Notes on Presentation to the San Diego Privacy Advisory Board
31 May 2023

I am glad for the opportunity to discuss these issues with you. I have been teaching and writing about the Fourth Amendment for almost forty years. My page is here: https://www.sandiego.edu/law/centers/ilp/directory/biography.php?profile_id=2793

To be clear, I am appearing as an academic. I'm not your lawyer and you're not my clients. You face an important public issue and I'm here to help you with that insofar as I am able to do so.

So here's a *very* short tour of the legal landscape.

I. Relevant Fourth Amendment Law—*Jones* and *Carpenter*

(1) United States v. Jones, 565 U.S. 400 (2012)

Agents attached a tracking device on the undercarriage of Jones's car, monitoring the vehicle's location with GPS accuracy for more than four weeks.

The majority, per Scalia, J., relied on a trespass test:

* * *

The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a "search" within the meaning of the Fourth Amendment when it was adopted

* * *

The Court was unanimous, but four justices joined separate concurring opinions adopting the "mosaic theory." The mosaic theory recognizes a the aggregation of discrete observations, none itself a violation of the Fourth Amendment, as an intrusion on reasonable expectations of privacy and therefore a "search" presumptively requiring a traditional warrant.

Justice Alito in *Jones* said:

* * *

relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. See Knotts, 460 U. S., at 281–282. But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period. In this case, for four weeks, law enforcement agents tracked every movement that respondent made in the vehicle he was driving. We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark. .

* * *

Justices Ginsburg, Breyer and Kagan joined the Alito opinion.

Justice Sotomayor filed a separate concurring opinion. Justice Sotomayor said:

* * *

in cases involving even short-term monitoring, some unique attributes of GPS surveillance relevant to the *Katz* analysis will require particular attention. GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.
See, *e.g., People* v. *Weaver*, 12 N.Y.3d 433, 441–442, 909 N.E.2d 1195, 1199 (2009) ("Disclosed in [GPS] data . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on").

* * *

(2) Carpenter v. United States, 585 U.S. ___ (2018)

Agents obtained Carpenter's historical cell site location data from Verizon, by using an administrative subpoena authorized by statute, rather than by obtaining a traditional search warrant.

Chief Justice Roberts wrote the majority opinion, joined by Justice Ginsburg, Breyer, Kagan and Sotomayor. Chief Justice Roberts said:

* * *

we need not decide whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be. It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search.

* * *

The majority opinion, however, also said:

* * *

Our decision today is a narrow one. We do not express a view on matters not before us: 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). We do not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras.

* * *

Justice Thomas, Justice Kennedy, Justice Alito and Justice Gorsuch each filed dissenting opinions.

Since *Carpenter* Justices Kennedy, Ginsburg and Breyer have left the Court, and Justices Kavanaugh, Barret and Jackson have joined it. I do not expect the Court to either reconsider *Carpenter,* but how far beyond *Carpenter* any current majority is willing to go remains an open question.

II. Developments since *Carpenter*

(1) Aerial Surveillance—Leaders of a Beautiful Struggle v. Baltimore Police Department, 4 F.4th 330 (4th Cir. 2022) (en banc).

The Baltimore Police Department contracted with Persistent Surveillance Systems, a private firm, to operate planes equipped with digital cameras. The system's capabilities were summarized as follows:

* * *

The cameras capture roughly 32 square miles per image per second. The planes fly at least 40 hours a week, obtaining an estimated twelve hours of coverage of around 90% of the city each day, weather permitting. The PSA limits collection to daylight hours and limits the photographic resolution to one pixel per person or vehicle, though neither restriction is required by the technology. In other words, any single AIR image—captured once per second—includes around 32 square miles of Baltimore and can be magnified to a point where people and cars are individually visible, but only as blurred dots or blobs.

* * *

The majority concluded:

* * *

because the AIR program enables police to deduce from the whole of individuals' movements, we hold that accessing its data is a search, and its warrantless operation violates the Fourth Amendment. Therefore, we reverse and remand.

* * *

But the court was closely divided; eight judges were in the majority, but six filed dissenting opinions.

(2) Pole Cameras—United States v. Moore-Bush, 36 F.4th 320 (1st Cir. 2022) (en banc) (per curiam)

Agents installed a pole camera with a view of the suspect's home, and collected video for eight months. **The judges split three to three on whether or not this constituted a search.** The defendant and the ACLU sought review from the Supreme Court, but SCOTUS denied the petition for certiorari in May 2023.

(3) Geofence Warrants for Google Location Data

These are sometimes referred to as "reverse warrants" because law enforcement does not have an identified suspect when the data are sought. The warrants initially require Google to share location data from the immediate are of a reported crime, without identifying information about who owns the various devices that will show up in the data. After receiving the anonymized location data, the agents compare the anonymized data with other evidence, and then apply for a second warrant disclosing the consumer identity associated with the suspected devices. The government has not conceded that a warrant is required, but has sought such

warrants, generally successfully so long as the requested data is particularly defined in terms of space and time. *See, e.g.,* Matter of the Search of Information that is Stored at Premises Controlled by Google, 2023 WL 2236493 (S.D. Tx.) (Feb. 14, 2023).

