MEMORANDUM

TO: Chicago CLE Attendees
FROM: Catherine Crump, Clinical Professor, Berkeley Law School, ccrump@law.berkeley.edu
DATE: May 15, 2022
RE: Key Lower Court Decisions Applying *Carpenter v. United States*

Overview

This document provides an overview of how lower courts have applied the Supreme Court's landmark location tracking case, *Carpenter v. United States*, 585 U.S. ___, 138 S. Ct. 2206 (2018), to other digital searches. Below I identify various government electronic surveillance techniques and flag cases where courts have addressed whether the technique at issue is a search in light of *Carpenter*. I have tried to identify the major cases, but this document is not comprehensive, and focuses primarily on federal circuit court and state Supreme Court decisions that decide the issue on federal Fourth Amendment grounds.

I plan to update this document occasionally. The most recent version will be viewable at https://n2t.net/ark:/85779/j4ww8w

Historical Cell Site Location Information

One question *Carpenter* left open is for what duration of time law enforcement must collect location data for it to have conducted a Fourth Amendment search. In *Commonwealth v. Wilkerson*, the Massachusetts Supreme Judicial Court concluded that, "[c]ollecting more than six hours of CSLI data invades a defendant's reasonable expectation of privacy, and, therefore, under the Fourth Amendment to the United States Constitution and art. 14 of the Massachusetts Declaration of Rights, requires a warrant supported by a showing of probable cause." *Commonwealth v. Wilkerson*, 486 Mass. 159, 165–66, 156 N.E.3d 754, 766 (2020). This appears to be the shortest duration for which courts have held a warrant is required.

Real-time Cell Site Location Information

The Supreme Court in *Carpenter* expressly reserved decision on whether law enforcement agents must obtain a warrant to track a cell phone in real time. A few state supreme courts have concluded that a warrant is required. *See Commonwealth v. Pacheco*, 263 A.3d 626, 640 (Pa. 2021) ("*Carpenter's* warrant requirement for the collection of historical CSLI, which provides 'a comprehensive chronicle of the user's past movements, applies with equal force to the collection of real-time CSLI in the instant case," which involved 108 days of real-time CSLI); *State v. Muhammad*, 451 P.3d 1060, 1073 (Wash. 2019) (single ping of real-time CSLI requires a warrant); *see also*

Tracey v. State, 152 So. 3d 504 (Fla. 2014) (pre-*Carpenter* case requiring a warrant for real-time cell phone tracking before *Carpenter*).

Pole Camera Cases

Sometimes law enforcement agents conduct long-term surveillance of a home by installing a hidden video camera on a utility pole (a "pole camera"). One question is whether this long-term surveillance is a search. There is a split in the circuit and state supreme court authority on this question.

Some courts have held that even long-duration surveillance through a pole camera is not a search. *See United States v. Tuggle*, 4 F.4th 505, 511 (7th Cir. 2021) (18 months of pole camera surveillance did not violate the Fourth Amendment because "the governmentls use of a technology in public use, while occupying a place it was lawfully entitled to be, to observe plainly visible happenings, did not run afoul of the Fourth Amendment"); *United States v. Moore-Bush*, 963 F.3d 29, 31 (1st Cir 2020) (pole cameras are a "conventional" surveillance technique that, under *Carpenter*, does not require a warrant) (rehearing en banc granted); *United States v. Houston*, 813 F.3d 282 (6th Cir. 2016) (no Fourth Amendment search when police observed home through pole camera for ten weeks).

But other courts have held that long-term pole camera surveillance is a search. *See United States v. Cuevas-Sanchez*, 821 F.2d 248, 251 (5th Cir. 1987) (holding long-term use of pole camera placed to overlook suspect's 10-foot high fence and record activity in his back yard is a search but concluding that district court's advance permission was adequate); *People v. Tafoya*, 494 P.3d 613, 623 (Colo. 2021) (use of a pole camera to surveil the fenced-in curtilage of a defendant's house for three months violated the Fourth Amendment); *State v. Jones*, 903 N.W.2d 101, 113 (S.D. 2017) (holding, pre-*Carpenter*, that deploying a pole camera to record a residence for nearly two months is a search).

Vehicle location data

In *United States v. Diggs*, the United States District Court concluded that collection of a month's worth of historical vehicle location data was a search under *Carpenter*. *United States v. Diggs*, 385 F. Supp. 3d 648, 652 (N.D. Ill. 2019) ("The GPS data at issue here fits squarely within the scope of the reasonable expectation of privacy identified by the Jones concurrences and reaffirmed in Carpenter.").

In contrast, the United States District Court for the Middle District of Alabama concluded that real-time GPS tracking of a borrowed truck was not a search where the owner consented to installation of the GPS device, the tracking was "not an extended duration," and, in the court's view, GPS data is less invasive than CSLI. *United States v. Howard*, 426 F. Supp. 3d 1247, 1256–57 (M.D. Ala. 2019).

Tower Dumps

In some cases, law enforcement agents seek to identify all cell phones that utilized a particular cell phone tower during a particular time frame (a "tower dump").

In *Commonwealth v. Perry*, 489 Mass. 436, 184 N.E.3d 745, 762–63 (2022), the Supreme Judicial Court held, on *state constitutional grounds*, that law enforcement must obtain a warrant for seven tower dumps. It wrote, that "analyzing small increments of CSLI over the course of several days" violates a defendant's reasonable expectation of privacy. 184 N.E.3d at 763. But the court rejected the argument that tower dumps are per se unconstitutional because they are inadequately particularized. 184 N.E.3d at 745.

