

Utah Bans Police From Searching Digital Data Without A Warrant, Closes Fourth Amendment Loophole

Forbes.com

April 16, 2019

By Nick Sibilla

Alexa, get a warrant.

In a major win for digital privacy, Utah became the first state in the nation to ban warrantless searches of electronic data. Under the Electronic Information or Data Privacy Act (HB 57), state law enforcement can only access someone's transmitted or stored digital data (including writing, images, and audio) if a court issues a search warrant based on probable cause. Simply put, the act ensures that search engines, email providers, social media, cloud storage, and any other third-party "electronic communications service" or "remote computing service" are fully protected under the Fourth Amendment (and its equivalent in the Utah Constitution).

HB 57 also contains provisions that promote government transparency and accountability. In most cases, once agencies execute a warrant, they must then notify owners within 14 days that their data has been searched. Even more critically, HB 57 will prevent the government from using illegally obtained digital data as evidence in court.

In a concession to law enforcement, the act will let police obtain location-tracking information or subscriber data without a warrant if there's an "imminent risk" of death, serious physical injury, sexual abuse, livestreamed sexual exploitation, kidnapping, or human trafficking.

Backed by the ACLU of Utah and the Libertas Institute, the act went through five different substitute versions before it was finally approved—without a single vote against it—last month. HB 57 is slated to take effect in mid-May.

Ensuring that the Fourth Amendment is still relevant can sound like an obvious, common-sense reform (and it is). Yet Utah's new law is also a surprisingly radical break from the status quo. Thanks to the "third-party doctrine," in 49 states and on the federal level, the government can access a striking amount of private data without a search warrant, simply by working through third parties.

Back in the late 1970s, the U.S. Supreme Court issued a pair of decisions (*United States v. Miller* and *Smith v. Maryland*) that upheld the warrantless searches of bank records and dialed phone numbers. In both cases, the court ruled that the defendants' Fourth Amendment rights were not violated because they had no "legitimate expectation of privacy," since they had "voluntarily conveyed" the information at hand to third parties.

The third-party doctrine, in other words, opened a massive loophole that bypasses the Fourth Amendment, letting the government collect reams of very personal information. Unfortunately, HB 57 does not extend to medical or financial records held by third parties, leaving Utahns still vulnerable to warrantless snooping.

Last year, the Supreme Court narrowed the third-party doctrine in *Carpenter v. United States*. By a margin of 5-4, the court ruled that accessing time-stamped mobile phone records known as “cell-site location information” (CSLI) qualifies as a search under the Fourth Amendment. “A person does not surrender all Fourth Amendment protection by venturing into the public sphere,” Chief Justice John Roberts wrote for the majority.

“When the Government tracks the location of a cell phone it achieves near perfect surveillance,” Roberts warned, “as if it had attached an ankle monitor to the phone’s user.” If the government wants to access CSLI, the chief justice bluntly told them to “get a warrant.”

In *Carpenter*, Roberts acknowledged that CSLI “does not fit neatly under existing precedents,” since it’s a form of “personal location information maintained by a third party.” As a result, the court “decline[d] to extend *Smith* and *Miller*.” “Given the unique nature of cell phone location records,” he wrote, “the fact that the information is held by a third party does not by itself overcome the user’s claim to Fourth Amendment protection.”

First, CSLI is automatically recorded any time someone uses their phone, without any input from the user, which undermines the notion that CSLI is “voluntarily” handed over. Moreover, phones have become so embedded and prevalent that “carrying one is indispensable to participation in modern society,” Roberts added.

Second, “seismic shifts in digital technology” mean that “there is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today.” “With just the click of a button,” Roberts noted, “the Government can access each carrier’s deep repository of historical location information at practically no expense.” In the *Carpenter* case, the government obtained nearly 13,000 location points over 127 days when it investigated Timothy Carpenter for a series of robberies in Detroit.

Roberts convincingly explained why the third-party doctrine is a poor fit for CSLI. Yet even though many of those detailed reasons also apply to other forms of electronic data, the chief justice was adamant that his decision was a “narrow one.” *Carpenter* explicitly states that it does not directly consider the constitutionality of the government obtaining less than seven days’ worth of cell-site records, real-time CSLI, “conventional surveillance techniques and tools,” or business records, though many of those law enforcement tools are now covered by HB 57 in Utah.

While *Carpenter*’s long-term impact on digital data will largely depend on how the Supreme Court reconciles the decision with its woefully outdated precedents, in Utah, the Electronic Information or Data Privacy Act has already struck a major blow against the third-party doctrine. Utah’s sweeping reform warrants becoming a model for other states.

Nick Sibilla, Senior Contributor

I'm a writer and legislative analyst at the Institute for Justice (IJ), a public interest law firm. As a member of IJ's Communications team, I regularly write opeds and blog about economic liberty, private property rights, the First Amendment and judicial engagement.