BerkeleyLaw
UNIVERSITY OF CALIFORNIA

Samuelson Law, Technology
& Public Policy Clinic

The Fourth Amendment & Third-Party Doctrine after *Carpenter*

2019 CJA Conference in the District of New Jersey

February 2, 2019

Megan Graham
Samuelson Law, Technology & Public Policy Clinic
U.C. Berkeley School of Law
mgraham@clinical.law.berkeley.edu

In *Carpenter v. United States*, the Supreme Court declined to extend the third-party doctrine to cell site location information ("CLSI") held by cell phone companies and opened the door to a wide array of challenges to the government's habit of obtaining digital third-party records without a warrant. This session will discuss the Fourth Amendment frameworks that led to *Carpenter*, the holding and reasoning of the case, and potential challenges to litigate in the wake of *Carpenter*.

I. Background

A. Third Party Doctrine

- 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).
- *United States v. Miller*, 425 U.S. 435 (1976)
    - No reasonable expectation of privacy in several months' worth of bank records (e.g., canceled checks, deposit slips, account statements) held by a bank. Therefore, law enforcement agents can obtain those records via subpoena, without a search warrant.
    - "On their face, the documents subpoenaed here are not respondent's 'private papers.' . . . [R]espondent can assert neither ownership nor possession. Instead, these are the business records of the banks." *Miller*, 425 U.S. at 440.
    - "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 [the third party] 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." *Id.* at 443.

- *Smith v. Maryland*, 442 U.S. 735 (1979)
    - No reasonable expectation of privacy in the phone numbers dialed to place a call, and thus the government can obtain those numbers from the phone company without a warrant.
    - "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." *Smith*, 442 U.S. at 743.
    - "[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. 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." *Id.* at 743–44 (internal citations and quotation marks omitted).
- *But see, e.g.*, *Ferguson v. City of Charleston*, 532 U.S. 67 (2001) (finding reasonable expectation of privacy exists in diagnostic test records held by a hospital); *Minnesota v. Olson*, 495 U.S. 91, 98–99 (1990) (indicating that "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").

B. Fourth Amendment & Technology

- *Kyllo v. United States*, 533 U.S. 27 (2001)
    - Individual has a reasonable expectation of privacy in thermal signatures emanating from a home, and thus a warrant is presumptively required to use thermal imaging equipment.
    - "[O]btaining by sense-enhancing technology any information regarding the home's interior that could not otherwise have been obtained without physical intrusion into a constitutionally protected area constitutes a search—at least

where (as here) the technology in question is not in general public use." *Kyllo v. United States*, 533 U.S. at 34.

- "While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development." *Id.* at 36.

- *United States v. Jones*, 565 U.S. 400 (2012)
  - Scalia Majority
    - "We hold that the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search.'" *Jones*, 565 U.S. at 404 (footnote omitted).
    - "It is important to be clear about what occurred in this case: 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." *Id.* at 404–05.
    - "Fourth Amendment rights do not rise or fall with the *Katz* formulation. At bottom, we must assure preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted. As explained, for most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates. *Katz* did not repudiate that understanding." *Id.* at 406–07 (internal citation, quotation marks, and footnote omitted).
  - Sotomayor Concurrence
    - Justice Sotomayor joined the Majority, and agreed in substantial part with Justice Alito's concurrence. But she wrote separately to discuss how she would apply the *Katz* test to GPS monitoring, indicating that she would find individuals have a reasonable expectation of privacy in the detailed cataloging of movements that GPS tracking provides, even for short durations of time.
    - "[A] search within the meaning of the Fourth Amendment occurs, at a minimum, where, as here, the Government obtains information by physically intruding on a constitutionally protected area. . . . Of course, the Fourth Amendment is not concerned only with trespassory intrusions on property. Rather, even in the absence of a trespass, a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable." *Jones*, 565 U.S. at 413–14 (Sotomayor, J., concurring) (cleaned up).
    - "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. . . . The Government can store such records and efficiently mine them for information years into the future. . . . And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: limited police resources and community hostility." *Id.* at 415–16 (internal citations and quotation marks omitted).

        - "I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on." *Id.* at 416.

    - Alito Concurrence in the Judgment

        - "In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken." Jones, 565 U.S. at 429 (Alito, J., concurring in the judgment).

        - "[R]elatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." *Id.* at 430.

        - "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." *Id.* at 430.

- *Riley v. California*, 134 S. Ct. 2473 (2014)

    - Cell phones are qualitatively and quantitatively different than other items an arrestee might be carrying, so a warrant is presumptively necessary to search contents even when the device is lawfully seized incident to arrest.

    - "The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the

purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone." *Riley*, 134 S. Ct. at 2489.

- The Court pointed to four factors in reaching its conclusion, *id.* at 2489–90:
  - (1) The combination of information cell phones contain reveals a significant amount about a person, much more than a single record.
  - (2) Even a single category or type of information can now convey far more than previously possible.
  - (3) The time horizon of records stored has increased a significant amount.
  - (4) The pervasiveness of information carried around on cell phones and the pervasive use of cell phones in modern society.

