Carpenter v. United States: What Happened, and Where Do We Go from Here

Federal Community Defender Office, EDPA
Fall Training Seminar for CJA Panel Attorneys
October 18–19, 2018

Nathan Freed Wessler
Staff Attorney, ACLU Speech, Privacy, and Technology Project
nwessler@aclu.org • (212) 519-7847

In *Carpenter v. United States*, the Supreme Court provided long-overdue guidance about the scope of the third-party doctrine in the digital age. That doctrine, which arose out of a pair of cases decided in the 1970s, was previously often understood to provide that a person necessarily loses his or her reasonable expectation of privacy in information they have shared with a third party. Whatever can be said about the wisdom of the third-party doctrine in the 1970s, it had come to stand as a major impediment to protection of Fourth Amendment rights in the digital age, when a great deal of our most sensitive information is stored not in our homes and filing cabinets, but by third-party companies on remote servers. In *Carpenter*, however, the Supreme Court declined to extend those 1970s cases to cover the pervasive and voluminous cell site location data held by cellular service providers, which can provided a detailed accounting of people's locations and movements over time. In doing so, the Court created space to challenge other forms of location surveillance, as well as warrantless access to other kinds of sensitive records held by third-party companies.

This session will address the underpinnings of the third-party doctrine, the holding of *Carpenter*, and the possible ramifications of the Supreme Court's decision in *Carpenter* for advocacy on behalf of criminal defendants.

I. Origins of the Third-Party Doctrine

A. Government informant cases: People assume the risk when confiding in others that those confidants may turn out to be police informants. *See Hoffa v. United States*, 385 U.S. 293 (1972).

B. *United States v. Miller*, 425 U.S. 435 (1976)

1. A person has no reasonable expectation of privacy in several months' worth of cancelled checks, deposit slips, account statements, and similar records held by their bank. Therefore, law enforcement agents can obtain those records via subpoena, without a search warrant.
2. "The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information

is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."

C. *Smith v. Maryland*, 442 U.S. 735 (1979)

1. A person has no reasonable expectation of privacy in the phone numbers they dial to place a call, and thus the government can obtain those numbers from the phone company without a warrant.
2. "Telephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes. Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret."
3. "[E]ven if petitioner did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not 'one that society is prepared to recognize as "reasonable."' *Katz v. United States*, 389 U.S., at 361, 88 S.Ct., at 516. This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties. . . . This analysis dictates that petitioner can claim no legitimate expectation of privacy here. When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed."

II. Pre-Carpenter Cases Suggesting Limitations on the Third-Party Doctrine

A. Federal Fourth Amendment Cases

1. *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010) (reasonable expectation of privacy in the contents of emails held by a service provider, and therefore a warrant is required); *In re Grand Jury Subpoena, JK-15-029* (*United States v. Kitzhaber*), 828 F.3d 1083 (9th Cir. 2016) (quashing grand jury subpoena seeking former Oregon governor's private emails stored on state server because of the reasonable expectation of privacy in emails held by a third party)
2. *Ferguson v. City of Charleston*, 532 U.S. 67 (2001) (reasonable expectation of privacy in diagnostic test records held by a hospital)
3. *Kyllo v. United States*, 533 U.S. 27 (2001) (reasonable expectation of privacy in thermal signatures emanating from a home)
4. *Bond v. United States*, 529 U.S. 334, 336 (2000) (reasonable expectation that police won't probe and manipulate a bag on the luggage rack of bus, even though the bag is exposed to the public)

5. *Minnesota v. Olson*, 495 U.S. 91, 98–99 (1990) ("an overnight guest has a legitimate expectation of privacy in his host's home" even though his possessions may be disturbed by "his host and those his host allows inside")
6. *Stoner v. California*, 376 U.S. 483 (1964) (Fourth Amendment protects privacy in hotel room even though a guest "undoubtedly gives implied or express permission to such persons as maids, janitors or repairmen to enter his room in the performance of their duties")

B. State Constitutions
   1. A number of states have rejected application of the third-party doctrine under their state constitutions. *See* Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 Cath. U. L. Rev. 373 (2006).

