POLSINELLI

July 2018

In *Carpenter v. United States*, the Supreme Court Extends Fourth Amendment Protections to Consumer Data Held by Wireless Carriers

By D. Rockwell Bower

The U.S. Supreme Court recently ruled in *Carpenter v. United States*[1] that the government must have a warrant to access an individual's cell phone location history from wireless carriers. The Court held, in a 5–4 opinion issued by Chief Justice Roberts and joined by Justices Ginsburg, Breyer, Sotomayor and Kagan, that individuals have a reasonable expectation of privacy in their cell phone location history, even if shared with third parties. Therefore, the Court held, law enforcement access to a cell phone location history requires a warrant. This ruling is narrow and largely confined to the facts of this case. The Court did not find that location information – in and of itself – is protected by the Fourth Amendment, holding instead that location information sufficient to track an individual's every movement for four months is protected and would require a warrant. In recognizing that such business records are sometimes entitled to Fourth Amendment protection, the Court also rejected the previous doctrine that disclosure to a third-party categorically waives protection under the Fourth Amendment. The case is expected to have lasting ramifications for privacy concerns in an evolving digital age where third parties often have access to and process private information from individuals in large quantities over protracted periods of time.

Procedural Background

In 2011, police officers arrested four men suspected of a string of robberies in the Detroit area. One of the men confessed to the crimes and identified several accomplices who had participated in the robberies. He also provided some of their cell phone numbers. Based on that information, law enforcement applied for a court-ordered subpoena under the Stored Communications Act ("SCA") to obtain cell phone records for Timothy Carpenter.

The SCA authorizes the government to compel disclosure of specific telecommunications records when it provides "specific and articulable facts showing that there are reasonable grounds to believe" that the records "are relevant and material to an ongoing criminal investigation."[2] Pursuant to that authority, investigators obtained two court orders directing Carpenter's wireless carriers (MetroPCS and Sprint) to disclose their cell tower records for Carpenter's location over a four month period.

[1] 585 U.S. ___ (2018).
[2] 18 U.S.C. § 2703(d).

Author:

D. Rockwell Bower
Associate
214.661.5510
rbower@polsinelli.com

Additional Contacts:

Gregory M. Kratofil, Jr.
Practice Chair
303.583.8270
gkratofil@polsinelli.com

Bruce A. Radke
Shareholder
312.463.6211
bradke@polsinelli.com

Jarno J. Vanto
Shareholder
212.413.2841
jvanto@polsinelli.com

Michael J. Waters
Shareholder
312.463.6212
mwaters@polsinelli.com

Cell phones operate by continuously connecting to a network of radio antennas referred to as "cell towers." Cell phones automatically and continuously connect to the closest cell tower to transmit and receive information, such as phone calls and text messages. Cell phones also autonomously connect without any direction from the user, constantly checking for new alerts such as e-mails, software updates, application notifications, or updating the phone's location which is utilized in a variety of features. The more densely populated the area, the more cell towers are needed to provide service to customers. In more densely populated areas where there are more cell towers, a person's proximity to a cell tower can be identified in a radius within tenths of a mile. Each time a cell phone connects to a cell tower, it generates a time-stamped record referred to as cell-site location information ("CSLI"). This information is routinely collected by wireless carriers for business purposes, and is generally retained for five years, based on the individual carrier's business practices.

Pursuant to the SCA, investigators obtained Carpenter's CSLI for a period of four months, which generated nearly 13,000 location points (over 100 per day) cataloging Carpenter's movements. With this information, prosecutors created maps depicting Carpenter's location at the time of four robberies, placing him in the vicinity at the time each crime occurred. In closing arguments, the government relied heavily on Carpenter's location data, contending that the information confirmed Carpenter was "right where the . . . robbery was at the exact time of the robbery."[3]

Carpenter unsuccessfully moved to suppress his CSLI on the grounds that the information was a warrantless search in violation of the Fourth Amendment. Carpenter was convicted on several counts and sentenced to over 100 years in prison. The Sixth Circuit affirmed, holding that Carpenter lacked a reasonable expectation of privacy over the CSLI as he had voluntarily shared it with his wireless carriers. The appellate court determined that the information constituted third-party business records unprotected by the Fourth Amendment and on that basis ruled that such records could be subpoenaed under the SCA.

