HWG | HARRIS, WILTSHIRE & GRANNIS LLP

ADVISORY

June 25, 2018

Supreme Court's Decision in *Carpenter v. United States* Shifts Third Party Doctrine, With Potential Ripple Effects

Adrienne E. Fowler and Lauren Snyder

The decision

On Friday, the Supreme Court issued a 5-4 decision in *Carpenter v. United States*, a watershed case in privacy law. The Court held the government generally needs a warrant to access historical cell phone records that chronicle a user's movement because "an individual maintains a legitimate expectation of privacy in the record of his physical movements" captured through cell phone location information. The FBI had obtained location information from Carpenter's cell phone provider that spanned 127 days. Chief Justice Roberts, writing for the majority, analogized tracking a user's cell phone to attaching an ankle monitor to the user.

The Court rejected the government's primary argument, which was based on the "third party doctrine"—the idea that an individual has no expectation of privacy in information he or she voluntarily discloses to a third party. Here, the information came from business records containing data Carpenter had voluntarily shared with his wireless carrier. Because cell phones are "indispensable to participation in modern society," and a cell phone logs information "without any affirmative act on the part of the user beyond powering up," Roberts concluded that "in no meaningful sense does the user voluntarily assume the risk of turning over a comprehensive dossier of his physical movement." Nonetheless, the Court emphasized that its decision was limited to cell phone tracking information collected by cell phone carriers, and the decision does not extend to conventional surveillance techniques or other business records that might incidentally reveal location information. Justices Anthony Kennedy, Samuel Alito, Clarence Thomas, and Neil Gorsuch each wrote a dissenting opinion, criticizing the new standard as unworkable.

What now?

Wireless providers and other companies who receive law enforcement demands for location information: Before *Carpenter*, the government only needed to show that there were "reasonable grounds" to believe the cell phone records were relevant and material to an ongoing criminal investigation before a court could issue an order requiring electronic communication service or remote computing service providers to release cell phone location information and similar records pursuant to the Stored Communications Act, 18 U.S.C. §2703(d). Those providers can no longer release cell phone location information unless the government obtains a warrant. Cell phone providers will likely need to revise their law enforcement compliance guides and internal compliance policies because, in light of *Carpenter*, "[a]n order issued in Section 2703(d) is [no longer] a permissible mechanism for accessing historical cell-site records." Other types of companies that offer electronic communications or remote computing services covered by the Stored Communications Act—e.g., cloud service providers, mobile email apps—should also carefully consider how to approach law enforcement requests for user location information.

Criminal defendants: The government must now have the requisite probable cause—as opposed to merely showing that the evidence might be relevant to an ongoing investigation—to obtain a warrant before requesting cell phone location records from providers. Any criminal defendant whose cell phone

records were obtained without a warrant may now have grounds to suppress that evidence—and potentially have a plausible argument to suppress location information collected without a warrant from other types of companies that offer electronic communications or remote computing services covered by the Stored Communications Act.

Big picture: The *Carpenter* decision, at the very least, continues the Supreme Court's trend toward protecting personal cell phone data that began with *Riley v. California* (2014), in which the Court held that police generally needed a warrant to search a cell phone obtained from a person who had been arrested. *Carpenter* also furthers the trend toward protecting individual privacy, particularly in the contexts of Big Data and location information. *Carpenter* may provide persuasive support (at both the state and federal levels) for legislators, regulators, consumer groups, and companies seeking to limit government and private sector access to compilations of data that reveal intimate details about Americans' everyday lives.

* * *

For more information regarding the decision, privacy, law enforcement access to information, or our criminal defense practice, please contact afowler@hwglaw.com, lsnyder@hwglaw.com, or the HWG lawyer with whom you regularly work.

This regulatory advisory is not intended to convey legal advice. It is circulated to HWG clients and friends as a convenience and is not intended to reflect or create an attorney-client relationship as to its subject matter.