One Giant Leap for Privacy: Texas Now Requires a Warrant for Content

by Jadzia Butler
June 18, 2013

On June 14, the Lone Star State became a national leader in electronic privacy by enacting HB 2268: a bill requiring Texas law enforcement officials to obtain a warrant before accessing email and other communications content. Texas Governor Rick Perry signed the measure, which passed in the legislature overwhelmingly.

By requiring a warrant for communications content, Texas took two huge steps forward: First, it updated, at the state and local level, an electronic communications privacy law in a way that makes sense for our 21st century world. The old standard was based on a 27-year old federal law, the Electronic Communications Privacy Act (ECPA). ECPA sets the federal standard as well as a privacy floor for state law. ECPA and the old Texas law left gaping legal loopholes: Texas law enforcement officials could seize, without a warrant, opened email no matter its age, unopened email more than 180 days old, and documents, calendars, pictures and other information that Texans stored in the cloud. In addition, emails stored on a user's desktop computer were protected, while emails stored with service providers were not.

These distinctions do not reflect user expectations today. Today, most communications providers offer their users nearly unlimited storage capacity and emails are often kept indefinitely (as letters and other correspondence used to be). In addition, email providers have made it easier than ever before to search, save and retrieve digital communications, and much of these communications are stored on the providers' computers. Unfortunately, courts have been slow to address the application of the Fourth Amendment to these changes. As a result, consumers are confused about the security of their data. Today, consumers in Texas can rest assured that Texas law enforcement officials will only read their email when they have a warrant.

Second, requiring a warrant for content will help grow the cloud computing industry in Texas -- an industry expected to expand to $241 billion globally by 2020. Businesses across the world are increasingly turning to cloud-based services in order to save money on equipment and to achieve better computing reliability and data security. Thus far, American companies, including several in Texas, have been the global leaders in cloud computing, which has resulted in innovation, economic growth, and job creation. Cloud computing companies need to be able to assure their customers that data stored in the cloud will be as secure against government access as data stored locally. By applying the same protections to all stored communications, Texas is helping local companies give that assurance, and is making an important contribution to the protection of America's stake in a booming industry that will continue to grow well into the future.

While a great overall example of what needs to be done to bring consumer privacy laws up to speed with modern technology, two provisions of HB 2268 raise concerns. The statute's long-arm authority will mean that a communications service provider in a distant "reciprocity state" (currently California, Florida and Minnesota) can be served with a warrant from Texas even if the provider has little connection to Texas. In addition, the time limits the statute imposes for communications service providers to respond to demands that they turn over user content could actually be counterproductive. It could slow disclosures in priority and emergency cases as providers put those demands aside in order to fulfill lower priority demands that are already approaching the statutorily imposed deadline. Allowing judges to tailor deadlines to the circumstances seems more appropriate.

The big news here, though, is that Texas beat U.S. Congress to the punch by updating its own electronic privacy laws first by requiring a warrant for law enforcement access to stored communications content. It is now time for Congress to follow Texas's example and pass measure that would do the same thing, the ECPA Amendments Act, S. 607, which was reported by the Senate Judiciary Committee in April. In fact, it's time for other states to follow Texas's lead and pass

legislation to update their own electronic communications privacy laws.

The content of this document is from Center for Democracy & Technology.
Copyright © 2013 by Center for Democracy & Technology. CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. Details.
Source URL:
https://www.cdt.org/blogs/1806one-giant-leap-privacy-texas-now-requires-warrant-content