Inquiry Into CI's Database Use Raises New Data Questions

Posted on Oct. 14, 2020
»
Learn more

By Nathan J. Richman

A letter from two senators asking about the IRS Criminal Investigation division's subscription to a commercial database including cellphone data provokes even more questions about how emerging technology interacts with the Fourth Amendment.

Senate Finance Committee ranking member Ron Wyden, D-Ore., and Sen. Elizabeth Warren, D-Mass., asked about CI's subscription to a database provided by Venntel Inc., but practitioners say consideration of the applicable constitutional right to privacy could implicate even more advanced emerging issues like big data collection, social media, and cryptocurrency blockchains.

Upon the senators' request, the Treasury Inspector General for Tax Administration has begun to look into CI's 2017-2018 Venntel subscription in light of the Supreme Court's 2018 ruling in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), because the commercial database included information from taxpayers' cellphones.

In *Carpenter*, the Supreme Court held that the FBI should have obtained a warrant before demanding cell site location information (CSLI) that wireless carriers keep for their own internal business use. The information request implicated the defendant's reasonable expectation of privacy in his physical movements because the CSLI could be used to retroactively track his location over a long period of time, according to the Court.

The senators' letter notes that Venntel sold CI information that could have been put to similar use. The Supreme Court's opinion noted the import of publicly shared information — a legal principle that allows law enforcement access to things like bank records without a warrant — but it distinguished CSLI based on the uniquely ubiquitous nature of mobile phone use in modern society.

Sanford J. Boxerman of Capes, Sokol, Goodman & Sarachan PC told *Tax Notes* that the Court's analysis of publicly shared information could have interesting applications in the pseudonymous world of cryptocurrencies. "Can you have a reasonable expectation of privacy on the blockchain when one of the distinguishing characteristics, and selling points, of the bitcoin blockchain is it's all a public ledger?" he asked.

Many cryptocurrencies, and certainly the current market leader, bitcoin, allow a form of identity masking but rely on blockchains as public ledgers that verify transactions and generate trust. CI has subscribed to a cryptocurrency tracing tool offered by Chainalysis Inc. since 2017.

Travis W. Thompson of Sideman & Bancroft LLP pointed out that social media sharing is likely easily distinguished from the CSLI at issue in *Carpenter*, explaining that even if it's done on a cellphone, there's clear intent to share when a post is made publicly viewable. That raises the question of how and where Venntel harvested the data in its database, he said.

A Search by Any Other Name

Jeffrey A. Neiman of Marcus Neiman Rashbaum & Pineiro LLP said it would be difficult for a defense attorney to assert a violation of a defendant's right to have a warrant issued for a Fourth Amendment search when CI peruses otherwise publicly available information. "However, as soon as CI avails itself to access of information beyond what is publicly, commercially available, the Fourth Amendment may very well be implicated" and the IRS may have to address section 6103 taxpayer privacy considerations, he noted.

Thompson said the propriety of CI's Venntel subscription may turn on both where the company got the data and what the agency planned to do with it. He noted the particular privacy right at issue in *Carpenter* was the defendant's historical location, so looking for suspects' locations would probably be constitutional searches. However, the Supreme Court attempted to couch its opinion as narrowly applying to historical CSLI, he added.

Thompson also wondered what a court applying *Carpenter* would think about information harvested from an app that required the user to share information as a condition of use. He said a different question arises if CI is simply feeding the Venntel data into one of its data analytics programs in search of potential suspects, instead of following an existing suspect.

The specific procedures and timing of CI's subscription to Venntel also matter given that the agency's subscription ended in the year the Supreme Court released its decision in *Carpenter*, according to Thompson.

Boxerman said his initial reaction to the idea of a commercial database subscription was that it's unlikely to be a search under the Fourth Amendment. But a close reading of *Carpenter* shows that the key question would be the defendants' expectation of privacy, rather than the government's method of obtaining the relevant data, he added.

Whether and to what extent Venntel anonymized its data would also matter for the question whether CI needed a warrant for the subscription, Boxerman said.

With all of those questions in mind, the senators' inquiry is certainly important, but the idea that CI violated the rule from *Carpenter* is hardly obvious, Boxerman said, although they are asking the right questions, he added.