional works at: https://scholarship.law.slu.edu/lawjournalonline

 Part of the Law Commons

Evolving Societal Norms and the Fourth Amendment: Government Tracking of Cellphone Locations in an Era of Commercial Tracking

By Paul Tahan*

The precise locations of 200 million smartphones in the United States were commercially tracked in 2017.[1] As many as seventy-five companies collected the location of these smartphones.[2] In some instances, businesses gathered the precise location, accurate to within a few yards, of individual smartphones as often as 14,000 times per day.[3] Some used the information to personalize ads.[4] Others sent this hyper-localized private information unsolicited to partner businesses, some of whom did not want to receive it.[5] Although the location data was anonymized, in many instances it was specific enough for individual identities to be discerned.[6] For example, one set of data reviewed by the New York Times followed a smartphone arriving at the site of a homicide before going to a nearby hospital.[7] The phone returned throughout the night to the local police station.[8] Another set of data, associated with a teacher named Lisa, was specific enough for journalists to determine Lisa's full name and interview her for the article.[9]

The ease with which companies can obtain precise smartphone location data raises compelling questions about the reasonableness of a person's expectation of privacy in their location. This is an important issue because the Government may subpoena a smartphone's historical GPS information from a third party such as an advertiser without a warrant if a person no longer has a reasonable expectation of privacy in such.[10] Thus we come to

* J.D. Candidate, 2020, Saint Louis University School of Law

[1] 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?module=inline.

[2] *Id.*

[3] *Id.*

[4] *Id.*

[5] *Id.* (emphasis added).

[6] Valentino-DeVries, *supra* note 1.

[7] *Id.*

[8] *Id.*

[9] *Id.*

[10] *See* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

the critical question: at what point is a smartphone's GPS location so public as to render tracking of it by the Government reasonable and not violative of the Fourth Amendment?

The reasonableness of a search under the Fourth Amendment is closely tied to the existence, or lack thereof, of an expectation of privacy to the area sought to be searched "that society is prepared to recognize as 'reasonable.'"[11] A person travelling in an automobile on public roads, for example, has no reasonable expectation of privacy in their movements because, by so doing, they voluntarily convey that they are traveling over particular roads in a particular direction.[12] Combined with strong jurisprudence critical of an individual's expectation of privacy in information voluntarily turned over to third parties,[13] the Court may conclude that a person no longer has a reasonable expectation of privacy in their GPS-enabled smartphone's historical location data.

For the moment, the Supreme Court has disposed of a similar issue. In Carpenter v. United States the Court found that, given the unique nature of cellphone 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."[14] While this is reassuring to those of us attached to our smartphones, your author is not convinced that it is impenetrable jurisprudence. The Carpenter dissent posited that "[c]ell-site records… are no different from the many kinds of business records the Government has a lawful right to obtain by compulsory process."[15] In an era where Apple's Find My Friends allows users to permit friends to track the location of their smartphone, and where seventy-five companies have access to the location information of 200 million smartphones, location information is arguably

[11] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).
[12] United States v. Knotts, 460 U.S. 276, 281–82 (1983). *Knotts* involved law enforcement's use of an electronic "beeper" tracking device. *Id.* at 285. The Court found that the use of such did not invade the defendant's reasonable expectation of privacy, and thus did not constitute a search. *Id.*
[13] *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (no expectation of privacy in dialed phone numbers because the information is voluntarily conveyed to the phone company); United States v. Miller, 425 U.S. 435, 443 (1976) (no expectation of privacy in bank records).
[14] 138 S. Ct. at 2206, 2217.
[15] *Id.* at 2224 (Kennedy, J., dissenting).

more public than other business records, such as bank records, that the Government may obtain by subpoena.

There is additional cause for concern: Carpenter specifically protected "cell-site location information" ("CSLI") which is different from GPS information.[16] CSLI is available to the individual's carrier whether the consumer likes it or not; it is a record of each cell tower the phone connects to.[17] GPS tracking, conversely, is "opted into." On an iPhone, for example, users can turn off GPS entirely or limit which apps can see their location.[18] This is an important difference from Carpenter: the Court emphasized CSLI is not "shared" as one normally understands the term because (1) carrying a cellphone is indispensable to participation in modern society and (2) a cellphone logs CSLI without any affirmative act on the part of the user beyond powering it up.[19] GPS data, on the other hand, is (1) not necessarily indispensable to participation in modern society and (2) requires the user to affirmatively opt-in. Part (2) also distinguishes smartphone GPS information from traditional GPS trackers placed by law enforcement: not only is the user aware they are being tracked, but they consent to their smartphone's ability to do so.[20]

The Carpenter Court, as it tends to do in contentious cases, stressed that its holding was "a narrow one."[21] To be extremely precise, the Court held that "accessing seven days of CSLI constitutes a Fourth Amendment search."[22] The Court expressly declined to consider "whether there is a limited period

[16] *Id.* at 2217.

[17] *Id.* at 2211.

[18] *Turn Location Services and GPS on or off on your iPhone, iPad, or iPod touch*, Apple Inc. (Sept. 20, 2017), https://support.apple.com/en-us/HT207092.

[19] 138 S. Ct. at 2220.

[20] The Supreme Court has traditionally required a warrant for law enforcement to install GPS tracking devices. United States v. Jones, 565 U.S. 400, 404–05 (2012). In *Jones* the Supreme Court found that warrantless installation of a GPS device on a target's vehicle, and use of that device to monitor the vehicle's movements, constituted a "search." *Id.* at 404. The Court emphasized, however, that its holding was based upon the physical intrusion that accompanied placing of the monitor. *Id.* at 404–05. In contrast, tracking of an individual's cellphone via GPS or reviewing historical location records requires no physical intrusion and cannot be accomplished unless the individual has consented to outside companies tracking their location.

[21] 138 S. Ct. at 2220.

[22] *Id.* at 2217 n.3.

for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny."[23] In addition, although the Court emphasized that CSLI is collected without consumer consent,[24] it did not address treatment of similar information that is collected with consumer consent, such as historical GPS location information. In fact, the Court expressly declined to address the issue, stating its opinion did not "address other business records that might incidentally reveal location information."[25]

There is a ray of hope for the privacy-conscious among us: the Carpenter majority emphasized the invasiveness of cellphone tracking, the intimacy of the information it reveals, and the ease and low cost compared to traditional investigative tools,[26] concerns that would certainly apply to GPS information. The Court also implied that the greater locational accuracy enabled by GPS tracking of an individual's movements might be even more invasive.[27] Combined with recognition of a person's reasonable expectation of privacy in the whole of their physical movements tracked by information held by a third party,[28] a cellphone's historical GPS data seems to be protected from warrantless search. For now.

Edited by Carter Gage

[23] *Id.*

[24] See, e.g., *id.* at 2220 ("… a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up.").

[25] *Id.*

[26] *Carpenter*, 138 S. Ct. at 2217–18.

[27] See *id.* at 2218 (stating that it did not matter that CSLI was less precise than GPS information).

[28] *Id.* at 2219.