III. *Carpenter v. United States* and Protections for Cell Site Location Information

A. Cell Site Location Information
   1. Cellular service providers log and retain location information for calls, text messages, and data connections. This stored data is known as cell site location information, or CSLI. Typically, these records indicate which cell tower ("cell site") and which directional antenna of that tower ("sector") the phone was connected to at the time of each call, text, or data session. The locational precision of this information will vary according to the broadcast coverage of the cell site. Cell sites are generally more densely arrayed in urban areas, and therefore cover smaller geographic areas. Over time, as service providers have erected more towers and as network technology has advanced, the locational precision of CSLI has increased. Service providers also increasingly log and retain not just tower and sector information, but estimates of the precise location of the phone.
   2. Law enforcement agencies have generally invoked the Stored Communications Act, 18 U.S.C. § 2703, to request historical CSLI from service providers. For these kinds of non-content records, § 2703 provides two options: a warrant, *id.* § 2703(c)(1)(A), or a court order issued upon a showing of "specific and articulable facts showing that there are reasonable grounds to believe that the . . . the records or other information sought[] are relevant and material to an ongoing criminal investigation," *id.* § 2703(d). Prior to *Carpenter*, the government generally obtained the latter orders, rather than warrants.[1]

[1] In the absence of more protective state legislation, state and local law enforcement agents may rely on the Stored Communications Act. *See* 18 U.S.C. § 2703(d). However, a number of states have enacted laws requiring state and local agencies to obtain a warrant for access to historical CSLI. *See* Cal. Penal Code § 1546.1(b); Me. Rev. Stat. tit. 16, § 648; Minn. Stat. §§ 626A.28(3)(d), 626A.42(2); Mont. Code Ann. § 46-5-110(1)(a); N.H. Rev. Stat. Ann. § 644-A:2;

3. In *Carpenter*, the government requested 152 days' worth—and received 127 days' worth—of the defendant's historical CSLI from his service provider using an order issued under § 2703(d). That amounted to 12,898 location points, or an average of 101 per day.

B. In a split panel opinion, the Sixth Circuit in *Carpenter* held that the Supreme Court's third-party doctrine cases compel the conclusion that there is no reasonable expectation of privacy in historical CSLI because it is exposed to and held by the service provider. *United States v. Carpenter*, 819 F.3d 880 (6th Cir. 2016).
   1. Every other federal court of appeals to address the issue had reached the same conclusion, often over dissents. *See United States v. Thompson*, 866 F.3d 1149 (10th Cir. 2017); *United States v. Stimler*, 864 F.3d 253 (3d Cir. 2017); *United States v. Graham*, 824 F.3d 421 (4th Cir. 2016) (en banc); *United States v. Davis*, 785 F.3d 498 (11th Cir. 2015) (en banc); *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013)
      a. The Third Circuit had held that people do not voluntarily disclose their location data to their cellular service provider and so the third-party doctrine does not apply, and thus that magistrate judges have discretion to deny applications for historical CSLI made under § 2703(d) when they believe Fourth Amendment privacy interests are implicated. *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304 (3d Cir. 2010). Subsequently, however, the Third Circuit concluded that there is no reasonable expectation of privacy in historical CSLI, and so its acquisition does not require a warrant. *United States v. Stimler*, 864 F.3d 253 (3d Cir. 2017).
   2. The Massachusetts Supreme Judicial Court reached the opposite conclusion under the state constitution, holding that there is a reasonable expectation of privacy in historical CSLI. *Commonwealth v. Augustine*, 4 N.E. 3d 846 (Mass. 2014).

C. In *Carpenter v. United States*, 138 S. Ct. 2206 (2018), the Supreme Court held that acquisition of historical CSLI is a Fourth Amendment search, and that such search is unreasonable without a warrant.
   1. <u>Application of the Third-Party Doctrine</u>
      a. The Court "decline[d] to extend *Smith* and *Miller* to cover these novel circumstances. Given the unique nature of cell phone 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." *Id.* at 2217.

