United States Supreme Court Issues Important Privacy Ruling in Carpenter

June 22, 2018

What happened?

The United States Supreme Court held today that the Constitution protects individual geolocation data maintained by phone carriers. This cell-site data, gathered from the pinging of cell phones to nearby towers, gives "the Government near perfect surveillance and allow it to travel back in time to retrace a person's whereabouts, subject only to the five-year retention policies of most wireless carriers." *Carpenter v. U.S.*, No. 16-402, 585 U.S. ___ at *13 (June 22, 2018).

In a 5-4 decision, the Court determined that the Government should have obtained a 4th Amendment search-and-seizure "probable cause" warrant before acquiring alleged robber Timothy Carpenter's cell-site records from MetroPCS and Sprint, rather than just a court order based on "reasonable grounds" his records were "relevant and material to an ongoing investigation" under the Stored Communications Act. In an interesting mix, Chief Justice Roberts wrote for the majority joined by Justices Ginsburg, Breyer, Sotomayor and Kagan.

Why should I care about the cell phone records of a robbery suspect in a criminal case?

Carpenter sheds important light on how the federal government will treat the constant and enormous volumes of digital data thrown off by Americans. This data reveals our web browsing, retail purchases, driving habits, daily steps, heart rates, music, television and news preferences, and nearly every other aspect of our lives. In most instances, this valuable data is exchanged in the terms of use of a website or service, or for some other convenience. *Carpenter* explains what individual expectation of privacy is reasonable under these circumstances.

In dissent, Justice Kennedy argued that "[c]ustomers….do not own, possess, control, or use the [cell-site] records, and….have no reasonable expectation…they cannot be disclosed pursuant to lawful compulsory process." Chief Justice Roberts and the *Carpenter* majority rejected the argument that "cell-site records are fair game because they are 'business records' created and maintained by the wireless carriers," and given by voluntary consent. *Id*. at 15. The Chief Justice wrote:

> Virtually any activity on the phone generates [data], including incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates. Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily "assume[] the risk" of turning over a comprehensive dossier of his physical movements.

Id. at 17. Thus, Carpenter indicates that personal data like cell-site geolocation falls within the penumbra of privacy under the Constitution because of "its depth, breadth and comprehensive reach" and "the inescapable and automatic nature of its collection." *Id*. at 20.

How does enhanced protection of individual location data affect US businesses?

The EU and much of the rest of the world already treats personal data protection as a fundamental human right, as illustrated by the EU General Data Protection Regulation that became effective on May 25, 2018. Facebook, for example, is facing questions and litigation on both sides of the Atlantic arising from the disclosure of "friends'" personal data to third party applications, including that of election consultant Cambridge Analytica.

Carpenter reflects a trend toward a greater expectation of privacy for Americans' personal data. To that end, one can expect state attorneys general and consumers to scrutinize the reasons and consents obtained for collection of such data. American businesses should continue to treat personal data as an extremely valuable business asset, but recognize that transparency and security in the handling and use of such data can have a profound effect on the bottom line.

What should a business do in light of *Carpenter* and other privacy protections?

Take stock of all the personal data in your possession, particularly sensitive information regarding location, financial accounts or health. Be prepared to explain your reasons for collecting it, the measures you take to protect it, and have a plan for responding to demands by law enforcement or third party litigants for access to it. To ignore these issues is to put in peril your ability to use the data upon which most businesses and our economy now relies.

Let the cybersecurity/data privacy professionals at Lathrop Gage, Tedrick Housh and Jason Schwent, assist you with any of your data compliance questions or concerns.
