

Utah House Passes Bill to Hinder Federal Surveillance, Warrantless Access to Cloud Data

In Front Page, Tech Freedom

February 28, 2019

<https://thelibertarianrepublic.com/utah-house-passes-bill-to-hinder-federal-surveillance-warrantless-access-to-cloud-data/>

By Michael Maharrey

SALT LAKE CITY, Utah – Last week, the Utah House unanimously passed a bill that would require police to get a warrant before accessing data stored in the “cloud.” The proposed law would not only increase privacy protections in Utah; it would also hinder the federal surveillance state.

Rep. Craig Hall (R-West Valley City) filed House Bill 57 (HB57) on Dec. 28. The proposed law would prohibit law enforcement agencies from accessing electronic information or data transmitted to a “remote computing service” without a warrant based on probable cause in most situations. In effect, it would prohibit police from warrantlessly accessing information uploaded into the “cloud.”

On Feb. 22, the House passed HB67 by a 71-0 vote.

HB57 does provide some exceptions to the warrant requirement that would allow law enforcement agencies to obtain location information in the event of an emergency involving an imminent risk to an individual of death, serious physical injury, sexual abuse, live-streamed sexual exploitation, kidnapping, or human trafficking; or if a remote computing service inadvertently discovers information that appears to pertain to the commission of a felony, or of a misdemeanor involving physical violence, sexual abuse, or dishonesty.

The proposed law specifically excludes information obtained in violation of the law from judicial proceedings.

HB57 would expand existing laws already on the books in Utah requiring police to get a warrant before accessing location information, stored data, and transmitted data from an electronic device. The current laws effectively ban the warrantless use of “stingrays.” These devices essentially spoof cell phone towers, tricking any device within range into connecting to the stingray instead of the tower, allowing law enforcement to sweep up communications content, as well as locate and track the person in possession of a specific phone or other electronic device. Current law also requires police to get a warrant before accessing electronic data from third-party providers. Passage of HB57 would further limit the ability of law enforcement agencies to warrantlessly gather electronic information and data.

IMPACT ON FEDERAL PROGRAMS

It has become standard practice for law enforcement agencies to upload warrantless surveillance data gathered at the state level to federal *fusion centers* operated by the Department of Homeland Security (DHS) and other federal agencies. Fusion centers serve as clearinghouses for all kinds of information shared between federal, state and local law enforcement agencies—including data gathered by surveillance cameras, drones, intercepted

cellphone and email communications, social network spying, as well as ALPRs and other invasive modes of surveillance. The DHS funds and ultimately runs 79 fusion centers across the U.S. The DHS describes homeland security intelligence/information fusion as the "...process of managing the flow of information to support the rapid identification of emerging terrorism-related threats requiring intervention by government and private-sector authorities." Fusion centers were sold as a tool to combat terrorism, but that is not how they are being used. The ACLU pointed to a [bipartisan congressional report](#) to demonstrate the true nature of government fusion centers: "They haven't contributed anything meaningful to counterterrorism efforts. Instead, they have largely served as police surveillance and information sharing nodes for law enforcement efforts targeting the frequent subjects of police attention: Black and brown people, immigrants, dissidents, and the poor." Fusion centers operate within a broader federal system known as the "information sharing environment" or ISE. According to [its website](#), the ISE "provides analysts, operators, and investigators with information needed to enhance national security. These analysts, operators, and investigators...have mission needs to collaborate and share information with each other and with private sector partners and our foreign allies." In other words, ISE serves as a conduit for the sharing of information gathered without a warrant. Known ISE partners include the Office of Director of National Intelligence which oversees 17 federal agencies and organizations, including the NSA. ISE utilizes these partnerships to collect and share data on the millions of unwitting people they track. When states limit the data and information law enforcement agencies can collect, it minimizes the amount of information and data that can end up in this federal information-sharing pipeline. Legislation such as HB57 practically hinders the operation and growth of the federal surveillance state. Simply put if the data is never gathered in the first place, it can't be shared. In a nutshell, without state and local cooperation, the feds have a much more difficult time gathering information. Passage of HB57 would strike another blow to the surveillance state and would be a win for privacy.

WHAT'S NEXT

HB57 now moves to the Senate. It was referred to the [Senate Rules Committee](#) where it must pass by a majority vote before being referred to a standing committee.

Mike Maharrey

Michael Maharrey is the Communications Director for the [Tenth Amendment Center](#). He proudly resides in the original home of the Principles of '98 – Kentucky. See his [blog archive here](#) and his [article archive here](#). He is the author of the book, **Our Last Hope: Rediscovering the Lost Path to Liberty**. You can visit his personal website