Cloudy with a Chance of Clearing: U.S. CLOUD Act and European Response

May 8, 2018

Electronically stored data play a vital role in criminal investigations. The framework for the transfer of such data across national borders continues to be difficult to navigate. Recent legislative developments in the United States and the European Union signal a change in the approach to cross-border data transfer for law enforcement purposes on both sides of the Atlantic.

Debevoise & Plimpton

This Client Update sets out the main provisions of the recently adopted U.S. Clarifying Lawful Overseas Use of Data Act ("CLOUD Act") and of the draft EU regulation on sharing electronic evidence ("e-Evidence Regulation"). It then considers their implications not only for electronic communications providers to which these rules are directly applicable, but also for participants in other industries that often find themselves on the receiving end of law enforcement requests.

THE U.S. CLOUD ACT

The U.S. Congress enacted the CLOUD Act on March 23, 2018 as part of an omnibus budget bill. It modifies the Stored Communications Act ("SCA") to clarify it has extraterritorial effect, providing that the SCA's warrant authority requires "provider[s] of electronic communication service[s] or remote computing service[s]" to produce data in their custody and control, regardless of the data's location.[1] In other words, warrants issued pursuant to the SCA can reach data located on email servers in countries other than the U.S. and in the cloud.

Most immediately, the CLOUD Act mooted the *United States v. Microsoft* case, pending before the U.S. Supreme Court, the key question in which related to SCA's extraterritorial scope. The data being sought resided on servers in Ireland, which Microsoft personnel could reach from their U.S. keyboards. Future warrants like the one to Microsoft are now plainly enforceable.

[1] CLOUD Act §§ 102, 103(a).

In a development that may have more consequences for the future, however, the CLOUD Act also creates a new mechanism for U.S. and foreign law enforcement agencies to request data from providers of electronic communications and remote computing services. The CLOUD Act contemplates that the U.S. would enter into bilateral Executive Agreements with foreign governments enabling enforcement agencies in both countries to make direct requests to service providers if certain conditions are met.[2] This creates an alternative to the so-called "MLAT process," whereby a law enforcement agency must submit a data request to the central authority of the foreign state where the data reside, pursuant to a mutual legal assistance treaty ("MLAT").

Not every country, however, may enter into an Executive Agreement. The U.S. Attorney General and Secretary of State must certify to the U.S. Congress that the foreign government at issue provides "robust substantive and procedural protections for privacy and civil liberties" and that it has adopted procedures to "minimize the acquisition, retention, and dissemination of information concerning United States persons," among other requirements.[3] The CLOUD Act also prohibits non-U.S. law enforcement authorities from making certain document requests via the Executive Agreement process, including those that target a U.S. citizen or resident.[4]

The CLOUD Act also sets out a process for service providers—the targets of the law enforcement demands—to challenge requests from U.S. enforcement agencies made pursuant to Executive Agreements. Requests can be challenged in U.S. courts where they may be quashed if the court determines that (*i*) the service provider is not a U.S. person; (*ii*) compliance with the request would cause the service provider to violate the laws of the foreign government; and (*iii*) "the interests of justice dictate that the legal process should be modified or quashed."[5] While this challenge procedure is unavailable if no Executive Agreement covers the request, the service provider can use other means to attempt to quash or modify the request. That means that it will be difficult for companies to challenge extraterritorial requests in the short term (before Executive Agreements are negotiated), and even in the long term where the relevant foreign government does not qualify for an Executive Agreement.