---

12 R.I. Gen. Laws § 12-32-2; Utah Code Ann. § 77-23c-102(1)(a); Vt. Stat. Ann. tit. 13, § 8102(b). A number of other states have statutes that mirror the requirements of the federal Stored Communications Act.

b. Neither rationale offered by *Miller* and *Smith* – the limited nature of the information collected, nor the voluntariness of the conveyance of that information – apply to cell site location information.
    i. "There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today. . . . [This case] is about a detailed chronicle of a person's physical presence compiled every day, every moment, over several years. Such a chronicle implicates privacy concerns far beyond those considered in *Smith* and *Miller*." *Id.* at 2219-20.
    ii. "Neither does the second rationale underlying the third-party doctrine—voluntary exposure—hold up when it comes to CSLI. Cell phone location information is not truly 'shared' as one normally understands the term. In the first place, cell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society. Second, 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." *Id.* at 2220 (citing *Riley v. California*).

2. Reasonable Expectation of Privacy
    a. "As technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to 'assure [ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" *Id.* at 2214.
        i. "Prior to the digital age, law enforcement might have pursued a suspect for a brief stretch, but doing so 'for any extended period of time was difficult and costly and therefore rarely undertaken.' For that reason, '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.'" *Id.* at 2217 (quoting *Jones* (Alito, J., concurring in judgment)).
        ii. "Allowing government access to cell-site records contravenes that expectation" because it "provides an all-encompassing record of the [cell phone user's] whereabouts. As with GPS information, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'" *Id.* at 2217 (quoting *Jones* (Sotomayor, J., concurring).

iii. Government acquisition of CSLI violates reasonable expectations of privacy because people carry their phones with them virtually all the time, and so it gives the government access to "near perfect surveillance."
iv. Acquisition of CSLI also violates reasonable expectations of privacy because it gives police the new power to "travel back in time to retrace a person's whereabouts."

3. Warrant Requirement
   a. The government had argued that even if acquisition of CSLI is a Fourth Amendment search, it should be considered reasonable if carried out with a subpoena or other form of compulsory process (like a court order under the Stored Communications Act). The government took the position that subpoenas and similar compulsory process have always been upheld as long as they sought information relevant to the government's investigation and were not grossly overbroad.
   b. The Court rejected this position, holding that a warrant is required.
      i. "[T]his Court has never held that the Government may subpoena third parties for records in which the suspect has a reasonable expectation of privacy. . . . If the choice to proceed by subpoena provided a categorical limitation on Fourth Amendment protection, no type of record would ever be protected by the warrant requirement." *Id.* at 2221-22.

D. Property-Based Theories and Justice Gorsuch's Dissent
   1. In a dissent, Justice Gorsuch disagreed with the application of the *Katz* reasonable-expectation-of-privacy test, but suggested that records held by a third party could be protected under the Fourth Amendment by looking to property principles like those relied on by the Court in *United States v. Jones* and *Florida v. Jardines*, 133 S. Ct. 1409 (2013).
   2. Under Justice Gorsuch's theory, people's "papers and effects" can be protected under the Fourth Amendment even if they are held by a third party. In this view, even if the company with custody of digital records has *some* property rights in the data, the fact that the customer retains other property rights in those records can result in Fourth Amendment protections. To determine whether a person has a sufficient interest in the "paper" or "effect," Justice Gorsuch would look to positive law – statutes and common law property and tort principles.
   3. In the case of CSLI, the federal Telecommunications Act, 47 U.S.C. § 222, designates cell phone location records as "customer proprietary network information" and prohibits carriers from disclosing them "without the express prior authorization of the customer." This and similar legal protections give customers "substantial legal interests in this information, including at least some right to include, exclude, and

control its use. Those interests might even rise to the level of a property right." *Carpenter*, 138 S. Ct. at 2272 (Gorsuch, J., dissenting).

4. Justice Gorsuch ultimately declined to decide whether CSLI could be protected under his property principles because he believed Carpenter failed to adequately argue the property theory. But he clearly signaled that in future cases, criminal defendants should more vigorously make these arguments so that they are properly presented and form the basis for possible decision.

IV. After *Carpenter,* What's Next?

A. The Court purported to be issuing a "narrow" decision. It stated that it was not ruling on a number of related issues, including:
   1. Requests for less than seven days of historical CSLI
   2. Real-time CSLI
   3. Tower dumps (ie, "a download of information on all the devices that connected to a particular cell site during a particular interval").
   4. "We do not disturb the application of *Smith* and *Miller*"
   5. "[C]onventional surveillance techniques and tools, such as security cameras."
   6. "[O]ther business records that might incidentally reveal location information."
   7. "[O]ther collection techniques involving foreign affairs or national security."