Disclosure of Information to Third-Parties No Longer Categorically Waives Fourth Amendment Protection

Fourth Amendment precedent has historically drawn a line between an individual's private papers and effects and information that is voluntarily shared with a third-party. Information held by an individual is protected from warrantless search and seizure by the Fourth Amendment; information voluntarily shared with someone else is not. Under this "third-party doctrine," an individual assumes the risk that information shared with third-parties can be obtained without reaching the threshold of the Fourth Amendment. This doctrine was expressly recognized in *United States v. Miller*,[4] where the Court determined that bank records (i.e., deposit slips and monthly statements) were "business records of the banks"[5] and not entitled to Fourth Amendment protection. This doctrine was later affirmed in *Smith v. Maryland*,[6] when the Court determined that the government's use of a pen register (a device that records outgoing phone numbers dialed on a landline) was not a search and thus not subject to the protection of the Fourth Amendment.

As technology has evolved, however, the continuing viability of the third-party doctrine has come into question, and *Carpenter* has unquestionably advanced the process of reconciling it with the new reality of third-party possession of extensive private information as a part of everyday life in the digital era. Both the majority of five justices and a dissenting Justice Gorsuch acknowledged that the nature of information that is now shared with third parties has qualitatively changed since *Miller* and *Smith*. The majority's opinion recognizes there has been a "seismic shift[] in digital technology"[7] and "in no meaningful sense does the user 'assume the risk.' "[8] Following this reasoning, the majority implies that Fourth Amendment protection should no longer end simply because information is shared with third-parties, but rather should be based on the totality of circumstances, including but not limited to the content of the communication, where the information resides, and who has access to it, such as a private third-party.

Justice Gorsuch's dissent describes how categorically classifying information disclosed to a third-party as automatically devoid of Fourth Amendment protection is unrealistic in today's modern world. He specifically outlines how individuals still have (and should have) an expectation of privacy in certain information shared with third-parties, such as private e-mails on third-party e-mail services, DNA information with a genetic testing company or a private letter entrusted to a close confidant. Indeed, Justice Gorsuch appears to question the reasoning and validity of the third-party doctrine in its entirety, noting that "[c]onsenting to give a third party access to private papers that remain my property is not the same thing as consenting to a *search of those papers by the government*." [9]

[3] *Carpenter,* 585 U.S. at ___ (slip op., at 4).

[4] 425 U.S. 435 (1976).

[5] *Id*. at 440.

[6] 442 U.S. 735 (1979).

[7] *Carpenter*, 585 U.S. at ___ (slip op., at 15).

[8] *Id.*, at ___ (slip op., at 17).

[9] *Id.*, at ___ (slip op., at 5) (Gorsuch, J. dissenting) (emphasis in original).

Carpenter Follows Recent Trend Expanding Scope of Fourth Amendment Protection to Modern Technology

Carpenter takes a broad view of the scope of the Fourth Amendment and its application to technology, in line with the Court's recent trend of extending Fourth Amendment protections to new categories of information in response to evolving technology. For instance, in *United States v. Jones*,[10] the Court unanimously held – for varying reasons – that placing a GPS tracking device on a suspect's vehicle to track its whereabouts without a warrant violated the Fourth Amendment. Justices Sotomayor and Alito filed concurrences that GPS tracking of a suspect's vehicle violated an individual's reasonable expectations of privacy and therefore constituted a search warranting Fourth Amendment protection.

