Published on *The National Law Review* https://natlawreview.com

The CLOUD Act's Dramatic Impact on International Privacy Laws

Article By:

Peter Vogel

Just when the European Union's General Data Protection Regulation, or GDPR, was about to go into effect, the United States Congress created the CLOUD Act (Clarifying Overseas Use of Data).

Without any public hearings, review or public comment, Congress passed the legislation as part of the US$1.3 trillion government spending bill. The CLOUD Act changed the privacy provisions that were in effect under the 1986 Stored Communications Act.

Originally created to protect privacy in telephone records, the SCA has been used by Internet service providers to restrict access to Internet content in the U.S., except with the owner's permission.

Needless to say, Internet privacy issues create headlines around the world every day. So the fact that the U.S. government would modify the SCA without public hearings, review or public comment has raised red flags for many.

What Happened in US v. Microsoft?

As a result of the CLOUD Act, the U.S. Supreme Court this spring dismissed the *U.S. v. Microsoft* case after hearing arguments earlier this year.

The case related to Microsoft's reliance on the 1986 SCA to justify its refusal to comply with a federal search warrant requiring the production of an alleged drug dealer's emails, which were stored in Ireland. Because the suspect of the federal investigation was an American citizen but had created his email account while overseas, the case presented a new wrinkle as to how Fourth Amendment search and seizure principals should apply in an increasingly digital world.

Microsoft argued that because the emails at issue were located on a data server in Ireland, they were outside of the Justice Department's reach. The Justice Department responded that the emails essentially were under Microsoft's American control, which placed them squarely within U.S. jurisdiction.

While both the Justice Department and Microsoft relied heavily on public policy in making their

arguments -- Microsoft citing citizen privacy rights and the Justice Department raising national security concerns -- Congress's enactment of the CLOUD Act ultimately ended the debate.

What Is the CLOUD Act?

The Electronic Frontier Foundation earlier this year described the CLOUD Act as "a far-reaching, privacy-upending piece of legislation" designed to do the following:

- Enable foreign police to collect and wiretap people's communications from U.S. companies, without obtaining a U.S. warrant.
- Allow foreign nations to demand personal data stored in the United States, without prior review by a judge.
- Allow the U.S. president to enter "executive agreements" that empower police in foreign nations that have weaker privacy laws than the United States to seize data in the United States while ignoring U.S. privacy laws.
- Allow foreign police to collect someone's data without notifying them about it.
- Empower U.S. police to grab any data, regardless if it's a U.S. person's or not, no matter where it is stored.

The theory behind the CLOUD Act is that it removes much of the "red tape" federal investigators previously faced when seeking private citizen data stored in foreign nations but controlled by U.S. companies.

In the past, foreign data sharing was limited to countries with whom Congress had approved a mutual legal-assistance treaty, or MLAT. If the country housing the desired data had not been approved for an MLAT, the process for approval could take months, potentially nullifying the usefulness of the data.

The CLOUD Act grants the Executive branch (including the president, attorney general and State Department) authority to approve immediate data-sharing arrangements with foreign nations, bypassing congressional approval.

Another important feature of the CLOUD Act is that it expressly grants law enforcement officials the ability to order production of digital records, regardless of where the data physically is stored. Data storage companies may petition a court to resist disclosure, but they are required to ensure the data is still accessible if a court chooses to enforce the search warrant.

Privacy Rights Community Reactions

Information technology industry leaders, including Microsoft, Apple, Google, Facebook and Oath, have offered public praise for the Act seeing it as much-needed clarification of how to deal with cross-border data sharing issues.

The ACLU, the Center for Democracy and Technology, and the Open Technology Institute have spoken out against the Act.

Pointing toward the safeguards previously offered by MLATs, the ACLU has argued that the Act will allow the executive branch to enter foreign data-sharing agreements without congressional oversight or proper vetting.

Similarly, the CDT and OTI have cited the need to protect citizen privacy and expressed fear that foreign governments could use obtained data to commit human rights violations.

Will the CLOUD Act Comport or Conflict With the EU GDPR?

The European Union has taken a remarkably different approach in addressing citizen data protection. The EU General Data Protection Regulation, which went into effect last month, applies to any business that processes EU citizen data. For example, companies that are effected by a data breach are required to disclose such occurrences within a 72-hour window.

Additionally, EU citizens are free to request records from the EU data controller, detailing who has accessed their information, when, and for what purpose. To encourage compliance, the GDPR mandates that significant violations can result in a maximum fine the greater of 4 percent of gross revenue or 20 million euros.

In contrasted with the CLOUD Act, which places data-sharing authority solely within the executive branch, the GDPR resembles the former U.S. approach of using MLATs to monitor foreign data sharing.

Still to be resolved is whether the CLOUD Act and GDPR will exist in harmony, or whether the conflicting agreements will require representatives to negotiate how private citizen data will be shared in the future.

Preliminary Conclusions

The CLOUD Act could have major implications in the world of e-commerce. U.S. law enforcement officials will be permitted to access international transaction data without significant oversight, as well as enter agreements providing foreign governments with reciprocal information.

While it is too early to tell how far the ramifications of the CLOUD Act will spread, those who utilize cloud-based storage providers, or conduct online business with foreign entities, should keep the CLOUD Act and GDPR at the top of their news-to-watch list.

Stephen Jones contributed to this post.

National Law Review, Volumess VIII, Number 158