Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

CLOUD Act: Start Or End For Cross-Border Data Exchanges?

By **Saad Gul and Mike Slipsky** (April 9, 2018, 3:51 PM EDT)

Saad Gul

Mike Slipsky

This February, in U.S. v. Microsoft Corp, the U.S. Supreme Court considered whether a United States warrant could be used to access data that an American company had stored on a server located in Ireland. The technical legal question at issue was arcane: whether the 1986 Stored Communications Act, or SCA, had extraterritorial reach.

However, the practical implications of the case were clear: in an age of cloud computing, could American law enforcement gather data stored anywhere in the world?

But before the court could address the issue, Congress stepped in. Attached to the recently enacted 2,232-page, $1.3 trillion spending bill was the Clarifying Lawful Overseas Use of Data, or CLOUD, Act, which answers a number of questions that had been raised in the litigation.

First, it confirmed that an SCA order applied worldwide, regardless of location. The only requirement is that the targeted data be in the "possession, custody or control" of the recipient of the warrant. This applies "regardless of whether [the subpoenaed] communication, record or other information is located within or outside of the United States."

Second, the legislation attempts to soften the extraterritorial impact of this provision by including additional safeguards. A recipient can seek to quash the subpoena if it can show that the affected individual is not a United States person and that the required disclosure of that individual's data would violate the laws of a "qualifying foreign government".

The legislation defines "qualifying foreign governments" as those who have signed an executive agreement with the United States to cooperate in cross-border data access. To qualify, a foreign government would need the approval of the State Department and the U.S. Department of Justice. They would also have to agree to adhere to significant substantive and procedural privacy and civil liberties protections.

Congress would have 90 days to pass a joint resolution of disapproval to prevent an executive agreement from going into effect. Agreements would be subject to renewal at five-year intervals. The United States would have the ability to audit compliance. These are clearly stringent requirements. While other countries will almost certainly follow, only the United Kingdom, which has already negotiated such an arrangement, will be likely to qualify in the immediate future.

Third, the CLOUD Act requires courts considering a motion to quash to conduct a comity analysis. The act directs the court to consider the location of the target, the nationalities involved, alternative avenues to the data, the interests of the United States, and the interests of the foreign sovereign. This provision is presumably intended to allay international concerns about state sovereignty.

Whether the provision will actually accomplish that remains to be seen, as comity is an endlessly

malleable standard.

Notably, the U.S. Supreme Court has not even addressed the issue of comity since the 19th century case of Hilton v. Guyot. So it is notable that the legislation explicitly protects recourse to common law comity for nonqualifying countries. This permits providers to raise comity claims even absent explicit statutory authority to do so, and seek to quash based on the basis that execution of warrant will generate a conflict of laws.
Foreign concerns on this count may be offset by the amendment of the SCA's blocking provisions. Those provisions had previously barred U.S. providers from disclosing data to foreign governments. The bar applied even to friendly foreign governments conducting a bona fide criminal investigation of their own citizens. In other words, the CLOUD Act could assist foreign as well as American law enforcement: the data would flow both ways.

The CLOUD Act was broadly supported by the technology industry, but the full implications will take time to become evident. However, some concerns are likely to manifest themselves early:

- Foreign governments, particularly those not deemed to be "qualifying foreign governments," may mandate data localization;
- The Privacy Shield program, which is already under legal attack, may be struck down by European courts as incompatible with EU data privacy principles;
- While the CLOUD Act and European Union's new omnibus General Data Protection Regulation, or GDPR, address different issues, simultaneous compliance will be difficult. In particular, Article 48 of the GDPR prohibits the transfer of personal data absent "an international agreement [] such as a mutual legal assistance treaty." While the CLOUD Act's executive agreements would meet Article 48 requirements, transfer absent such an agreement or mutual legal assistance treaty (MLAT) would violate GDPR strictures and cause friction.
- Depending on implementation, foreign governments may enact blocking statutes, specifically forbidding compliance with American warrants outside their own legal processes;
- Data processors dealing with cross-border data transactions should contemplate additional safeguards, such as Microsoft's German "trustee" program, in order to minimize the risk of being trapped between conflicting legal regimes — the proverbial "rock and a hard place".

In conclusion, while legislative action was welcome, the CLOUD Act is unlikely to be the last word on the issue. Game theory predicts that other players, from individuals to foreign governments to law enforcement, will respond to the new legal environment with their own innovations. When that happens, Congress will have to revisit the issue. We can confidently predict that the next Congressional action involving the SCA and these kinds of cross-border data privacy issues won't be another 30-plus years in the making.

Saad Gul and Mike E. Slipsky are partners with Poyner Spruill LLP in Raleigh, North Carolina, and editors of NC Privacy Law Blog. They advise clients on a range of privacy, data security and cyber liability issues, including risk management plans, regulatory compliance, cloud computing implications and breach obligations.

Disclosure: The authors represented five European business federations before the Supreme Court in the case of United States v. Microsoft.