LAW ENFORCEMENT ACCESS TO DATA STORED ABROAD ACT

ISSUE: 30-YEAR-OLD ELECTRONIC EVIDENCE GATHERING LAWS DO NOT REFLECT HOW USERS SHARE, STORE AND COMMUNICATE IN TODAY'S NETWORKED WORLD

- The laws governing how law enforcement can access electronic communications and related data were originally passed in 1986 and are woefully outdated.

- They were designed for a time when early "Internet" users would dial-in to third-party service providers from their home or work computers and download their emails, which were generally only stored temporarily on the provider's servers. Unfortunately, that legal structure makes little sense in today's networked world where users are always online, can access their emails and other content from anywhere in the world, and use cloud and Internet service providers to store their data in the cloud.

- As a result, U.S. laws do not provide an adequate modern-day framework to U.S. law enforcement or companies on the legal processes to obtain data in the cloud and globally. Ambiguities have created situations where U.S. investigators are forced to push boundaries to try to obtain data in foreign countries, regardless of whether it is related to U.S. persons.

- Questions over how the U.S. can or cannot obtain data stored abroad is creating problems for companies operating globally. Nations are responding by threatening to require data to be stored locally (e.g. Germany by wanting to create its own cloud and Russia enacting an arcane localization law). Cross border data flow is being threatened in international trade conversations. There is also increasing concern that other countries may require companies doing business in their nations to reach back into the U.S. to get data off U.S. servers without working with the U.S. government and respecting U.S. laws.

SOLUTION: THE LAW ENFORCEMENT ACCESS TO DATA STORED ABROAD ACT ("LEADS ACT") UPDATES U.S. ELECTRONIC EVIDENCE GATHERING LAWS TO PROTECT ACCESS TO THE EMERGING TECHNOLOGIES OF 2015 NOT THE DIAL-UP SERVERS OF 1986.

Specifically, the LEADS Act does the following:

- Requires that law enforcement agencies obtain a warrant in order to obtain any content of electronic communications stored with service providers in the cloud. Currently, there are archaic rules on when and whether such communications can be accessed.

- Recognizes that law enforcement agencies may have a legitimate need to obtain, through lawful process, electronic communications relevant to criminal investigations relating to U.S. persons even when that data is stored abroad. It authorizes a warrant to extend overseas if the warrant seeks the contents of electronic communications of a U.S. person.

- Reforms the Mutual Legal Assistance Treaty ("MLAT") process. MLATs create treaty-based frameworks that allow a law enforcement agency in one country to obtain evidence located in another country. The bill requires the Attorney General to create an online docketing system for MLAT requests and to publish new statistics on the number of such requests.

- Establishes the sense of Congress that data providers should not be subject to data localization requirements. We have seen proposed laws emerge in places such as Russia and Brazil. Congress should make clear that such requirements are incompatible with the borderless nature of the Internet, an impediment to online innovation, and unnecessary to meet the needs of law enforcement.