- *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010)
  - Individuals have a reasonable expectation of privacy in the contents of emails held by a service provider, and therefore a warrant is presumptively required to obtain them.
  - "Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection. . . . It follows that email requires strong protection under the Fourth Amendment; otherwise, the Fourth Amendment would prove an ineffective guardian of private communication, an essential purpose it has long been recognized to serve." *Id.* at 285–86.
  - "As an initial matter, it must be observed that the mere ability of a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy." *Id.* at 286.
  - "Accordingly, we hold that a subscriber enjoys a reasonable expectation of privacy in the contents of emails that are stored with, or sent or received through, a commercial ISP. The government may not compel a commercial ISP to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause." *Id.* at 288 (internal citation and quotation marks omitted).
  - At this point, *Warshak* operates as the law of the land in practice. *See* Electronic Frontier Foundation, *Who Has Your Back?* 7 (2017), https://www.eff.org/files/2017/07/08/whohasyourback_2017.pdf ("Every company we evaluate has adopted baseline industry best practices, such as publishing a transparency report and requiring a warrant before releasing user content to the government.").
  - *See also, e.g.*, 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).

- *But see, e.g.*, *Walker v. Coffey*, 905 F.3d 138, 147 (3d Cir. 2018) (indicating that individual must have a reasonable expectation of privacy in messages at issue for Fourth Amendment to require warrant in context of a qualified immunity analysis).

II. *Carpenter v. United States*

- Cell Site Location Information

  - In *Carpenter*, cell site location information ("CSLI") was used "to identify Petitioner Timothy Carpenter's whereabouts over more than four months. The records, which are logged and retained by cellular service providers whenever people carry modern cell phones, make it possible to reconstruct in detail everywhere an individual has traveled over hours, days, weeks, or months." Brief for Petitioner, *Carpenter v. United States*, 138 S. Ct. 2206 (2018), https://www.aclu.org/sites/default/files/field_document/16-402_ts_1.pdf.

  - "In order to access the cellular network, cell phones must connect to nearby cell towers (known as 'cell sites'), thereby creating a record of the phone's location. The precision of a cell phone user's location reflected in CSLI records depends on the size of the cell site 'sectors' in the area. Most cell sites consist of multiple directional antennas that divide the cell site into sectors. The majority of cell sites comprise three directional antennas that divide the cell site into three sectors (usually 120 degrees each), but an increasing number of towers have six antennas (covering approximately 60 degrees each). The coverage area of each cell site sector is smaller in areas with greater density of cell sites, with urban areas having the greatest density and thus the smallest coverage areas. The smaller the coverage area, the more precise the location information revealed and recorded." *Id.* (internal citations omitted).

  - For a sense of scale, a recent study of how Google gathers information about its users found that Android—a common phone operating system owned by Google—is a key driver in how the company learns about and tracks its customers. The report indicates that with *no user interaction*, Google made 40 requests for information per hour to an Android phone, and more than 900 requests per day. Roughly 35 percent of those requests were for location information. Douglas C. Schmidt, *Google Data Collection* (2018), https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf.

  - Before *Carpenter*, law enforcement agencies commonly 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 indicates law enforcement can get 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 records "are relevant and material to an ongoing criminal investigation," *id.*

§ 2703(d). For obvious reasons, law enforcement most commonly sought § 2703(d) orders.

- *Carpenter* in the lower courts

  - In *Carpenter*, the government requested 152 days'—and received 127 days'—worth of Mr. Carpenter's historical CSLI from his service providers using a § 2703(d) order. That amounted to 12,898 location points, or an average of 101 per day. The government also received 7 days' worth of historical CSLI from a second service provider that covered time when Mr. Carpenter was out of state and roaming on the second providers' cell towers.

  - In a split 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).

  - Every other federal court of appeals to address the issue had reached the same conclusion, though the panel decisions were often split. *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); *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).

- *Carpenter* in the Supreme Court, *Carpenter v. United States*, 138 S. Ct. 2206 (2018)

  - Supreme Court held that acquisition of historical CSLI is a Fourth Amendment search, and that such search is presumptively unreasonable without a warrant.

  - Third-Party Doctrine

    - 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." *Carpenter*, 138 S. Ct. at 2217.

    - The Court framed *Miller* and *Smith* as resting on two key realities: First, the Court in those cases examined "the nature of the particular documents sought" and found that the information collected from a pen register and bank records was limited. Second, the *Carpenter* Court said the earlier third-party doctrine cases rested on the voluntary nature of the disclosure of information to the third party. Neither of these realities—limited information collected and collection of voluntarily surrendered information—is present for historical CSLI.

      - "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.

- "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*).

- Reasonable Expectation of Privacy

  - "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 (alteration and quotation marks omitted).

  - "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 *United States v. Jones* (Alito, J., concurring in judgment)).

  - "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 *United States v. Jones* (Sotomayor, J., concurring)).

  - The Court wrote that "when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user." *Id.* at 2218. As a result, collection of historical CSLI violates a phone user's reasonable expectation of privacy when done without a warrant.

  - 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." *Id.* at 2218.