Similarly in *Riley v. California,*[11] the Court unanimously held that law enforcement could not search the contents of a suspect's cell phone without a warrant. The Court's opinion noted that cell phones contain "the privacies of life"[12] for most Americans and merit Fourth Amendment protection. Justice Alito again filed a concurrence noting that the quantity and quality of information that can be stored on cell phones, "some highly personal," "calls for a new balancing of law enforcement and privacy interests."[13]

Relying on *Jones* and *Riley*, the majority in *Carpenter* concluded that a person has a "reasonable expectation of privacy in the whole of their physical movements." The Court recognized that wireless carriers' CSLI is a "sweeping mode[] of surveillance"[14] that is "detailed, encyclopedic, and effortlessly compiled,"[15] effectively giving the government "near perfect surveillance, as if it had attached an ankle monitor to the phone's user."[16]

Carpenter is both an affirmation of *Riley* and the Court's awareness of the immense amount of private information that may be stored within cell phones. It also opens the door to a myriad of new challenges to determine where Fourth Amendment protections may apply in the context of obtaining an individual's business records held by a third-party. The majority in *Carpenter* affirmed the Court's prior rulings in *Miller* and *Smith* and did not hold that access to CSLI itself always requires a warrant – only that the government will now need a warrant to download four months of systematic tracking of an individual's whereabouts.

[10] 565 U.S. ___ (2012).
[11] 573 U.S. ___ (2014).
[12] *Id*., at ___ (slip op., at 28).
[13] *Id*. at ___ (slip op., at 4) (Alito, J., dissenting).
[14] *Carpenter*, 585 U.S. at ___ (slip op., at 10).
[15] *Id*. at ___ (slip op., at 13).
[16] *Id*.

Justice Alito May be the New "Swing Voter" for Fourth Amendment Challenges

As we assess the future scope of the Fourth Amendment and its impact on data privacy, the changing composition of the Court will have an undeniable impact. Recent opinions do not readily lend themselves to a scorecard of liberal versus conservative views. Instead, the Court appears to be incrementally and cautiously considering the scope of constitutional protections as it grapples with the pervasive use of technology in our daily lives. While it is difficult to predict where these trends will lead, Justice Alito is emerging as a compelling guidepost in reconciling the Fourth Amendment with technology and data privacy in the modern era.

Indeed, Justice Alito could become the Court's swing vote on the scope of Fourth Amendment privacy protections. Although Justice Alito joined unanimous pluralities in *Jones* and *Riley*, his concurrences in each opinion made clear his competing concerns between re-drawing historical constitutional precedent and a reasonable expectation of privacy in an evolving technological world.

Dissenting in *Carpenter*, Justice Alito takes a unique approach in assessing CSLI, extensively examining the historical precedent distinguishing between a physical and constructive search of an individual's effects. Justice Alito takes the view that CSLI is the property of a third-party, that a document subpoena directed to a third-party does not involve a physical intrusion into a private space or taking of property, and therefore does not constitute a search.

Relying upon a series of cases dating from *Oklahoma Press Publishing Company v. Walling*,[17] Justice Alito contends that a search of a third-party's records is not an "actual search" of an individual and therefore is not subject to the Fourth Amendment's warrant requirement. His dissent in *Carpenter* takes a markedly different approach than his concurrences in *Jones* and *Riley*, which evaluated the omnipresent nature of digital technology in our daily lives and the information we entrust to it. In *Carpenter*, Justice Alito instead focuses on whether information entrusted to a third-party is entitled to Fourth Amendment protection.

As technology changes, however, Justice Alito and the rest of the Court will undoubtedly have to continue reassessing what

[17] 327 U.S. 186 (1946).

constitutes a search, especially as information is processed and consolidated by private entities. Justice Alito himself recognizes that "some of the greatest threats to individual privacy may come from powerful private companies that collect and sometimes misuse vast quantities of data about the lives of ordinary Americans."[18] This concern is especially prescient as it was recently reported[19] that AT&T – which recently merged with Time Warner – is partnered with the National Security Agency to utilize its massive infrastructure to allow the NSA to monitor billions of e-mails, phone calls, and online chats passing through the United States.

