Utah Warrant Bill Raises Stakes For Cops' Digital Data Grabs

Link: https://www.law360.com/technology/articles/1151791/utah-warrant-bill-raises-stakes-for-cops-digital-data-grabs

Law360 (April 23, 2019, 9:30 PM EDT) -- A new Utah law that forces police to obtain a warrant before they can gain access to any person's electronic data could have implications far beyond law enforcement, including for how employers and big tech companies respond to police demands for data.

House Bill 57 was signed into law late last month and is set to go into effect in May. The law goes against the third-party doctrine, a 1970s-era legal principle that states people who voluntarily give their personal information to banks, phone companies or internet service providers can't reasonably expect that information to stay private.

The U.S. Supreme Court has started to chip away at that notion in recent years with decisions finding that historical cellphone location records and other narrow categories of sensitive data are entitled to greater privacy protections. But the new Utah law goes a step further by making individuals the owners of their data, not the companies they work for or the digital platforms — such as Google, Facebook and Microsoft — to which they entrust that data.

Aside from limiting police authority, the Utah law will likely change the dynamics for any company, including employers, that gathers and stores people's data. And the first-of-its-kind law, enacted in a Libertarian-leaning state and inspired by several critical recent Supreme Court decisions, reflects a legislative recognition of individual privacy rights that is likely to be replicated in other state houses, experts say.

"Given the breadth of what's covered by this law and how high the bar now is to get any of this digital information, this new law sets a significant precedent, and the possibility or even likelihood of copycat legislation in other states certainly can't be ruled out," said Robert Cattanach, a former federal prosecutor who is now a partner at Dorsey & Whitney LLP.

States have been increasingly active on the privacy front, with California last year enacting the first U.S. state law to regulate how online companies use, share and sell consumer data and more than a dozen states currently considering similar laws. But none has yet ventured into the territory covered by the Utah law.

"The Utah law has shifted the privacy conversation from protecting an individual's private information from private industry — such as the large tech firms — to protecting it from law enforcement," said Craig A. Newman, a partner with Patterson Belknap Webb & Tyler LLP and

chair of the firm's privacy and data security practice. "By any measure, this is landmark legislation because it protects electronic information that individuals turn over and entrust to third parties."

Under the federal Stored Communications Act, prosecutors must obtain a search warrant for digital data that is less than 180 days old but can obtain information that has been in storage for longer than that using a subpoena or court order, which have lower evidentiary burdens than warrants.

The Utah law removes the 180-day rule — which the federal government rarely uses anymore in the wake of the Sixth Circuit's 2010 decision in U.S. v. Warshak , but which Congress has yet to formally strike down — and in the process establishes a higher standard for state law enforcement officers seeking email, location data and other digital records from service providers.

"This is part of a broader trend that we're seeing in the legislative and judicial arenas to really sort of define the parameters of cyber investigations in terms of what's available to law enforcement and under what standard," said Edward McAndrew, a DLA Piper partner and former federal cybercrime prosecutor. "As the Supreme Court has said, digital is different, and I think this is a recognition of that, at least by one state."

The law is also likely to have sweeping implications on how law enforcement gathers data from employers, which have traditionally viewed worker data as company property and have had broad leeway in deciding whether to share this information with law enforcement, Cattanach noted. But the Utah law "turns that 180 degrees" by saying that employees own this information and that the government needs a search warrant to access it, he said.

"That's way more aggressive than any judicial precedent we've seen from the Supreme Court under the Fourth Amendment," he said. "The practical effect for Utah employers is almost to slam the door on any cooperation with law enforcement for employee data unless it's accompanied by a search warrant, and that's a pretty big sea change."

The Utah law's high threshold for obtaining these records is almost certain to narrow the universe of information that state law enforcement are able to obtain in cybercrime, stalking, child exploitation, employee theft and a range of other criminal matters where this digital data is vital, given that they typically use this information to build probable cause to obtain a more targeted search warrant down the line.

"An investigation is like a jigsaw puzzle where sometimes the pieces fit together and sometimes they don't," Cattanach said. "So on its face, this warrant requirement is a pretty major hurdle for law enforcement, and one that could end up really changing how they conduct their business."

The statute additionally requires law enforcement to "destroy in an unrecoverable manner" the data it obtains "as soon as reasonably possible after the electronic information or data is collected." This mandate is not found in federal law and is likely to prompt legal challenges about what constitutes a "reasonable" period of time for the government to hold on to seized data, according to McAndrew.

"Data seized for one type of investigation can sometimes end up being helpful in a different, wholly unrelated investigation months or years down the line, so I expect the question of whether the government held on to this information for too long to certainly be the subject of litigation," he said.

The law is also likely to ignite new disputes over how companies respond to data requests from state law enforcement, and from federal officials who are not bound by the same laws. Cattanach noted that the statute "raises more questions than it answers with regard to how it applies beyond the borders of Utah."

Businesses across the country will almost certainly need to revamp their procedures for responding to law enforcement data demands in the wake of the new warrant requirement, attorneys say.

"There's been so much focus on federal warrants and court orders and subpoenas, so one of the very important takeaways here for any electronic communications service or remote computing service is that they also need to be aware of and compliant with state laws popping up that may not be identical to the federal requests they're more familiar with," McAndrew said.

The passage of the Utah law, which was sponsored by Republican Rep. Craig Hall, comes on the heels of a series of Fourth Amendment decisions at the state and federal level attempting to set clear markers for law enforcement access to digital data, including several narrow rulings by the U.S. Supreme Court that have limited but not abolished the third-party doctrine.

In its June 5-4 decision in Carpenter v. U.S. , the high court rejected the government's argument that individuals don't have a legitimate expectation of privacy in the business records that third-party service providers make of the location of cell towers used to route calls to and from cellphones, instead finding that this information deserves more stringent protection than other customer information held by service providers.

The Carpenter ruling was in line with the high court's previous decisions in U.S. v. Jones and Riley v. California , which both endorsed similar privacy protections for the narrow categories of GPS tracking data and data stored in cellphones, respectively.

The Utah Legislature's decision to unanimously enact the new blanket warrant requirement for all digital records was almost certainly inspired by these court decisions as well as the greater attention being paid to personal privacy issues in general, according to legal observers.

"This seems to be very much an outgrowth of and a codification of what we've seen in terms of constitutional law developments related to the Fourth Amendment from the Supreme Court and others," McAndrew said. "The Supreme Court's word on these issues is something being raised in state courthouses across the country, and, as is often the case in response to judicial cases, we're seeing legislative action."

This movement is unlikely to be limited to Utah, with attorneys saying they wouldn't be surprised to see increasingly tech- and privacy-savvy lawmakers in other states soon follow the Beehive State's lead.

"This is front of mind for almost all state legislatures, so it's unlikely that this Utah bill is going to be just some one-off," Cattanach said.