B. The Court's decision, however, clearly opens space for litigation over other kinds of particularly sensitive third-party-held records that should be protected by the Fourth Amendment. In thinking about what kinds of post-*Carpenter* challenges to bring, look to how other kinds of data compare to CSLI along the dimensions identified in *Carpenter*:
   1. Pervasiveness
   2. Retrospectivity
   3. Granularity or precision of the data now, or the trend toward greater granularity or precision as technology advances
   4. Unavoidability of creation
   5. Reveals "privacies of life"
   6. Access to data gives police a categorically new power that they did not possess prior to the advent of the technology in question
   7. Data available not just for criminal suspects, but for all Americans

C. Some of the most promising types of data for future challenges could include:
   1. Communicative "contents." All nine Justices appeared to agree that the contents of emails are protected by the Fourth Amendment. The contents of other electronic communications, such as text messages and private social media messages, as well as

documents, photos, and videos stored privately in the cloud (ie, Dropbox, Google Docs, etc), search queries entered into a search engine, and web browsing history should also be protected by a warrant requirement.

2. Information about the interior of the home. This includes data from so-called "smart" and "internet of things" devices, such as smart meters (which collect granular, moment-by-moment information about electricity consumption), smart thermostats (which know when a person is a home and possibly which room they are in), smart refrigerators (which can know what a person is consuming and at what rate), smart mattresses (which know when a person goes to bed and how well they sleep), and many more devices. Also of great concern is audio recorded by in-home smart assistants, such as Amazon Alexa, Google Home, etc.
3. Information about the state of the body. Heart-rate data from a smartwatch, information about sexual activity from a fertility tracking app, third-party-held medical records, etc.
4. Other kinds of stored location information. Location history held by Apple, Google, or location-enabled apps.
5. Other kinds of pervasive location tracking technologies: Automated license plate readers, facial recognition-enabled networked surveillance cameras, pervasive aerial surveillance.
6. Real-time cell phone location tracking: Even shorter-term real-time cell phone location tracking can violate expectations of privacy, because it gives police a new power to pluck a person's location out of thin air. This is different from the shorter-term GPS tracking that Justice Alito suggested might be acceptable without a warrant in *Jones*, because in the GPS context police know where the car is at the start of surveillance and use technology to augment their ability to follow it. With cell phone tracking, police gain location information that would have been categorically unavailable to them without cell phones.

D. Practice Tips
   1. Always raise and preserve property-based arguments along the lines of Justice Gorsuch's opinion in *Carpenter*
   2. At the suppression hearing, introduce the full set of records obtained by the government from the third-party company, not just the portion of those records that you seek to suppress. Introducing the full set of records can help appellate counsel illustrate how sensitive and revealing the data is, and helps avoid focus on the particular data points that are most incriminating.
   3. At the suppression hearing, question the government about full capabilities of the technology at issue and the full scope of data that can be obtained. Illustrate the invasiveness and pervasiveness of the data.

Additional Resources

Carpenter v. United States:

Brief for Petitioner (Supreme Court):
https://www.aclu.org/sites/default/files/field_document/16-402_ts_1.pdf

Briefs and related materials in *Carpenter* (from Sixth Circuit and Supreme Court):
https://www.aclu.org/cases/united-states-v-carpenter

Materials related to other sensitive data held by third-party companies:

Pre-*Carpenter* briefs arguing that the third-party doctrine should not apply to confidential prescription records held in a state prescription monitoring program database:
US DOJ v. Utah Dep't of Commerce:
https://www.aclu.org/sites/default/files/field_document/25_intervenors_opposition_to_dea_petition.pdf
Oregon Prescription Drug Monitoring Program v. US DEA:
https://www.aclu.org/sites/default/files/field_document/intervenors_9th_cir_brief_filed.pdf

Police Use Fitbit Data to Charge 90-Year-Old Man in Stepdaughter's Killing, N.Y. Times, Oct. 3, 2018, https://www.nytimes.com/2018/10/03/us/fitbit-murder-arrest.html

Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521 (7th Cir. 2018) (applying *Carpenter* to smart meter data)