Despite this concession, Justice Alito affirms that it is the legislature, not the judiciary, which must protect individual privacy, and prefers that the SCA be applied in its current form until modified by Congress. This position somewhat varies with his concurrence in *Jones*, which observed that courts "should not mechanically apply the rule used in the predigital era to the search of a cell phone"[20] and that because cell phones "are capable of storing and accessing a quantity of information, some highly personal, . . . "[t]his calls for a new balancing of law enforcement and privacy interests."[21] Justice Alito's strict constructionist approach to the Stored Communications Act in *Carpenter* should be juxtaposed with his reasoning in *Jones* and *Riley* that signaled he is aware of today's technological privacy challenges.

Future Implications

The growing amount of personal information that is processed and stored by private third-parties will likely become an immense battleground as litigants in civil and criminal cases seek to challenge efforts to obtain information from our digital profile that is collected, stored, and analyzed by wireless carriers and mobile applications for the features we use every day. As privacy professionals, we can only hope that the Court will take seriously its recognition "that CSLI is an entirely different species of business record—something that implicates basic Fourth Amendment concerns about arbitrary government power much more directly than corporate tax or payroll ledgers."[22]

The scope of *Carpenter's* holding and the Court's application of the Fourth Amendment to digital technology may be tested sooner than we anticipate. The majority in *Carpenter* recognizes the immense amount of information entrusted to digital technology and seeks to determine the boundaries of Fourth Amendment protections. Even in dissent, Justice Alito recognizes that "[l]egislation is much preferable"[23] to developing Fourth Amendment protections than judicial intervention, and Justice Gorsuch further opines that the information individuals share with third-parties "might even rise to the level of a property right." [24]

These opinions may soon be tested as pro-privacy legislation, like California's recent Consumer Protection Act of 2018 or Europe's General Data Protection Regulation (GDPR), convey new rights to individuals, such as the right to be forgotten and the right to prevent the sale of consumer information. Will the Court recognize property interests in these new statutory protections? Will the Court enforce a penalty against a U.S. corporation for failing to comply with the GDPR's privacy requirements? These questions and others in the ever-changing privacy landscape remain unanswered.

It is therefore vital for privacy professionals to continue monitoring legislative developments and challenges to private interests, including the ability to enforce statutory privacy protections and defend against unwarranted intrusions. *Jones*, *Riley* and *Carpenter* provide an initial framework for such protections. As technology continues to become embedded in our daily lives and we expand the amount of information shared with technology platforms and suppliers, it will fall to privacy professionals and their clients to secure and enforce the protections they have been afforded by the Constitution.

---

[18] *Carpenter*, 585 U.S. at ___ (slip op., at 27) (Alito, J., dissenting).

[19] Ryan Gallagher & Henrik Moltke, *The Wiretap Rooms*, The Intercept (June 25, 2018, 7:00 a.m.), https://theintercept.com/2018/06/25/att-internet-nsa-spy-hubs/.

[20] *Riley*, 573 U.S. at ___ (slip op., 4) (Alito, J., concurring).

[21] *Carpenter*, 585 U.S. at ___ (slip op., at 27) (Alito, J., dissenting).

[22] *Id*. at ___ (slip op., at 20).

[23] *Id*. at ___ (slip op., at 27) (Alito, J., dissenting).

[24] *Id*. at ___ (slip op., at 21) (Gorsuch, J., dissenting).

Learn more...

For questions regarding this information or to learn more about how it may impact your business, please contact one of the authors, a member of our **Privacy and Cybersecurity** practice, or your Polsinelli attorney.

To learn more about our **Privacy and Cybersecurity** practice, or to contact a member of our **Privacy and Cybersecurity** team, visit https://www.polsinelli.com/services/privacy-and-cybersecurity or visit our website at polsinelli.com.

About this Publication