(4) Tower Dumps

A tower dump shares all the cell phones in contact with the tower(s) near in time to a reported crime. As with geofence warrants, the government has sought warrants for these tower dumps without conceding that warrants are required by the Fourth Amendment. The courts generally have upheld these warrants so long as there were reasons to believe that the data could help solve the crime (as when a single suspect is thought to have committed two similar offenses at different places) and the disclosure is limited in space and time. *See, e.g.,* United States v. James, 3 F.4th 1102 (8th Cir. 2021).

(5) The California Electronic Communications Privacy Act

The CECPA, Ca. Code, Title 12, §§1546-1546.5, was signed into law in 2015. Under the Act, California law enforcement officers need a warrant, consent, or an emergency to obtain electronic records, including the envelope information for emails and texts, browsing histories, and consumer transactions. The Act, however, does not apply to data collected by law enforcement officers.

II. The Smart Street Lights Contract

Query, does the tech empower investigators to trace a particular plate number across time, or only to recover plates from a particular date/time point? If the former, the case looks very much like the geofence and tower dump cases. Federal agents are seeking, successfully, search warrants in these cases. Are those warrants constitutionally required or not? The issue was left open in *Carpenter* and is still open.

But if the technology permits tracing the location of individual vehicles over long periods of time, it looks much like *Carpenter* itself.

III. Comparing the Contract with the *Carpenter* Case

(1) Pertinent similarities

Assuming vehicle location data is as private as cell phone location data (*Jones* would suggest that much), the policy enables law enforcement officers to access vehicle location data without a search warrant.

(2) Pertinent differences

There is no voluntary transfer of the location data from the individual to a third party; the contractor works for the police.

To access the location data, the police begin with a location, not with a suspect.

The amount of location data accessed might be smaller than the 7 days deemed to trigger the warrant requirement in *Carpenter.*

The data are "purged" after 15 days.

IV. Immediate Liability Risks are Minimal

Even when a court concludes that police should have applied for a search warrant, the qualified immunity doctrine protects the officers from civil liability unless a warrant was clearly required by existing law at the time of the search. A similar doctrine, the "good faith exception to the exclusionary rule", allows prosecutors to use evidence obtained by unconstitutional searches so long as the officers reasonably relied on established law at the time of the search. In both *Carpenter* and *Moore-Bush* the evidence was ultimately held admissible. *Beautiful Struggle* was a civil action for an injunction prohibiting future aerial surveillance.

V. The emerging Fourth Amendment argument

Is it "reasonable" *to collect* pervasive surveillance data *ex ante* WITHOUT regulating access by the warrant process *ex post*? This was not addressed in *Carpenter* because Verizon collected the data. When police collect the data themselves, it can be argued that there is no voluntary sharing of the data by consumers, as there was in *Carpenter*. On the other hand, how can there be a reasonable expectation of privacy in data the police previously collected in public space?

VI. Common Sense Questions (many very bad ideas are perfectly constitutional)

(1) How will the police proceed if they can't use the surveillance technology?

The biggest problem prosecuting the most serious crimes is a shortage of credible witnesses. Often those who know who committed the crime are loyal to the suspect or afraid of the suspect, or both. Eyewitness testimony is notoriously unreliable. Compared to familiar methods of investigation, these surveillance technologies offer important advantages. They offer the same advantages in holding police accountable for alleged misconduct.

(2) Why the 2 week purge? Consider:

(a) The FBI and the NSA want location data on a suspected terrorist leader known to have been in San Diego three weeks ago. "Sorry, we don't have it any more"?

(b) A defendant accused of a robbery eight months ago claims alibi, saying the suspect was at a roadhouse underneath a smart street light at the time of the robbery. Same question--"Sorry, we don't have it any more"?

(c) A civil right plaintiff sues a police officer for excessive force during an arrest under a smart street light a year ago. Both parties seek discovery of the video. Same question--"Sorry, we don't have it any more"?

(3) Why not require search warrants to access the data?

As measured by "hit rates," warrant searches have a very good record, with hit rates over 50% and in many studies much higher. This is due in at least substantial part to the time cost of the warrant process; the officers have other things to do, and organizing the information, writing up the application, having it reviewed by a prosecutor, and then waiting for the judge to decide, takes time. But that's the point; if the police practice at issue touches especially important privacy concerns, it *ought to be* subject to a costly pre-screening process.

In the model case of a reported crime in a surveillance zone, probable cause isn't a problem. In the deep investigations, pole camera evidence often supports applications for warrants; moving the warrant requirement back to the data collection stage might impede those investigations. But unless the tech permits law enforcement to monitor individual plates across time, it can't help much with deep investigations. If the tech does permit accessing cross-time location data, it runs into *Carpenter*