[2] *See* CLOUD Act §§ 103, 105.
[3] *Id.* § 105(a).
[4] *See id.*
[5] *Id.*

THE EU PROPOSAL FOR SHARING ELECTRONIC EVIDENCE

In April 2018, and at least in part in response to the CLOUD Act, the European Commission issued the draft e-Evidence Regulation, which would allow law enforcement agencies in the EU Member States to obtain electronic evidence located outside the EU. The e-Evidence Regulation, as drafted, would apply to providers of electronic communication services, social networks, certain online marketplaces, hosting services and internet domain name and IP numbering services that are based in the EU or offer their products and services in the EU. The draft e-Evidence Regulation introduces two new methods for obtaining or preserving electronic evidence:

- ***First***, European Production Orders would allow EU law enforcement authorities to obtain a production order against an EU-based service provider. The service provider would then need to produce electronic evidence in its possession, regardless of its location, within 10 days (or six hours in cases of imminent threat to life or physical integrity of a person or critical infrastructure).

- ***Second***, European Preservation Orders, obtained in the same way as Production Orders, would require an EU-based service provider to preserve data, wherever located, for as long as it may be necessary for a later production pursuant to a European Production Order or an MLAT request. The requesting law enforcement authority must confirm within 60 days of issuing the Preservation Order that it has launched a request for production.

Non-EU-based service providers subject to the e-Evidence Regulation would be required to appoint a legal representative in the EU to receive and respond to the European Production and Preservation Orders in a timely manner.

Notably, the draft e-Evidence Regulation provides a mechanism to challenge European Production and Preservation Orders. The recipient of the Order can seek its review in the relevant EU Member State court on the basis that compliance would violate foreign law to which it is subject. Where the foreign law at issue is aimed at protecting fundamental rights of individuals or the third country's fundamental interests relating to national security or defense, the court must seek the relevant third country's opinion on whether a conflict of laws exists. If the third country determines that a conflict does exist and objects to the Order's execution, the court must withdraw the Order.

IMPLICATIONS FOR SERVICE PROVIDERS AND OTHERS

U.S. law enforcement agencies and courts have long viewed the MLAT process as too cumbersome and have devised various ways to bypass it. In particular, they often serve subpoenas and other process directly on companies based in the U.S., arguing (as the U.S. government did in the *Microsoft* case) that such requests are not extraterritorial when the company can "migrate" the data to the U.S. with a click of a button. For the most part, the U.S. authorities also gave little heed to foreign data protection laws and rarely viewed them as a reason to quash otherwise valid U.S. process. The EU authorities, on the other hand, have generally insisted that the MLAT process is the sole proper mechanism for cross-border data transfer to foreign law enforcement authorities.

The U.S. CLOUD Act and e-Evidence Regulation suggest that legislators on both sides of the Atlantic may be moving towards a harmonized approach, albeit slowly and with likely roadblocks along the way. If Executive Agreements are actually put in place between the U.S. and EU Member States, service providers would have a way to challenge extraterritorial requests from U.S. authorities on the basis of their conflict with EU data protection laws. Much discretion remains with the U.S. courts, and historically U.S. authorities have tended to prevail in such cases. However, the Executive Agreement mechanism may provide additional clout to the qualifying foreign governments and their legal systems, which may alter the analysis. Conversely, the e-Evidence Regulation suggests that the EU may be abandoning the rigid "MLAT-only" line in favor of a more pragmatic approach.

A cooperative relationship between U.S. and EU law enforcement agencies would be a welcome development for companies that find themselves stuck between the rock of U.S. subpoenas and a hard place of EU data protection laws. The CLOUD Act and e-Evidence Regulation apply only to electronic communications service providers and similar businesses. Their underlying principles, however, can be used by other "frequent fliers" in the law enforcement subpoena space, including financial services companies, to argue for similar treatment. Law enforcement authorities often subpoena financial services firms for the same reasons they do communications services providers—for their customer data, often located abroad or in the cloud. If a greater harmonization works in the communications service provider sector, it is possible that broader changes are afoot.

* * *

Please do not hesitate to contact us with any questions.

NEW YORK

Jeremy Feigelson
jfeigelson@debevoise.com

Bruce E. Yannett
beyannett@debevoise.com

Anna R. Gressel
argressel@debevoise.com

LONDON

Jane Shvets
jshvets@debevoise.com

Ayushi Sharma
asharma@debevoise.com