THE
NATIONAL LAW REVIEW

DOJ White Paper Answers Questions about the Scope and Applicability of the CLOUD Act

Drinker Biddle
Article By
Laura H. Phillips
Drinker Biddle & Reath LLP
DBR on Data

- Administrative & Regulatory
- Communications, Media & Internet
- Global

- All Federal

Monday, April 22, 2019

Last year Congress enacted the CLOUD Act (the Clarifying Lawful Overseas Use of Data Act) to clarify the means for foreign legal authorities to access electronic information held by U.S.-based global providers. The U.S. Department of Justice (DOJ), in April 2019, issued a White Paper entitled "Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act." This White Paper lays out the policy and legal reasons for enactment of the CLOUD Act, and explains how the CLOUD Act overlays and interacts with existing laws and established inter-governmental practices.

As the White Paper observes, communications service providers (CSPs) have operations and customers all over the world and may store data in facilities located in different countries and as a result this data could be subject to more than a single country's laws. This situation can lead to conflicting legal obligations related to sovereignty, criminal due process and privacy protection concerns. Nevertheless, the United States and other countries need a workable framework under which individual governments have the ability to acquire extra-territorial electronic evidence that could be vital in pursuing criminal, cybersecurity and similar public safety investigations. While historically these "conflict of law" problems are resolved by the use of Mutual Legal Assistance Treaties (MLATs) between countries, the DOJ White Paper notes that the global legal system has faced increasing challenges in keeping up with the proliferating demands for electronic evidence in

criminal investigations worldwide. As a result, the question of how to provide efficient and effective access to evidence needed to protect public safety while preserving respect for sovereignty and privacy standards remains relevant.

The CLOUD Act has two distinct parts. First, the Act authorizes the United States to enter into executive agreements with other countries that meet certain criteria, such as respect for the rule of law, to address the conflict of law problem. For investigations of serious crime, CLOUD Act agreements can be used to remove restrictions under each country's laws so that CSPs can comply directly with qualifying, lawful orders for electronic data issued by the other country. Second, the CLOUD Act makes explicit in U.S. law an established U.S. and international law principle that a company subject to a country's jurisdiction can be required to produce data the company controls, regardless of where that data is stored at any point in time. The DoJ White Paper notes that the CLOUD Act simply clarified existing U.S. law on this issue and did not change the existing standards under U.S. law that must be met before law enforcement agencies can require disclosure of electronic data.

The White Paper also discusses the pre-CLOUD Act operational framework and discusses how the CLOUD Act agreements are intended to work to simplify lawful access to electronic data held by CSPs. CLOUD Act executive agreements are expected to reduce the burden on the pre-existing MLAT system by allowing CSPs to respond directly to covered foreign orders without fear of a conflict between the two countries' laws. The DOJ White Paper states that the CLOUD Act did not expand U.S. investigative authority, nor did it extend U.S. jurisdiction to any new parties.

Nations have legitimate interests in protecting data from other governments that do not adhere to appropriate legal standards or abuse their authority for illicit purposes. The challenge is to ensure that governmental powers to compel production of electronic data are exercised in a way that respects the rule of law, protects privacy and human rights, and appropriately reduces conflicts between the laws of the countries in question. As the White Paper explicitly recognizes, a failure to address these situations would increase incentives for data localization across the world, which would be harmful both to global commerce and to public safety. The DOJ White Paper concludes that the CLOUD Act framework of executive agreements among "rights respecting" countries will support those countries' efforts to investigate serious crime, which is vital to keeping their citizens safe.

The White Paper concludes with a series of Frequently Asked Questions (FAQs) about the purpose of the CLOUD Act, the parties that can enter CLOUD Act agreements and what CLOUD Act agreements may and may not cover. These FAQs also address the effect of amendments to the Stored Communications Act, including the circumstances where there is a need for a warrant to access stored content. The White Paper is a helpful overview both to the purpose and practical effects of the CLOUD Act.