CLOUD Act Washes Away Barriers To Cross-Border Surveillance

By Austin Mooney |

The CLOUD Act has been enacted, effectively mooting the closely watched *United States v. Microsoft* case and marking a watershed moment in federal and international surveillance law. The Act codifies mechanisms for both US and foreign governments to enforce surveillance orders on data located outside of their territorial boundaries, with major consequences for providers of electronic communications and remote computing services who have operations in the United States. The two major points are as follows.

First, the Act partially lifts the Stored Communications Act's ("SCA") "blocking provision," which generally prohibits providers from disclosing the contents of data stored in the United States to foreign governments outside of US legal process. Under the CLOUD Act, providers can produce such data directly to foreign law enforcement where the foreign government has entered into an "executive agreement" with the United States. For an executive agreement to be valid, the foreign government must satisfy a long list of requirements, including that it:

- Has domestic law that "affords robust substantive and procedural protections for privacy and civil liberties";
- Will never use the mechanism to intentionally acquire the communications of US persons, and adopts minimization procedures to protect US person communications if unintentionally acquired;
- Will not use the mechanism to compel companies to decrypt the contents of messages;
- May only use the mechanism to target specific individuals for the purpose of preventing "serious crime," and never to infringe freedom of speech; and,
- Allows for a reciprocal mechanism by which US law enforcement can access data stored within its borders.

Where these and other conditions are met, companies are permitted to directly produce content in response to foreign orders without violating the SCA. What's more, they can do so while benefiting from the existing statutory liability protections under the SCA.

Second, the Act establishes that the domestic legal process obligations imposed on providers under the SCA apply to data stored overseas. This moots the central question in *United States v. Microsoft*, which concerns the validity of an SCA warrant vis-a-vis email content stored on Microsoft servers in Ireland. (For more information, check out the Supreme Court amicus brief we filed on behalf of leading technology companies in the case.) The Act does not, however, grant *carte blanche* authority for US law enforcement to demand overseas data, a circumstance that would place providers at risk of violating foreign laws with "blocking" effects similar to the SCA. Instead, the Act allows providers to, in certain circumstances, move to quash SCA orders on the ground of international conflicts. Federal judges can quash an order if they are satisfied that three conditions are met: (1) the customer is not a US person, (2) disclosure would require the provider to violate "qualifying" foreign law (i.e., of a country that has entered into an executive agreement described above), and (3) the "interests of justice" dictate that the order

should be quashed. For point (3), the Act details a number of factors for a court to consider in conducting its comity analysis, including the risk to the provider, the importance of the information to the investigation, and the interests of the respective countries.

These changes will have material consequences for providers with operations in the United States and internationally. Companies will need to reexamine and update their law enforcement compliance programs to adapt to the new regime, including by keeping an eye on which countries enter into executive agreements and carefully scrutinizing data protection laws in the countries in which they currently store content.

Electronic Communications Privacy Act (ECPA)/Stored Communications Act (SCA)