

Guest opinion: Utah makes a surprising leader for electronic privacy

By Marina Lowe and Connor Boyack

For the Deseret News

Published: March 29, 2019 9:00 am

<https://www.deseretnews.com/article/900062918/guest-opinion-utah-makes-a-surprising-leader-for-electronic-privacy.html>

Utah is renowned for many things: We lead the nation in birth rate, volunteerism and even Jell-O consumption — but it may come as a surprise that our state is a leader when it comes to protecting electronic privacy.

Utah's legacy of valuing electronic privacy is evident in the laws our Legislature passes. In 2012, the Utah Legislature enacted SB236, establishing that GPS tracking constitutes a search that requires judicial authorization. In 2014, Utah became the first state in the nation to enact legislation simultaneously protecting location information and electronic communications content, regardless of age, from government access.

In the wake of several stunning abuses by law enforcement in accessing the prescription drug database, in 2015 the Utah Legislature specified that a warrant is required before police may access the electronic prescription drug records of Utahns. Now, in 2019, Utah is once again leading out, establishing through HB57 sponsored by Rep. Craig Hall, R-Dist. 33 — which passed unanimously — that a warrant must be secured before law enforcement may access electronic data held by a third party.

Why is this such a big deal? It is well established that law enforcement must seek and obtain a warrant before they can access the contents of your home or car or even your phone. But what about the electronic information that you transmit to a remote computing service? What about your electronic information when it is held by a third party, such as a cellphone service provider, photo sharing service, or social media company, as a necessary condition to operating? And what about the data created about us by companies with whom we interact?

Traditional legal analysis would have dictated that under what is known as the Third Party Doctrine, a person has no legitimate expectation of privacy in information he or she voluntarily turns over to third parties. But the relevance of the Third Party Doctrine may be waning in a world where increasingly we share information with third parties on a near constant basis: uploading photos, cellphone call logs, financial information and calendar entries, to name just a few.

The Supreme Court of the United States has been inching nearer every year to confirming that the Third Party Doctrine does not absolve the need for law enforcement to secure a warrant, as evidenced in the court's decision in *Carpenter v. U.S.* in 2018. Mr. Carpenter's legal woes began in 2011, when without getting a probable cause warrant, the government obtained several months' worth of cellphone location records for suspects in a criminal investigation in Detroit. For Mr. Carpenter, the records revealed 12,898 separate points of location data — an average of 101 each day over the course of four months. With the assistance of his counsel and the American Civil Liberties Union, among others, Mr. Carpenter objected to the warrantless disclosure of this information to law enforcement. The Supreme Court agreed, holding that a customer does indeed have an expectation of privacy in his or her cell service location information. In order to seek and use this type of information, the court stated in the *Carpenter* decision that law enforcement must first obtain a warrant under the Fourth Amendment. In so doing, the Supreme Court tacitly acknowledged that privacy principles need to adapt for the digital era. In general, the courts are slow to catch up to technological advances, underscoring why the passage of HB57 is so significant. The bill codifies the *Carpenter* decision but also goes further, making clear a

warrant is required before law enforcement may obtain, use, copy or disclose electronic information regardless of whether it is stored on our phones or on a server owned by a third party.

HB57 is essential in ensuring that the privacy rights of Utahns are protected in the digital age. And Utah has demonstrated, once again, that

Marina Lowe is legislative and policy counsel for ACLU Utah. Connor Boyack is president of Libertas Institute.