HB57: Utah Now Requires Search Warrant To Access Electronic Data

Utah now has the strongest protection of your private data, including cell phone contents, by requiring police to get a search warrant before access. Law enforcement fought HB57 but lost to the Constitutional protections of the 4th Amendment. TN Editor

Gov. Gary Herbert signed off on HB57 on Wednesday designating Utah as the state with the strongest data privacy laws in the country when it comes to law enforcement accessing electronic information.

House Bill 57 modified provisions about privacy of electronic information and data for Utahns. Rep. Craig Hall, R-Utah, pitched the bill in order to require police to get search warrants before accessing Utahns' electronic information, which up until this point has not been a necessity.

"Traditionally, we have pretty good protection with case law and statutes

that protect our physical stuff if law enforcement wants to search any of our belongings such as our homes, cars, or hard drives," Hall explained. "If law enforcement wants to search any of those things, they have to get a warrant first."

It's a little vague with respect to the electronic world. Hall said the goal of HB57 "is to provide the same protections we have in the physical world and apply those to the electronic world."

The Libertas Institute, a think-tank that seeks to create a freer Utah through legal research and lawsuits, was active in the passage of this bill. Connor Boyack, the organization's founder, said, "The U.S. Supreme Court recently required that our cell phone location data be protected by a warrant, which is a small step in the right direction. Utah's new law takes that principle and puts it on steroids, applying it to all of our electronic data."

Specifically, HB0057 does the following:

- Requires the issuance of a search warrant to obtain certain electronic information or data.
- Necessitates that when someone's electronic data or information has been obtained there will be notification.
- Declares that electronic information and data obtained without a warrant be excluded from consideration in legal cases.
- "Electronic information and data" was defined as being any information or data including a sign, signal, writing, image, sound, or intelligence of any nature transmitted or stored in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo optical system. The definition includes location information, stored data, and transmitted data of an electronic device.

"In particular it protects information that is passed on to a third party," Hall said. "So, for example, if an individual decides to draft a document and they store it on their computer, then law enforcement would have to seek and obtain a warrant before that computer's hard drive could be searched. But what happens if the individuals store their document with

Dropbox or Google Drive? Well, in the past, law enforcement has not had the requirement to seek such information by warrant. This bill makes clear that the protections we have in the physical world are also given in the electronic world."

The bill seeks to establish a reasonable expectation of privacy for electronic information and data that has been stored in digital devices or servers.

Read full story here…