# IS COVID-19 DEADLY TO THE FOURTH AMENDMENT?

**ALBERT FOX CAHN, ESQ. &**
**ZACHARY SILVER**

**JULY 15, 2020**

STOP
SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

@ the Urban Justice Center:
40 Rector Street, 9th Floor
New York, New York 10006

www.StopSpying.org | (646) 602-5600

# Is COVID-19 Deadly to the Fourth Amendment?

By Albert Fox Cahn, Esp. and Zachary Silver

Our location history reveals much about who we are, showing what businesses we patronize, what doctors we see, and if we engage in political protest. It reveals who we cross paths with, both intentionally and unintentionally, and when we do so. It reveals our "familial, political, professional, religious, and sexual associations,"[1] and when we choose to engage in such associations.

So our alarm bells of course went off when the Wall Street Journal reported in late March that the mobile advertising industry is providing to governments at all levels the GPS location data it collects from millions of cell phones to aid their studies of the COVID-19's spread in major cities[2]. Since most Americans have a cellphone within a few feet at all times,[3] our phones' locations often are our locations. And those same alarm bells rang louder than an air-raid siren at the revelation that this location data may also be used by law enforcement.

The Fourth Amendment to the U.S. Constitution generally requires the government to obtain a warrant before conducting a search. For much of the Twentieth Century, law enforcement circumvented warrant requirements by invoking the "Third-Party Doctrine," which allows warrantless information collection from banks and other companies. But, in 2018, in *Carpenter v. United* States, the Supreme Court limited the Third-Party Doctrine's reach, holding a warrant was required to obtain a week or more of cell phone tower location data (so-called "CSLI") without a warrant[4]. Such data could create a comprehensive record of a person's movement,[5] which is tantamount to "attach[ing] an ankle monitor to the phone's user."[6]

By its terms, *Carpenter* was limited to a single tracking method: CSLI.[7] But the Constitution's framers did not limit the Fourth Amendment's protection to a single technology, let alone one unimagined at the time. Rather, they spoke to general principles to be applied to all forms of privacy invasion. The same pragmatic factors that guided the Supreme Court's decision in

---

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

2 Byron Tau, *Government Tracking How People Move Around in Coronavirus Pandemic*, Wall Street J. (Mar. 28, 2020), https://www.wsj.com/articles/government-tracking-how-people-move-around-in-coronavirus-pandemic-11585393202.

3 *Riley v. California*, 573 U.S. 373, 395 (2014) (citing Harris Interactive, *2013 Mobile Consumer Habits Study* (2013)).

4 *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

5 *Id.* at 2216–20.

6 *Id.* at 2218.

7 *Id.* at 2220.

*Carpenter* also require protections against other forms of location monitoring such as GPS cell phone tracking. GPS cell phone tracking precisely—and more accurately—mimics the dangers that alarmed the Court.[8]

So long as location data is collected, the privacy dangers are impossible to avoid. Many who claim to "anonymize" location data later learn true anonymization is nearly impossible.[9] Even aggregated data can provide law enforcement a window into "the privacies of life."[10]

If government agencies using mass surveillance to track COVID-19 realize that they are well beyond the limits of the Third-Party Doctrine, they may attempt to invoke the "Special Needs Exception," which permits warrantless searches when "special needs, beyond the normal need for law enforcement, make the warrant and probable cause requirement impracticable."[11] While the Special Needs Exception has not yet been evaluated in this context, it's unclear why the outcome should be any more permissive. No matter what doctrine is cited to justify new location tracking, the pragmatic considerations that undergird *Carpenter* remain.

Beyond the Fourth Amendment, federal officials also face statutory obstacles. The Privacy Act of 1974 prohibits federal employees from disclosing individuals' information except under narrowly defined circumstances.[12] Since COVID-19 tracking data is easily identifiable and reveals sensitive details, it should be subject to similar restrictions.[13] At a minimum, any cell phone data collected to track the virus's spread must be restricted to access by policymakers; it is completely indefensible if that data is provided to law enforcement for social distancing enforcement, let alone general criminal investigations. Furthermore, while any mass collection of location data is constitutionally suspect, such practices are particularly egregious if the data is retained longer than the current crisis. Currently, it is unclear how long agencies will retain this data and if their surveillance records will outlive the COVID-19 pandemic.

When rights are curtailed to address crises, those temporary exceptions often become the new default rule. From Red Scare-era loyalty oaths, to the growth of Cold War-era Presidential war powers, to the post-9/11 passage of the USA PATRIOT Act, many of the emergency measures of the past live with us to this very day. COVID-19 is the gravest health crisis in generations, and we must do more to safeguard American lives. But creating vast surveillance measures will do little to protect our families, while putting the rights of millions at risk.

---

8 *Id.* at 2217–18. Indeed, the Carpenter majority directly analogized CSLI tracking to GPS.

9 Alex Hern, *'Anonymized' Data Can Never Be Totally Anonymous, Study Says*, Guardian (July 23, 2019, 11:40 AM), https://www.theguardian.com/technology/2019/jul/23/anonymised-data-never-be-anonymous-enough-study-finds; *see also, e.g.*, Arvind Narayanan & Vitaly Shmatikov, *Robust De-anonymization of Large Datasets (How to Break Anonymity of the Netflix Prize Dataset)* (2008), https://arxiv.org/pdf/cs/0610105.pdf

10 *Carpenter*, 138 S. Ct. at 2217 (quoting *Riley*, 573 U.S. at 403).

11 New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) (Blackmun, J., concurring in the judgment).

12 5 U.S.C. § 552a(b)(3).

13 *Cf. id.* § 552a(e)(7) (prohibiting agencies from maintaining records "describing how any individual exercises rights guaranteed by the First Amendment" except in limited circumstances).

*Cahn (@FoxCahn) is the founder and executive director of the Surveillance Technology Oversight Project (S.T.O.P.) at the Urban Justice Center, a New York-based civil rights and privacy group and a fellow at the Engelberg Center for Innovation Law & Policy at N.Y.U. School of Law.*

*Silver is a civil rights intern at the the Surveillance Technology Oversight Project (S.T.O.P.) at the Urban Justice Center and a third-year law student at the Benjamin N. Cardozo School of Law.*

Surveillance Technology
Oversight Project, Inc.
40 Rector Street
9th Floor
New York, NY 10006
www.STOPSpying.org

STOP
SURVEILLANCE TECHNOLOGY
OVERSIGHT PROJECT