ALSTON & BIRD

WWW.ALSTON.COM

National Security & Digital Crimes and Cybersecurity Preparedness & Response ADVISORY ■

JULY 26, 2018

U.S. Supreme Court Builds On Individuals' Privacy Rights

by Kim Peretti, Larry Sommerfeld, and Nameir Abbas

The Supreme Court's recent decision in *Carpenter v. United States* continues to generate interest more than a month after its release. While the Court proclaimed its holding as narrow, its unprecedented recognition of an individual's privacy interest in data held by third parties could signal important changes in privacy more generally.

Background

Timothy Carpenter was convicted for his participation in a series of armed robberies.[1] While investigating Carpenter, law enforcement obtained court orders for cell-site location information under the Stored Communications Act (SCA). The SCA requires a showing of "specific and articulable facts … that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[2]

The court orders requested cell-site location information for periods of 127 days from one cell phone carrier and seven days from another.[3] The government's expert witness at Carpenter's trial explained that cell phone carriers log certain information each time a cell phone accesses the wireless network. Using this information, the government produced "maps that placed Carpenter's phone near four of the charged robberies."[4]

Carpenter argued that the government's seizure of his cell-site location information violated the Fourth Amendment because he had a reasonable expectation of privacy in the cell-site location information and because the government had not obtained a warrant supported by probable cause.[5]

---

1 *Carpenter*, 585 U. S. ____ (2018) (slip op., at 4).

2 18 U.S.C. § 2703(d).

3 *Carpenter*, 585 U. S. ____ (slip op., at 3). Note that the request for seven days of cell-site location information yielded only two days' worth of data.

4 *Id*. at 3-4.

5 *Id*. at 3.

Legal Landscape

The Fourth Amendment protects against "unreasonable searches and seizures" of "persons, houses, papers, and effects." In *Katz v. United States*, 389 U.S. 347, 351 (1967), the Supreme Court extended this protection to an individual's "reasonable expectation of privacy," beginning a lengthy line of cases testing the boundaries of privacy.

According to the majority opinion, *Carpenter* sits at the intersection of two sets of Fourth Amendment cases. The first, beginning with *United States v. Jones,* 565 U.S. 400 (2012), recognized an individual's expectation of privacy in a long-term surveillance of physical location and movement. Before *Jones*, the Court had held that augmented visual surveillance, involving use of a beeper attached to a vehicle and resulting in the tracking of an individual's movements, did not constitute a search.[6] The Supreme Court held in *Jones* that the placement of a GPS tracking device on a car was a trespass, and thus the collection of 28 days of location data using that device was a Fourth Amendment search.[7] More importantly, a collection of five concurrences in *Jones* agreed that "longer term GPS monitoring," in certain circumstances, "impinges on expectations of privacy."[8] It is this agreement among the concurrences that forms the first pillar of the Court's holding in *Carpenter*.

The second set of Fourth Amendment cases relates to what is commonly known as the third-party doctrine. That long-standing doctrine holds that an individual generally "has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[9] The Court has applied the third-party doctrine in contexts as varied as bank records and pen registers (that is, records of dialed phone numbers). For example, in *United States v. Miller*, 425 U.S. 435 (1976), the Court rejected a Fourth Amendment challenge to the collection of bank records partly because the records were not confidential and contained information that was exposed to the bank as part of the bank's business. Similarly, the Court has rejected a challenge to the use of a pen register because the dialed numbers are used by the telephone company.[10]

Court's Decision

The Supreme Court, by a 5–4 majority, agreed with Carpenter and held that the government's acquisition of cell-site location information covering a period of seven days or more was a search under the Fourth Amendment. In doing so, the Court for the first time recognized an individual's reasonable expectation of privacy in information generated and maintained by third parties in the course of business. The Court characterized the cell-site location information as "detailed, encyclopedic, and effortlessly compiled."[11] The Court emphasized that a comprehensive record of an individual's movements was sufficiently different from bank records and pen register information to which the Court had previously applied the third-party doctrine.[12]

---

6 *United States v. Knotts*, 460 U. S. 276 (1983).

7 *United States v. Jones*, 565 U.S. 400, 404 (2012)

8 *Id*. at 430 (ALITO, J., concurring in judgement); *id*., at 415 (SOTOMAYOR, J., concurring).

9 *Smith v. Maryland*, 442 U.S. 735, 743-744 (1979).

10 *Id*. at 742.

11 *Carpenter*, 585 U. S. _____ (slip op., at 10).

12 *Id*. at 11.

As the Court made clear, the comprehensive nature of the information at issue was a key consideration in its decision. An "all-encompassing record of the holder's whereabouts," capable of revealing information about not only "particular movements" but also "familial, political, professional, religious, and sexual associations," posed privacy concerns.[13] The ubiquity of cell phone usage and the fact that the data in question was retrospective in nature also factored into the Court's reasoning.[14] Notably, the Court explicitly based its reasoning on the likelihood that cell-site location information would improve, amplifying the privacy concerns associated with unfettered access to such information.[15]

The Court took pains to emphasize *Carpenter*'s limited Fourth Amendment application at great length: the decision does not address the real-time capture of cell-site location information (as opposed to retrospective collection), collection of cell-site location information covering a shorter period of time, or the capture of information on all devices that connected to a particular cell site during a particular time period. Nor does *Carpenter* itself upturn application of the third-party doctrine in other areas,[16] such as for bank records or pen register information, or invalidate legal process standards under the SCA or ECPA. However, as the dissents make clear, *Carpenter* represents a substantial departure from existing precedent under the third-party doctrine.[17]

Analysis

The *Carpenter* decision departs substantially from previous Fourth Amendment doctrine, expanding individuals' privacy interests in automatically and ubiquitously collected digital data held by third parties. Rather than apply the traditional bright-line rule that information given to a third-party loses Fourth Amendment privacy protection, the Court employed a kind of balancing test, focusing on the substance and nature of the information at issue along with the circumstances of its collection in determining whether individuals retained privacy interests in the information. By abandoning the previous bright-line rule, the Court invites substantial follow-on litigation with potentially broad applications.

