The CLOUD and Similar non-U.S. legislation

Academy of International Financial
Litigators
November 30, 2018

Bruce Zagaris
Berliner Corcoran & Rowe LLP
Washington, D.C. 20026
(202)293-2371 bzagaris@bcr-dc.com

BCR
BERLINER CORCORAN & ROWE, LLP

I. INTRODUCTION

- March 2018, Trump signed Clarifying Lawful Overseas Use of Data Act (the CLOUD Act).
- **Goal**: to help apply the 1986 Stored Communications Act so that law enforcement can gain access to electronic cross-border information in an era of "deterritorialization of data."
- This presentation discusses the Microsoft case, the CLOUD Act, the approach of other countries, and some final thoughts.

II. US v. Microsoft

- *US v Microsoft*: In 2013, US prosecutors serve Microsoft with an SCA warrant for information from a Hotmail account, allegedly used in a drug-trafficking case.
- Microsoft refused to produce content of Doe's emails, which, since Doe identified himself as a citizen of Ireland when creating the account, was stored on a server in Ireland.

II. US v. Microsoft

- Microsoft moved to quash the SCA warrant because SCA has no extraterritorial effect and cannot compel U.S. service provider to surrender data stored in a foreign country.
- US should use MLAT or other means.
- US Dist Ct: Microsoft must surrender data under its custody & control & no extraterritoriality exists..

II. US v. Microsoft

- US Ct of App (2d Cir.): reversed, holding that an SCA warrant could not compel disclosure of emails in Ireland.
- Presumption against extraterritorial application controls and key factor is where the data are stored.

II. US v. Microsoft

- U.S. Supr. Ct: Oct. 2017 granted certiorari.
- 4 groups of amici curiae positions:
- 1) law enforcement: SCA must give access to data stored abroad if accessible from the U.S.
- 2) Ireland &EU oppose infringement of sovereignty and esp. privacy;
- 3) Hi tech & communications firms: SCA does not extend to data stored abroad;
- 4) Privacy-focused civil society NGOs: SCA warrants should not infringe on cross-border privacy protections

III. CLOUD Act

- W apparent support of DOJ and Microsoft, Congress enacted CLOUD Act.
- 1st part clarifies US electronic providers must comply w an order under the SCA to disclose emails even where outside the US.
- 2nd part governs foreign governments' access to U.S-held data and authorizes the US to conclude reciprocal data-sharing "executive agreements" with foreign governments.

III. CLOUD Act

- Eligibility requires foreign governments to meet certain standards with regards to human rights and the rule of law:
- 1) Have laws that "affords robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities of the foreign government that will be subject to the agreement;"
- 2) Have "appropriate procedures to minimize the acquisition, retention, and dissemination of information concerning US persons subject to the agreement;"
- 3) Have procedures that guard against targeting, either direct or indirect, of a U.S. citizen or person located in the US.

III. CLOUD Act

- For a qualifying order for the disclosure of U.S.-held data to a foreign government, the Act requires that an order must:
- 1) Be for the purpose of "obtaining information relating to the prevention, detection, investigation, or prosecution of serious crime, including terrorism;"
- 2) Identify a "specific person" or other "specific identifier" as the object of the order;
- 3) Comply with the requesting country's domestic law;
- 4) Be subject to independent oversight by a judge, court, magistrate, or other legal authority; among other qualifications.

III. CLOUD Act

- Qualifying foreign government must submit to "periodic review of compliance" with the terms of the agreement, to be conducted by U.S. officials.
- The Act allows a foreign government to bypass the inefficient MLAT process when seeking access to e-evidence held by a U.S. service provider, provided the foreign government already has an executive agreement in place and believes the some of the burden on the inundated MLAT system.

III. CLOUD Act

- The Act also removes the requirement that U.S. legal standards be met for what is often a foreign local criminal investigation.
- Instead, the CLOUD Act relies on both the foreign government's own domestic law and the int'l normative standards set forth in the act.
- In resolving these problems, the CLOUD Act removes two main incentives that foreign governments have had until now to enact alternative measures, such as expanding their surveillance powers or requiring data localization policies.

III. CLOUD Act

- In cases concerning identifiable foreign interests, the act authorizes a US provider to challenge an SCA order by moving to quash if the request implicates the interests of a friendly foreign government.
- If a provider can show it “reasonably believes” that the customer or subscriber is not a US person and does not reside in the US and the disclosure would cause a “material risk” the provider would violate laws of a “qualifying foreign government” (QFG), the provider can obtain relief.

