THE
NATIONAL LAW REVIEW

Supreme Court Takes Another Step to Keep Up With the Digital Times: Criminal Procedure and Cell Phone Records in Carpenter

Sunday, July 8, 2018

Personal location information held by a third party now receives heightened protection from disclosure to law enforcement

Article By Robin B. Campbell
Tara M. Swaminatha Thomas E. Zeno
Katherine A. Spicer
Squire Patton Boggs (US) LLP
SECURITY & PRIVACY // BYTES
Communications, Media & Internet
Criminal Law / Business Crimes
Constitutional Law
Litigation / Trial Practice
All Federal

Thanks to Timothy Ivory Carpenter, Cell Site Location Information ("CSLI") is now part of our vernacular. More important, in light of the Supreme Court's June 2018 ruling in *Carpenter v. United States*, a company's collection and retention of a person's historical whereabouts (location information) now receives heightened protection from search and seizure by law enforcement.

Simply put, CSLI is a personal location record created when a cell phone connects to a nearby cell tower site. In *Carpenter*, the government received 127 days of Mr. Carpenter's CSLI without a warrant.[1] This data made it possible for law enforcement agents to recreate Mr. Carpenter's daily whereabouts over a four-month period with granular precision unlike other surveillance means available (i.e., store video cameras or witness recollection). At trial, the government offered this data as corroborating evidence to place Mr. Carpenter near the location of four of the charged robberies around the time those four robberies were committed. Mr. Carpenter was convicted and sentenced to nearly 116 years' of imprisonment.

The collection of this data makes "it possible to reconstruct in detail everywhere an individual has traveled over hours, days, weeks, or months."[2] As Chief Justice Roberts plainly states, "*the question [confronted] today is how to apply the Fourth Amendment to a new phenomenon: the ability to chronicle a person's past movements through the record of his cell phone signals*."

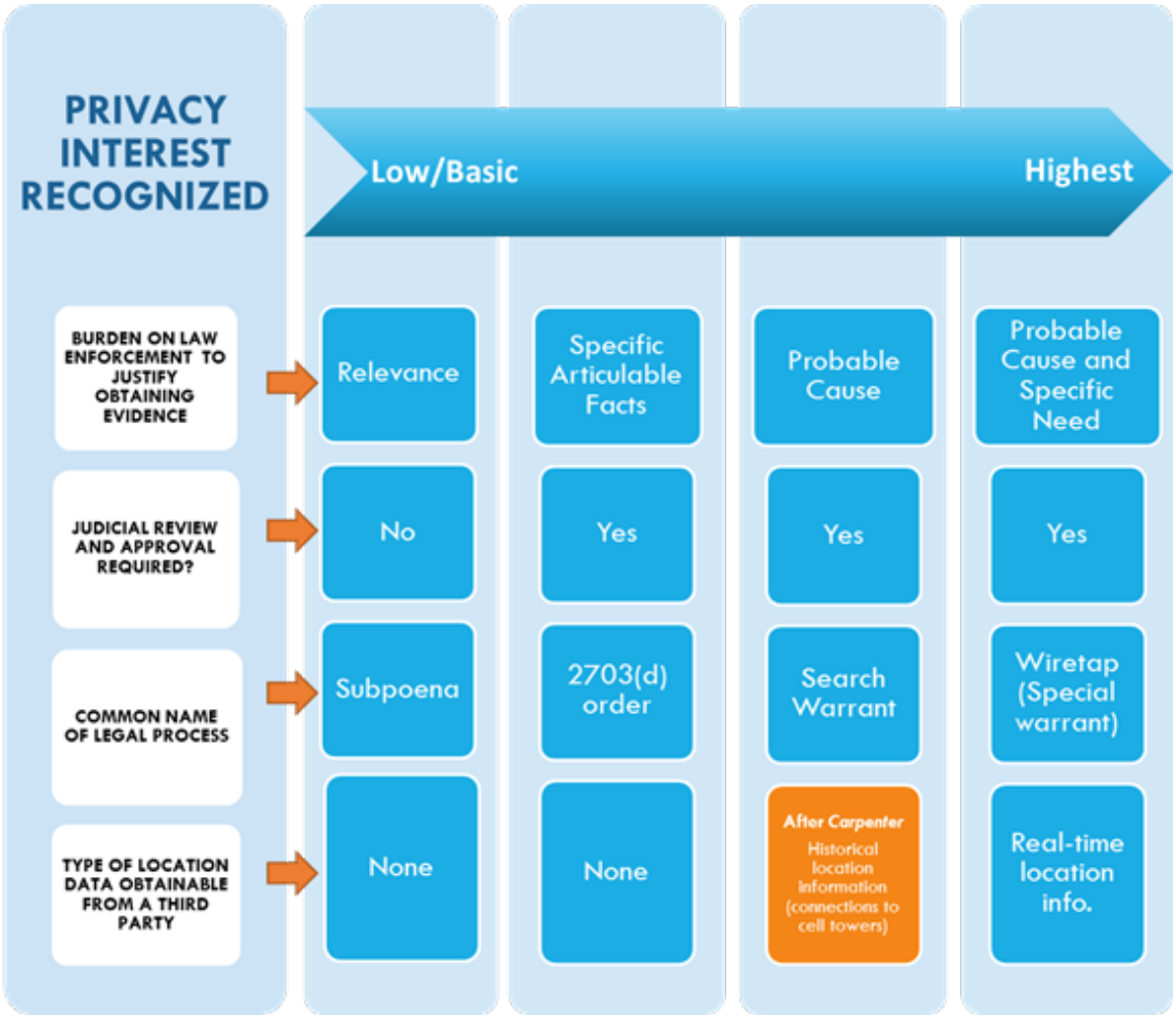
Before *Carpenter*, CSLI data held by a third party was considered simply a business record that did not require a search warrant. That has changed. Now, acquisition of CSLI I is "a search within the meaning of the Fourth Amendment."[3] Because an individual maintains a legitimate expectation of privacy in CSLI data, "the Government must generally obtain a warrant supported by probable cause before acquiring such records."[4]