- Warrant Requirement

  - The government 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 (e.g., a § 2703(d) order). The government took the position that subpoenas and similar compulsory process have been upheld when they sought information relevant to the government's investigation and were not grossly overbroad.

  - The Court rejected this position, holding that a warrant is required. "[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.

- Property-Based Theories and Justice Gorsuch's Dissent

  - In a dissent, Justice Gorsuch disagreed with the Majority's 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*, 569 U.S. 1 (2013).

  - 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. *Carpenter*, 138 S. Ct. at 2263 (Gorsuch, J., dissenting).

  - In the case of CSLI, Justice Gorsuch pointed out that the 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." *Id.* at 2272.

  - Justice Gorsuch declined to decide whether CSLI could be protected under his property principles because he believed Mr. Carpenter had failed to adequately argue the property theory. But Justice Gorsuch clearly signaled that criminal defendants should more vigorously make these arguments so that they are properly presented and may form the basis for possible decision. *See id.* at 2272.

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

- The Court indicated *Carpenter* is a "narrow" decision. It stated that it was not ruling on a number of related or similar issues, including:
    - Requests for less than seven days of historical CSLI
    - Real-time CSLI
    - Tower dumps (i.e., "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*"
    - "[C]onventional surveillance techniques and tools, such as security cameras"
    - "[O]ther business records that might incidentally reveal location information"
    - "[O]ther collection techniques involving foreign affairs or national security."
- But, the Court's reasoning is quite broad and opens the door to litigation over these and other kinds of sensitive third-party-held records that should be protected by the Fourth Amendment.
- In *Carpenter*, the Court examined a number of dimensions of the technology and information gathered, including:
    - Pervasiveness
    - Retrospectivity
    - Granularity or precision of the data now, or the trend toward greater granularity or precision as technology advances
    - Unavoidability of creation
    - Whether the data reveals "privacies of life"
    - Whether access to data gives law enforcement a categorically new power that they did not possess prior to the advent of the technology in question
    - Data available not just for criminal suspects, but for all Americans
- Promising Types of Data for Future Challenges
    - Location information of other types
        - Historical CSLI for less than 7 days

        - Real-time CSLI, StingRays
        - GPS tracking of cell phone
        - Tower dumps
        - Dumps of location information from Google, Apple, apps
        - Automated license plate readers, networked surveillance cameras, toll plaza or transportation system records
        - IP addresses
    - Other sensitive data
        - Communicative "contents" (e.g., text messages, private social media messages, documents and photos stored in the cloud, search queries entered into a search engine, web browsing history)
        - "Smart" devices in the home (e.g., smart meters, smart refrigerators)
        - Fitness and health trackers
        - Amazon Echo, Google Home
    - Other Fourth Amendment doctrines
        - Though these will be difficult to mount challenges to, *Carpenter*'s broad reasoning and articulation of the modern Fourth Amendment may undermine the foundation of the third-party doctrine more broadly.
        - It may also mean that the border search doctrine is no longer as broad as we once thought, particularly where digital devices are concerned.
        - *Carpenter*'s applicability to emerging and future technologies (e.g., facial recognition, iris scanning) has yet to be tested.

- Good Faith
    - Cases are already emerging that invoke the good faith exception in upholding the collection of location information without a warrant if the predates *Carpenter*.
    - *See, e.g.*, *United States v. Goldstein*, No. 15-4094, 2019 WL 273103 (3d Cir. Jan. 22, 2019); *United States v. Zodhiates*, 901 F.3d 137, 143 (2d Cir. 2018); *United States v. Curtis*, 901 F.3d 846 (7th Cir. 2018); *United States v. Pleasant*, No. 17-cr-62, 2018 WL 4252632 (E.D. Pa. Sept. 5, 2018); *United States v. Blake*, No. 3:16-cr-111-JBA, 2018 WL 3974716 (D. Conn. Aug. 20, 2018); *United States v. Williams*, No. 2:17-cr-20758-VAR-DRG, 2018 WL 3659585 (E.D. Mich. Aug. 2, 2018).

- The courts' rationale has been that, regardless of whether *Carpenter* applies retroactively (the courts are divided on that point), law enforcement's previous reliance on § 2703 orders does not warrant suppression.

- There is an outlier appellate case in Florida, resting on state law, that overturned a trial court's denial of a motion to suppress after *Carpenter*. *See Ferrari v. State*, No. 4D14-464, 2018 WL 4212142 (Fla. Dist. Ct. App. Sept. 5, 2018). In that case, law enforcement officers had obtained historical CSLI via a Florida procedure that permits the installation of a pen register or trap and trace device based on law enforcement affidavit. The court said that good faith is appropriate where officers act in reliance on binding decisional law or an applicable statute. The court then found that there was no binding decisional law about CSLI in 2001 when the data was obtained, and that the officers' reliance on the Florida pen register/trap and trace statute was inappropriate because it is not applicable to CSLI.

- Practice Tips

  - Always raise and preserve property-based arguments along the lines of Justice Gorsuch's opinion in *Carpenter*.

  - 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.

  - 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.

  - Keep a close eye on changes to warrant applications. Most warrant applications are rote and boilerplate, and even subtle changes to language can signal changes in law enforcement interpretations of what a warrant covers.