You're Gonna Need a Warrant for That....

Prepared by:
Rosemary McKenna
Jackson Lewis P.C.

LORMAN
Published on www.lorman.com - September 2018

INTRODUCING

Lorman's New Approach to Continuing Education

ALL-ACCESS PASS

The All-Access Pass grants you UNLIMITED access to Lorman's ever-growing library of training resources:

- ☑ **Unlimited Live Webinars** - 120 live webinars added every month
- ☑ **Unlimited OnDemand and MP3 Downloads** - Over 1,500 courses available
- ☑ **Videos -** More than 1300 available
- ☑ **Slide Decks -** More than 2300 available
- ☑ White Papers
- ☑ Reports
- ☑ Articles
- ☑ ... and much more!

Join the thousands of other pass-holders that have already trusted us for their professional development by choosing the All-Access Pass.

Get Your All-Access Pass Today!

SAVE 20%

Learn more: www.lorman.com/pass/?s=special20

Use Discount Code Q7014393 and Priority Code 18536 to receive the 20% AAP discount.

*Discount cannot be combined with any other discounts.

You're Gonna Need a Warrant for That….

Written by Rosemary McKenna – 7/9/18

On June 22, 2018, in Carpenter v. United States, the United States Supreme Court decided that the federal government would need a warrant in order to obtain historical location data from cellular service providers, based on cell tower "pings." ("Pings" are more formally referred to as cell-site location information or "CLSI.") As explained in more detail below, the issue at the center of the controversy in the Carpenter case was whether an individual's personal location (as reflected in the CLSI) was private information protected by the Fourth Amendment, or whether any expectation of privacy was revoked because the location information was shared with the cell service provider when the individual's cell phone accessed different cell towers.
This decision was by a divided court (5-4), with four separate dissenting opinions (in other words, the Court had a lot to say on this).

A bit of background on the laws that were relevant to the Court in the Carpenter case (because the Magic 8 Ball is predicting that as technology continues to be a critical aspect of our personal and business lives, there will continue to be legal activity on the issue of what is private vs. what is shared). The Fourth Amendment of the U.S. Constitution provides protections to the people of the United States to "be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," and that "no warrants shall issue, but upon probable

cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

The Stored Communications Act ("SCA") is one of the titles included in the Electronic Communications Privacy Act ("ECPA"). The ECPA (including the SCA) was codified in 1986. At that point in time, most people didn't own cell phones, and if they did, they didn't turn them on. (I only carried mine as a potential means of defense, as it was substantial enough to knock out a potential attacker (without the screen breaking).) As the Carpenter decision notes, however, "[t]here are 396 million cell phone service accounts in the United States – for a Nation of 326 million people." While the SCA has been amended since 1986, it is difficult for statutory and case law to keep up with the lightning speed of technology.

The SCA makes it unlawful to access or disclose stored electronic communications records, unless the government compels such disclosure as allowed by the statute. Some of the ways the government may compel disclosure include through an issued warrant, an authorized administrative subpoena or a court order that shows "specific and articulable facts" that show the information may be relevant to a criminal investigation. See, 8 USC §2703.

Now on to the facts….the Carpenter case involved a criminal investigation by the FBI into a series of robberies in Detroit, Michigan. Federal judges issued court orders requiring two national cell phone providers to provide CLSI for incoming and outgoing calls, both for the time the call started, and the time the call ended. This CLSI placed Mr. Carpenter near four of the robberies, and he was charged and convicted.

The use of the CLSI in criminal investigations is where you see many of the cases on this type of issue; however, the rights of the government to

obtain these records – or other use of the records — could have other implications. For example, this information can be used for other helpful purposes, such as to locate missing children or abducted individuals, or to track and locate terrorism suspects. It has also been used for purposes of tracking the location of individuals in state income tax audits, in order to determine if statutory residency tests have been met (which can impact businesses due to the potential negative impact on C-level employees who reside in a state other than where their principal office is located).

The Supreme Court found that the CLSI information was "intimate" data, which does more than simply show movements, but also shows "'familial, political, professional, religious and sexual associations.'" Moreover, this type of data is more personal than GPS attached to a car, as it travels with the individual and therefore accompanies an individual to the residence, physician's office, and other "potentially revealing locations." And, because it is stored for years, it provides a chronicled history of an individual's actions (unlike a public viewing of someone, which is a one-time event). The Court found this to be significant because courts should consider what kind of information is sought in making a determination whether or not an individual would legitimately expect the information to be private.

This ruling, however, was expressly stated to have narrow application. The Court advised that it did not apply to other types of business records that may "incidentally" include location information, and may not even apply to protect all CLSI. The opinion of the Court noted "[t]he Government will be able to use subpoenas to acquire records in the overwhelming majority of investigations. We hold only that a warrant is required in the rare case where the suspect has a legitimate privacy interest in records held by a third party."

So, at this point, it seems clear that the FBI cannot access historical, chronicled, CLSI records such as those obtained for Mr. Carpenter, in a criminal investigation, without a warrant. But for all of the other potential uses of this type of data? That Magic 8 Ball is stuck on "Reply Hazy, Try Again."