In *United States v. Walke*r, the United States District Court for the Eastern District of North Carolina concluded that a tower dump was not a search under *Carpenter*. 2020 WL 4065980, at *1, *8 (E.D.N.C. July 20, 2020) (no search because tower dumps only "capture CLSI for a particular place at a limited time" and are 'more akin to 'conventional surveillance techniques'").

Geofence Warrants

"Geofence" warrants, typically served on Google, seek location data for every user within a particular geographical location over a particular period of time. The one federal court that has weighed in on the Fourth Amendment question in the context of a suppression motion is *United States v. Chatrie*, No. 3:19-cr-130, 2022 WL 628905 (E.D. Va. Mar. 3, 2022).[1] The court held that the geofence warrant, in this case covering a circular area with a 150-meter radius, "plainly violates" the Fourth Amendment, because it lacked particularized probable cause as to the targets within its boundaries. *Id.* at * 1. But it upheld the search under the good faith exception to the exclusionary rule. *Id.*

[1] A number of other federal courts have analyzed geofence warrants at the point of issuance. *See, e.g.*, *In re Search of Information That is Stored at the Premises Controlled by Google LLC*, No. 2l-sc-3217, 2021 WL 6196136 (D.D.C. Dec. 30, 2021); *In re Search of Information that is Stored at the Premises Controlled by Google, LLC*, 542 F. Supp. 3d 1153 (D. Kan. 2021); *In re Search Warrant Application/or Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d 345 (N.D. Ill. 2020); *In re Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730 (N.D. Ill. 2020); *In re Search of Information Stored at Premises Controlled by Google*, No. 20M297, 2020 WL 5491763 (N.D. Ill. July 8, 2020).

Automatic License Plate Readers

Automatic license plate readers (ALPR) take a photo of every passing car, translating the license plate number into machine-readable text. The plate number can then be compared to "hot lists" of cars of interest, for example those registered to persons with outstanding arrest warrants. When ALPRs are spread throughout a city, the aggregate data can be used to track vehicles' locations over time.

In *Commonwealth v. McCarthy*, the Massachusetts Supreme Judicial Court concluded that use of four ALPRs to gather data over a ten-week period did not constitute a search. *Commonwealth v. McCarthy*, 484 Mass. 493, 142 N.E.3d 1090 (2022). Relying on *Carpenter*, the Court framed the question as, "whether ALPRs produce a detailed enough picture of an individual's movements so as to infringe upon a reasonable expectation that the Commonwealth will not electronically monitor that person's comings and goings in public over a sustained period of time." *Id.* at 505, 142 N.E.3d at 1193. The court held that the data at issue in the case did not cross this threshold, but that "with enough cameras in enough locations, the historic location data from an ALPR system in Massachusetts would invade a reasonable expectation of privacy and would constitute a search for constitutional purposes.") *Id.* at 506, 142 N.E.3d at 1104. *See also United States v. Yang*, 958 F.3d 851, 863 (2020) (Bea, J. concurring) ("I understand that ALPRs *may* in time present many of the same issues the Supreme Court highlighted in Carpenter. ALPRs can effortlessly, and automatically, create voluminous databases of vehicle location information.").

Aerial Surveillance

The City of Baltimore operated a unique surveillance operation, in which it flew manned planes over a 32-square mile area of Baltimore for 40 hours of week, recording the entirety of the daytime outdoor movements of anyone in the area and it stored that data for at least 45 days. *Leaders of a Beautiful Struggle v. Baltimore Police Dept.,* 2 F.4th 330, 334 (4th Cir. 2021) (en banc). The Fourth Circuit, ruling en banc, held that the case was squarely controlled by *Carpenter*, and that the "detailed, encyclopedic" information it gathered about the whole of people's movements triggered the Fourth Amendment's warrant requirement. *Id.* at431–42.

University Card Swipe Data

Many universities require their students to obtain key cards. Depending on how these cards are configured, they may be necessary to open the doors of various classrooms and residential buildings; to open a student's own dorm room; to check out library books; and to obtain meals at cafeterias and other on-campus eateries. Collectively this data can reveal much about a student's patterns of life. One open question is whether it constitutes a search when public universities access this information during disciplinary investigations.

In Gutterman v. Indiana University, Bloomington, 558 F.Supp.3d 720, 732–32 (S.D. Ind. 202) (appeal filed Sept. 24, 2021), a district court concluded that students a lacked reasonable expectation of privacy in card swipe data where agreement put them on notice that the university made use of data and retained ownership in the card, and where university made only a limited use of the data.

In a similar vein, *Commonwealth v. Dunkins*, 263 A.3d 247 (Pa 2021), involved in location data derived from a college student's phone's connections to campus wi-fi hot spots. The court similarly relied on the student's agreement to the terms of the student handbook to find that there was no Fourth Amendment violation.

Sources

Robert Fairbanks, *Masterpiece or Mess: The Mosaic Theory of the Fourth Amendment after Carpenter*, 26 Berkeley J. Crim. L. 71 (2021) (reviewing lower courts' treatment of the "mosaic theory" of the Fourth Amendment after *Carpenter*, and reviewing many post-*Carpenter* digital surveillance cases in the process).

Matthew Tokson, The Aftermath of Carpenter: An Empirical Study of Fourth Amendment Law, 2018-2021, 135 Harv. L. Rev. 1790 (2022) (provising a broad empirical analysis of how federal and state courts have applied *Carpenter*).

Additional help

The Berkeley Law Samuelson Clinic, which I direct, is available to consult on digital surveillance issues. Feel free to email me (ccrump@law.berkeley.edu).

The American Civil Liberties Union, Electronic Frontier Foundation, and the National Association of Criminal Defense Lawyers' Fourth Amendment Center have filed amicus briefs (and occasionally merits briefs) on many of these issues. Searching their websites will turn up useful materials, and they may also be willing to submit an amicus brief in support of your client or provide consultation.