Legitimate Reasons for Collecting or Disclosing CSLI

While your historical location data may seem like a futuristic big-brother phenomenon, providers collect this type of information to manage bandwidth and capacity, ensure quality of service and other benign purposes. Historical location information can be instrumental in law enforcement putting individuals near the scene of a crime at the time it occurred or meeting with co-conspirators at a weapons store. Location records can also be exculpatory evidence, such as proving a person was *not* near the scene of a crime when it happened, or never visited a location law enforcement believes to be important in proving the case.

Carpenter, Heightened Privacy Interests and Law Enforcement Burden to Justify Obtaining Location Information

Carpenter altered a long-standing practice of criminal procedure. The higher the privacy interest recognized in certain information (evidence) sought, the higher the burden on law enforcement to be able to obtain the evidence. For example, obtaining name, address and account number receive lower protection and require only a subpoena based on a law enforcement officer's belief that information sought is related to an ongoing criminal investigation, without much more. On the other hand, obtaining real-time location information and content of communications (i.e., a wiretap) receive some of the highest protections. (See chart below.)
Under *Carpenter*, historical location records carry a heightened privacy interest. Law enforcement can no longer obtain historical location records by using a simple subpoena.



Carpenter – next in a line of Fourth Amendment cases finding heightened privacy interests in certain digital personal information

As digital technology continues to advance, courts will continue to wrestle with the Fourth Amendment implications. In fact, two prior Supreme Court decisions about emerging technologies shaped the *Carpenter* decision:

In 2012, in a marked departure from long-standing precedent, the Court decided *United States v. Jones.* In *Jones*, the FBI attached a GPS device to a suspect's vehicle without a warrant. As a result, the government was able to remotely monitor Mr. Jones whereabouts for 28 days. The Court held that even though vehicular movements are disclosed to the public at large, individuals still have a reasonable expectation of privacy in their long-term whereabouts. As such, the government must obtain a warrant before it uses this type of technology to surveil suspects.

Two years later, the Court was called upon to answer the privacy interests raised by a "feature of human anatomy," the cell phone.[5] In *Riley v. California*, the government did not obtain a warrant before it searched Mr. Riley's cell-phone incident to his arrest. Further departing from decades-old exception to the search warrant requirement, the Court held that the unique capacity of cell phones and their ability to contain every intimate detail of a person's life trigger a privacy interest in a person's cell phone stored contents and data. As a result, police officers must generally obtain a warrant before searching a cell phone incident to an arrest.

How Carpenter Will Impact Many Organizations

Although *Carpenter* changes law enforcement investigative techniques, the decision also signals technology providers to consider changing their practices. According to the Amici Curiae brief filed by technology companies:

> Amici have a substantial interest in the legal standards governing law-enforcement access to data about their customers. Those customers entrust amici with some of their most intimate information, including what they search, where they are, and details of their daily lives. Given the sensitivity of this data, amici work continuously to secure their customers' privacy.

Undoubtedly in the coming months, organizations that record and store information about individuals' whereabouts, e.g., cell phone providers, internet service providers, fleet monitoring service providers, GPS and smart car services may consider re-examining their data retention policies, privacy policies and focusing closely on their subpoena and warrant compliance practices in light of *Carpenter*. Our teams collaborate to help organizations review internal procedures in light of this ruling.

[1] In *Carpenter*, the government did obtain an order under the Stored Communications Act ("SCA"). To obtain an order under the SCA, the government need not show probable cause. Instead, it needs only to "offer[] specific and articulable facts showing that there are reasonable grounds to be that . . . the records or other information sought[] are relevant and material to an ongoing criminal investigation." 18 U.S.C. 2703(d). For *Carpenter*, the government mentioned Mr. Carpenter's name "only once in a conclusory sentence at the end" of its application. Trn. of Oral Argument at 22:1-3.

[2] Pet. Brief at 3.

[3] *Carpenter v. United States*, 585 U.S. __, ___ (2018) (slip op., at 17).

[4] Id. at 18.

[5] *Riley v. California*, 573 U.S.__, __ (2014) (slip op., at 9).