How The CLOUD Act Can Reach Stored Data Across Borders

By **William Ridgway and Jordan Blain** (January 2, 2019, 2:33 PM EST)

William Ridgway

Jordan Blain

As global businesses move more of their data to the cloud, they may unwittingly be placing their sensitive information within the U.S. government's reach. The reason lies with a single phrase from the Clarifying Lawful Overseas Use of Data, or CLOUD, Act and its unexpected application to the cloud data industry.

Most regard the CLOUD Act, which went into effect in March 2018, as Congress' response to the battle Microsoft waged against the U.S. government over whether it needed to comply with a search warrant that sought emails stored overseas. And recent news reporting has focused on a possible "executive agreement" between the U.S. and the United Kingdom under the act, which would empower the U.K. to compel data from U.S. providers.

But most have overlooked the implications of the U.S. government's newfound power to collect data stored overseas, which extend far beyond the issues raised in the Microsoft litigation. All email and cloud storage providers with U.S.-based operations now must disclose emails and other stored data within their "possession, custody, or control," regardless of whether the data is stored in the U.S. or abroad.[1]

That provision in the CLOUD Act creates new and challenging questions for businesses that store data overseas with cloud providers. First, what type of ties to the U.S. will render overseas cloud providers subject to legal process under the CLOUD Act? Second, what happens when producing the data sought by the U.S. government violates the laws of the country where the data is stored?

Courts have not yet wrestled with these questions under the CLOUD Act, but case law from other legal contexts shed light on how U.S. courts will handle these questions.

What Ties Put Cloud-Based Data Under the "Control" of a U.S.-Based Provider?

The CLOUD Act made clear that overseas storage does not put data beyond the reach of the U.S. government, so long as the data is within a U.S. provider's "possession, custody, or control." That language mirrors the standard for subpoenas in the civil discovery context under Federal Rules of Civil Procedure 34 and 45, so courts will likely look to that case law in interpreting the act.

While "possession" and "custody" are straightforward inquiries, determining whether overseas data is within a U.S. provider's "control" is far more complicated, given the interconnectedness of the cloud industry at both the corporate and technical level. Not only do many major cloud providers operate within a network of corporate entities around the globe, they also often sublease services and infrastructure among one another, creating a complicated web that leaves the question of "control" uncertain.

Suppose, for example, a German business stores data with a cloud provider in Germany, but that provider uses the infrastructure of a U.S. provider to back up its data in Germany. If the U.S. government serves the U.S. provider with a search warrant under the CLOUD Act for data held in Germany, courts may be faced with a difficult question about "control." They will likely consider whether the U.S. provider has technical access to the data in an unencrypted format, whether the U.S. company accesses that data in the ordinary course of its business and whether the two companies otherwise have close corporate and financial ties.[2]

The analysis of "control" is fact-intensive, so no hard and fast rules can be drawn from the case law, but the inquiry boils down to whether a U.S. entity has a legal right or practical ability to access the overseas data. The problem for many businesses is that they may not even be aware of a subleasing arrangement or the existence of a sister corporate entity in the U.S. Thus, in selecting cloud providers, businesses should investigate the proposed arrangement to determine whether a company with a U.S. presence would have any level of access to its overseas data in an unencrypted format.

Some cloud providers offer technical features that may bear on the "control" analysis. One such feature is client-side encryption, a technique of encrypting a client's data before it is transmitted to the cloud computer server and entrusting the encryption key to the client exclusively. Deploying client-side encryption to restrict a cloud provider from accessing client data is typically viewed as a security feature, but it may well have important ramifications for the CLOUD Act's "control" analysis.

What Happens When Production of Cloud Data Violates Foreign Law?

The CLOUD Act itself touches on this issue by empowering the president to enter into executive agreements to create a framework for the sharing of data between countries and enable providers to try to prevent data productions that would violate the laws of that foreign government.[3] Yet no such executive agreements have been reached, and the CLOUD Act does not otherwise resolve the issue of conflicts with foreign law.

Given this gap, to predict how a court may handle a conflict with foreign law, one may look to cases involving so-called Bank of Nova Scotia subpoenas, where the U.S. government seeks to compel a domestic branch of a bank or business to produce records held by the bank or business in a foreign country. In the case from which the name derives, a Canadian bank refused to comply with a grand jury subpoena served on its Miami branch for documents in the Bahamas and the Cayman Islands,[4] arguing that compliance would violate Cayman bank secrecy laws. After weighing the respective national interests of the countries and the hardship that inconsistent enforcement would impose on the bank, the court ultimately upheld the enforcement of the subpoena and imposed sanctions against the bank.

Following that authority, U.S. courts will likely consider conflicting foreign privacy laws in deciding whether to enforce CLOUD Act legal process, but businesses and their providers cannot rely on that conflict to shield sensitive data from the reach of the U.S. government. This presents serious issues for businesses that operate in countries with strict data localization rules, such as Russia and China, or where cross-border data flows are highly regulated, such as in the European Union. Businesses may find themselves in the unenviable position of facing conflicting orders from two sovereigns, and neither may be

willing to budge. Those businesses have even more reason to analyze carefully their cloud arrangement, as discuss above.

As the U.S. government stressed in the Microsoft litigation, when seeking electronic data stored overseas, it much prefers to issue legal process on an entity in the United States, rather than invoke procedures under a mutual legal assistance treaty, which it regards as time-consuming, cumbersome and incapable of handling the demands of the digital age. The CLOUD Act — including its crucial "control" provision — thus gives the U.S. government a powerful weapon that it will undoubtedly wield. And the act will have broader reach than many expect, due to the cloud industry's complex interconnections. Yet the CLOUD Act's scope may be managed by thoughtful arrangements with providers, a factor that businesses should consider as they continue moving their data to the cloud.

William Ridgway is a partner and Jordan Blain is an associate at Skadden Arps Slate Meagher & Flom LLP.

[1] 18 U.S.C. § 2713.

[2] Cf. In re Subpoena to Huawei Techs. Co. Ltd. , 720 F. Supp. 2d 969, 977 (N.D. Ill. 2010); Afros SPA v. Krauss-Maffei Corp. , 113 F.R.D. 127, 129–30 (D. Del. 1986).

[3] 18 U.S.C. § 2703(h).

[4] See In re Grand Jury Proceedings Bank of Nova Scotia , 740 F.2d 817 (11th Cir. 1984).
