8-26-2018

Fourth Amendment Protection in the Digital Age

Daniel Sorkin
Golden Gate University School of Law, lawreview@ggu.edu

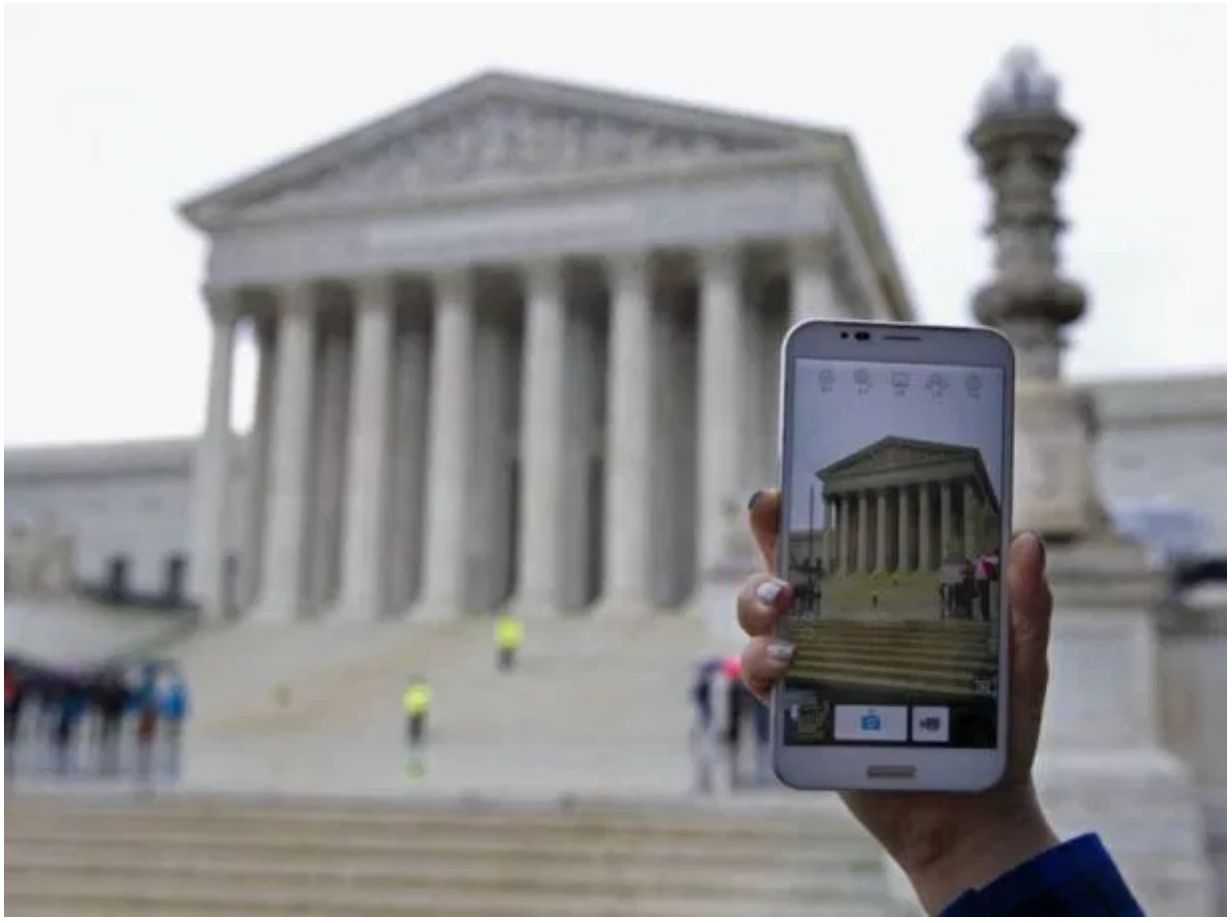
Golden Gate University Law Review

Fourth Amendment Protection in the Digital Age

PUBLISHED ON *August 26, 2018 by Daniel Sorkin*

During the course of an investigation into a series of armed robberies in Michigan and Ohio in 2010 and 2011 (http://www.scotusblog.com/wp-content/uploads/2016/10/16-402-cert-petition.pdf), the FBI submitted applications to three different magistrate judges for orders to access more than five months of historical cell phone location records for Timothy Carpenter. "But the data asked for and received weren't limited to the days and times of the known robberies—they included months of records that could reveal everywhere Carpenter was every time he made or received (http://www.scotusblog.com/wp-content/uploads/2016/10/16-402-cert-petition.pdf) a phone call." And the FBI obtained all of this information without (http://www.scotusblog.com/wp-content/uploads/2016/10/16-402-cert-petition.pdf) a warrant.

The Supreme Court granted certiorari in *Carpenter v United States*, a case that offers the Court another opportunity to address how far Fourth Amendment protections (http://www.scotusblog.com/2017/08/symposium-will-fourth-amendment-protect-21st-century-data-court-confronts-third-party-doctrine/) against warrantless searches and seizures extend. Specifically, the issue before the Court was "whether the warrantless seizure and search of historical cell phone records (http://www.scotusblog.com/wp-content/uploads/2016/10/16-402-cert-petition.pdf) revealing the locations and movement of a cell phone user over the course of 127 days is permitted by the Fourth Amendment."



On appeal before the Sixth Circuit, a divided three-judge panel held that "no search occurred under the Fourth Amendment because Carpenter had no reasonable expectation of privacy (http://www.scotusblog.com/wp-content/uploads/2016/10/16-402-cert-petition.pdf) in cell phone location records held by his service provider." The prosecution contended that cell-phone users "presumably understand that their phones convey data to their service providers as a necessary incident (http://www.scotusblog.com/wp-content/uploads/2017/02/16-402-BIO.pdf) of making or receiving calls."

Carpenter took a contrary position, arguing "magistrate judges have discretion (http://www.scotusblog.com/wp-content/uploads/2016/10/16-402-cert-petition.pdf) to require a warrant for historical data sought if they determine the location information will implicate the suspect's Fourth Amendment privacy rights." Carpenter cited a dissenting argument from the Third Circuit, which proposed:

A cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way. . . . [I]t is unlikely that cell phone customers are aware that cell phone providers collect and store historical location information. Therefore when a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed and there is no indication to the user that making that call will also locate the caller; when a cell phone user receives a call, he hasn't voluntarily exposed anything at all (http://www.scotusblog.com/wp-content/uploads/2016/10/16-402-cert-petition.pdf).

Carpenter further relied on Justice Sotomayor's explanation that "electronic location tracking implicates the Fourth Amendment because it generates a precise, comprehensive record of a person's public movements (http://www.scotusblog.com/wp-content/uploads/2016/10/16-402-cert-petition.pdf) that reflect a wealth of detail about his/her familial, political, professional, religious, and sexual associations."

Nonetheless, the Sixth Circuit majority agreed with the prosecution (http://www.scotusblog.com/wp-content/uploads/2016/10/16-402-cert-petition.pdf) and held that the fact the government obtained the cell site date from Carpenter's service provider, rather than from Carpenter himself, defeated his Fourth Amendment claim. On appeal to the Supreme Court, Carpenter asserted the weight of authority relied on by the Sixth Circuit, which elucidated the third-party doctrine, never treated "third party access to the records as dispositive (http://www.scotusblog.com/wp-content/uploads/2016/10/16-402-cert-petition.pdf)." "The mere fact that another person or entity had access or control over private records does not in itself—and without regard to any other circumstance—destroy an otherwise reasonable expectation of privacy (http://www.scotusblog.com/wp-content/uploads/2016/10/16-402-cert-petition.pdf)." Carpenter acknowledged that third-party access to records might indeed be "one factor weighing on the reasonable-expectation-of-privacy standard (http://www.scotusblog.com/wp-content/uploads/2016/10/16-402-cert-petition.pdf)." But Carpenter alleges *Miller* (https://supreme.justia.com/cases/federal/us/307/174/case.html) and *Smith* (https://supreme.justia.com/cases/federal/us/442/735/case.html), which predominantly outlined the basis of the third-party doctrine (http://www.scotusblog.com/wp-content/uploads/2016/10/16-402-cert-petition.pdf), did not intend for it to be treated as "an on-off switch."