III. CLOUD Act

- If the foreign citizenship of the data owner and a "material risk" of foreign prosecution exist, the court may find that "interests of justice" dictate that the order should be modified or quashed.
- There is a 7-factor comity analysis

III. CLOUD Act

- Does the CLOUD Act apply to non-US service providers? Perhaps, it depends on whether the service provider is subject to U.S. jurisdiction through doing business in the U.S.
- Will a non-US service provider which stores data outside the US and does not have an office or market its services in the US be subject to the SCA?
- Criminals may choose to select non-US based service providers w/o US presence to try to escape the SCA.

III. CLOUD Act

- What happens if a US service provider tries to quash a warrant or subpoena when it is at risk fo foreign prosecution by a government that has not qualified as a QFG.
- QFGs effectively prequalify to serve foreign law-enforcement requests directly on US service providers, rather than through the USG.

III. CLOUD Act

- At present, the CLOUD Act does not address how the executive agreements will work.
- The procedure for a recipient to contest an order and for the USG to render an executive agreement inapplicable as to any order for which USG concludes the agreement may not be properly invoked are not set forth.
- At present there are no imminent executive agreements. Given all the privacy, law enforcement, and other issues, it may be a while.

III. CLOUD Act

- What about work-arounds? *"Data trusts"* whereby local law would provide that data relating to communication services offered to citizens of a country would not be stored by the service provider, but instead would be automatically transferred to a "trustee," accountable to the government, who would store the data on independent servers.

III. CLOUD Act

- These trusts would enable the service provider served with an SCA order to claim that it does not have possession, custody, or control of data.
- Instead, the trust does.
- Local law allows the trustee to refuse any access that does not comply w local laws and procedures.

IV. Other Non-US Approaches

- **A. EU** - On April 17, 2018, the European Commission proposed a reg (on European Production and Preservation Orders for electronic evidence in criminal matters) and a directive (Laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings).
- *Production Order* allows an E.U. MS's judicial authority to compel a service provider in another State to produce electronic evidence.

IV. Other Non-US Approaches

- The Preservation Order allows a State's judicial authority to require a service provider in another state to preserve specific data while the data request is being processed.
- Both instruments are intended to:
  - significantly speed up the data request process,
  - introduce safeguards for the protection of individual rights, and
  - provide legal clarity for service providers regarding requests for electronic communications

IV. Other Non-US Approaches

- The proposed E-Evidence Directive would require overseas companies to appoint a legal representative in the EU who could provide access to data stored outside the EU w/I 10 days of a request, or w/i 6 hours in case of an emergency.
- Directive would apply to providers offering services in the EU and have a "substantial connection" to the EU, meaning that the company either has an establishment in an EU country or provides services to a large number of users in an EU country.

IV. Other Non-US Approaches

- **B. UK Overseas Production Act (OPA)**
- The OPA would allow law enforcement agencies to request electronic data directly from service providers, thereby bypassing the cumbersome mutual legal assistance process.
- The OPA covers data of "substantial value" to the ongoing investigation, and the production of the data must serve the public interest.
- It requires that an international agreement already be in place between the requesting country and the recipient country, similar to those envisaged by the CLOUD Act.

C. The Chinese Approach

- Sept. 20, 2016 prop. regs on collecting and transferring data in criminal investigations.
- Domestic operation is defined as providing products or services within China.
- A foreign network operator, which while not registered in China provides products or services to customers in China, is engaged in domestic operation and hence will be subject to China's cross-border data transfer requirements.

C. The Chinese Approach

- China's Cybersecurity law became effective last year and requires critical information infrastructure operators (CIIOs) to store personal information and important data collected and generated within the territory of the PRC.
- The regulations seem to authorize the unilateral extraction of data concerning anyone (or any company) being investigated under Chinese criminal law from servers and hard drives located outside of China."

C. The Chinese Approach

- In particular, Art. 9 of the regs authorize Chinese law enforcement officials to obtain data from storage media (such as servers and hard drives) located outside of mainland China.
- They may obtain this data through the Internet or via "remote network inspections."
- Hence, China is also developing compulsory measures to gain access to electronic data.

V. FINAL THOUGHTS

- Is the CLOUD Act a solution for a balkanization of the web due to country-by-country data localization instead of a globally networked internet or just a starting point?
- The CLOUD Act is quite limited, insofar as it applies only to the SCA and the ways to move and store data are multiplying as are the different ways for law enforcement to access data (e.g., unilateral, LR, Hague Convention, MLATs)

V. FINAL THOUGHTS

- Much legal analysis does not account for the kind of cloud in which data are stored.
- The problem is that different types of clouds raise distinct legal issues.
- Clouds differ when it comes to where and how they store information, and how they permit access to it.

V. FINAL THOUGHTS

- Does limiting access to HFGs create more balkanization of electronic data storage?