Privacy interest in a "comprehensive record"

Carpenter signals a shift in the characterization of Fourth Amendment privacy interests. Rather than hinging Fourth Amendment protection on an individual's "persons, houses, papers, and effects," or on whether the information is a business record or has been disclosed to a third party, the Court's decision weighs the sensitive nature of certain data—data that reveals the whole of a person's physical movements. Regardless of whether a third party generates such information or "the Government employs its own surveillance technology" to generate it, the Court has for the first time held that an individual has a reasonable expectation of privacy in comprehensive records of their movements, even when those records are held by a third party.[18]

---

[13] *Id.* at 12.

[14] *Id*. at 12-13.

[15] *Id.* at 14.

[16] *Id*. at 17-18.

[17] *Carpenter*, 585 U. S. ____ (slip op., at 7) (KENNEDY, J., dissenting).

[18] *Carpenter*, 585 U. S. ____ (slip op., at 11).

Put differently, the *Carpenter* decision recognized an individual's expectation of privacy in a comprehensive record of their movement generated and held by a third party, while the *Jones* concurrences recognized an individual's expectation of privacy in a comprehensive record of their public movements tracked and compiled by the government through a GPS tracker. By its terms, the Fourth Amendment protects the right of individuals "to be secure in their persons, houses, papers, and effects." In combination, the *Carpenter* decision and *Jones* concurrences imply that a comprehensive record of an individual's movements constitutes a paper or effect that belongs to the individual even when the record is not within the individual's possession and is not generated by the individual.

Privacy and the compilation of data

Carpenter continues the Court's recent interest in the compilation of data and digital technologies, underscoring the rationale for establishing arguably separate standards for digital and non-digital data. In particular, *Carpenter* discusses the "detailed, encyclopedic, and effortlessly compiled" nature of the location information at issue, its "ability to chronicle a person's past movements," and the continued and ongoing improvements in the underlying technology.[19] This discussion echoes the concurring opinions in *Jones*, which point to the wealth of information afforded by GPS monitoring and raise interesting questions about the broad array of data held by third parties and routinely compiled: phone numbers dialed or texted, URLs visited, emails exchanged, and even goods purchased.[20] Along those lines, *Riley v. California* carved out an exception for digital data, protecting cellular telephones from being searched incident to arrest. According to the Court in *Riley,* the collection of "many distinct types of information" on cell phones raised unique privacy concerns.[21]

Taken together, the Court's recent jurisprudence shows an underlying concern with the unprecedented availability of large amounts of comprehensive data through digital technologies. The Court's opinion in *Carpenter* abandons the traditional Fourth Amendment dividing line between private information and information held by third parties at least when huge volumes of digital data are generated, compiled, and stored automatically. Likewise, five Justices in *Jones* recognized a privacy interest even when location information is exposed to the public if it covers a sufficient length of time. And in *Riley*, the Court held that the nature and quantity of data on cell phones today is too great to fall under the rubric of a traditional warrantless arrest search. Digital, the Court is telling us, is different.

Takeaways

The Court's reasoning carries significance for privacy in the digital age. As a starting point, *Carpenter* portends only the beginning, rather than the end, of litigation concerning the third-party doctrine as it relates to digital data. While *Carpenter* focuses on a person's expectation of privacy in a comprehensive record of the person's movements, it is easy to imagine other scenarios in which the compilation of data exposed to the public or maintained by third parties produces similarly sensitive records. And as Justice Sotomayor's concurrence in the *Jones* case points out, we should not assume that an individual lacks an expectation of privacy in, for example, a comprehensive web browsing history or other online activities. More generally, *Carpenter* comes at a time of potential upheaval in the privacy space. *Carpenter's* ramifications will be litigated heavily at the state and federal levels, and its fallout may greatly interest legislators and privacy advocates in this country and elsewhere.

---

19 *Carpenter*, 585 U. S. _____ (slip op., at 10).

20 *See Jones*, 565 U.S. 400, 428 (SOTOMAYOR, J., concurring).

21 *Riley* v. *California*, 573 U.S. __ , __ (2014) (slip op., at 18).

You can subscribe to future *Privacy & Security* advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information please contact your Alston & Bird attorney or any of the following:

National Security & Digital Crimes
Cybersecurity Preparedness & Response

Kimberly Kiefer Peretti
202.239.3720
kimberly.peretti@alston.com

Jim Harvey
404.881.7328
jim.harvey@alston.com

Follow us: @AlstonPrivacy | www.AlstonPrivacy.com

www.alstonsecurity.com

ALSTON & BIRD

WWW.ALSTON.COM

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86 10 8592 7500
BRUSSELS: Level 20 Bastion Tower ■ Place du Champ de Mars ■ B-1050 Brussels, BE ■ +32 2 550 3700 ■ Fax: +32 2 550 3719
CHARLOTTE: Bank of America Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: 2828 North Harwood Street ■ 18th Floor ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ 919.862.2200 ■ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ 415.243.1000 ■ Fax: 415.243.1001
SILICON VALLEY: 1950 University Avenue ■ 5th Floor ■ East Palo Alto, California, USA, 94303-2282 ■ 650-838-2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333