In concluding that the Fourth Amendment does not protect people's cell site location records from warrantless searches, the Sixth Circuit relied on the Stored Communications Act (http://www.scotusblog.com/wp-content/uploads/2016/10/16-402-cert-petition.pdf). The court believed that the elected representatives in Congress had already struck a reasonable balance (http://www.scotusblog.com/wp-content/uploads/2016/10/16-402-cert-petition.pdf) between privacy protection and public safety. Carpenter further alleged that the legislation was decades old and was passed before the "proliferation of cell phones (http://www.scotusblog.com/wp-content/uploads/2016/10/16-402-cert-petition.pdf) and the availability of increasingly precise cell site location information."

Carpenter requests that the Supreme Court define the scope (http://www.scotusblog.com/wp-content/uploads/2016/10/16-402-cert-petition.pdf) of Fourth Amendment protection for newer forms of sensitive digital data or, at least in part, address the expansive application of the "third-party doctrine beyond the kinds of records at issue in *Miller* (https://supreme.justia.com/cases/federal/us/307/174/case.html) and *Smith* (https://supreme.justia.com/cases/federal/us/442/735/case.html)." He claims the Sixth Circuit erred in not relying on a totality of the circumstances (http://www.scotusblog.com/wp-content/uploads/2016/10/16-402-cert-petition.pdf) approach in their deliberation and that the Supreme Court should find his cell site location data be protected by the Fourth Amendment's warrant requirement.

Oral arguments (http://www.scotusblog.com/wp-content/uploads/2016/10/16-402-op-bel-6th-cir.pdf) were heard before the Supreme Court on November 29, 2017. Opinion by the Supreme Court (http://www.scotusblog.com/wp-content/uploads/2016/10/16-402-op-bel-6th-cir.pdf) has not yet been filed. The Supreme Court's decision on this case could potentially mean a substantial increase in warrant applications—"in 2016 Verizon and AT&T alone received about 125,000 cell site location requests (http://www.scotusblog.com/2017/08/symposium-will-fourth-amendment-protect-21st-century-data-court-confronts-third-party-doctrine/)." How the Supreme Court decides this case will have important implications, especially where "sensors and devices in our homes, cars (http://www.scotusblog.com/2017/08/symposium-will-fourth-amendment-protect-21st-century-data-court-confronts-third-party-doctrine/), and throughout our world will constantly collect, generate, and share data about us with little to no willingness on our part."

The Electronic Frontier Foundation (http://www.scotusblog.com/2017/08/symposium-will-fourth-amendment-protect-21st-century-data-court-confronts-third-party-doctrine/) and many others have argued it is time for the Supreme Court to revisit this outdated doctrine. A few of the considerations offered (http://www.scotusblog.com/2017/08/symposium-will-fourth-amendment-protect-21st-century-data-court-confronts-third-party-doctrine/) in support of this argument include the idea that "patients have a reasonable expectation of privacy in diagnostic test results, even when the hospital maintains the records, … and hotel guests are entitled to protections even though they provide implied or expression permission for third parties to access their rooms." Similarly, the Sixth Circuit has ruled in the past that people have an "expectation of privacy in email content (http://www.scotusblog.com/2017/08/symposium-will-fourth-amendment-protect-21st-century-data-court-confronts-third-party-doctrine/) even if they use a third-party service provider to transmit that email." Thus, the primary hurdle for the Supreme Court in *Carpenter* will be to determine how to reset the boundaries of the third-party doctrine (http://www.scotusblog.com/2017/08/symposium-will-fourth-amendment-protect-21st-century-data-court-confronts-third-party-doctrine/) in an age where people rely on technology.

CATEGORIES GGU LAW REVIEW