



Llinks Corporate and M&A Bulletin
May 2018

上海
上海市银城中路 68 号
时代金融中心 19 和 16 楼
邮编：200120
电话：+86 21 3135 8666
传真：+86 21 3135 8600

北京
北京市建国门北大街 8 号
华润大厦 4 楼
邮编：100005
电话：+86 10 8519 2266
传真：+86 10 8519 2929

香港
香港中环皇后大道中 5 号
衡怡大厦 27 楼
电话：+852 2969 5300
传真：+852 2997 3385

伦敦
1/F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

www.llinkslaw.com

SHANGHAI
19/F&16/F, ONE LUJIAZUI
68 Yin Cheng Road Middle
Shanghai 200120 P.R.China
T: +86 21 3135 8666
F: +86 21 3135 8600

BEIJING
4/F, China Resources Building
8 Jianguomenbei Avenue
Beijing 100005 P.R.China
T: +86 10 8519 2266
F: +86 10 8519 2929

HONG KONG
27/F, Henley Building
5 Queen's Road Central
Central, Hong Kong
T: +852 2969 5300
F: +852 2997 3385

LONDON
1/F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

master@llinkslaw.com

Cloud Act: Risks vs Opportunities

By Xun Yang

As an ‘insignificant’ part of ‘US\$ 1.3 Trillion Omnibus Spending Bill’, Clarifying Overseas Use of Data Act (‘CLOUD Act’) as a bipartisan act officially took effective on 23rd March 2018 after its quick execution by the President Trump.

In fact, the CLOUD Act was quietly and weirdly ‘included’ into and passed along with the 2232-page government spending bill, though its content has nothing to do with governmental expenditure. From its content, we believe that its enactment will ultimately resolve the long-standing controversy between Microsoft and U.S federal government on the federal power to compel the disclosure of overseas data, which have been lasted for more than five years. Moreover, with only brief stipulations, it will definitely have a profound influence on the trans-border data transmissions. This article will discuss its potential impacts on the Chinese market and companies in China.

1. Background of CLOUD Act

CLOUD Act is essentially a response to the outdated Stored Communications Act (“SCA”) for clarifying that how and to what extent “a provider of electronic communication service and remote computing service” (which is defined under SCA, for the purpose of this article, hereafter referred to as “**network service provider**”) must provide the data or record under its control.

如果您需要本出版物的中文本，
请与下列人员联系：

郭建良: (86 21) 3135 8756
Publication@llinkslaw.com

If you would like other Llinks
publications, please contact:

Roy Guo: (86 21) 3135 8756
Publication@llinkslaw.com

Llinks Law Offices
www.llinkslaw.com

Cloud Act: Risks vs Opportunities

CLOUD Act was adopted in response to the controversy raised in the case *United States v. Microsoft Corp.*, which began in 2013, where Microsoft received a U.S law enforcement request to disclose a customer's email data in relation to a narcotics investigation. However, Microsoft found that the data requested by the federal government were stored in its data centre in Ireland and it was prohibited under the Irish laws and EU regulations from transmitting the data overseas per request by the U.S government. Consequently, Microsoft refused to turn over such data and insisted that the U.S law agency needs to work with Irish government through Mutual Legal Assistance Treaty. In response, the Department of Justice filed a proceeding against Microsoft by arguing that US government has the power over the data controller to compel them to disclose the data in their control no matter where such data is located. The case tried by district court, court of appeals and then submitted to the US Supreme Court.

Despite that courts at different levels have different opinions, the controversial issue was always focused on the question whether the US government has power to compel the disclosure of data located in Ireland, regardless of relevant Irish laws. Those support '**data controller rule**' believe that US government has the power over entities in US and thus has the power to request for the disclosure act; those holding data location rule believe that Microsoft has no obligation to hand over emails because the SCA only 'authorized this sort of access only for data held within the territorial boundaries of the United States'.

Section 3 of CLOUD Act expressly resolved such question before the US Supreme Court trying this case by clarifying that Microsoft is obligated to hand over any communication or other information that 'is located within or outside of the United States', such as data located in Ireland. In other words, the U.S law enforcement agencies now have the right to compel the disclosure of data located in foreign countries bypassing foreign governments' censorship. Meanwhile, a channel for defending the disclosure request from law enforcement agency, has been provided under CLOUD Act. However, such defence is subjected to strict and "arbitrary" conditions. As a courtesy, the CLOUD Act also provides for a channel (very narrow though) for foreign government agencies apply for access to communication data or records located in United States.

2. What is CLOUD ACT about?

The CLOUD Act attempts to establish a new standard for global data transmission: the U.S government would have the right to access to the data located in foreign countries via its network service providers which are operated worldwide and, to the contrary, the foreign governments would have no access to data located in U.S. unless at the "mercy" of the U.S government.

Generally speaking, there are three major stipulations in the CLOUD Act: (a) the establishment of "the data controller rule" in order to resolve the essential issue in case *United States v. Microsoft Corp.*; (b) the definition of "qualified foreign government" which is eligible to request for data located in the territory of United States; and (c) the channel for telecoms service providers to defend the disclosure request made by the U.S. government.

Cloud Act: Risks vs Opportunities

First of all, it is required by the CLOUD Act that network service provider has to “preserve, backup or disclose the contents of a wire or electronic communication and any record or other information” upon the request of U.S. government, and no matter where the data or information is stored or located. Such obligations indicates the CLOUD Act has established and confirmed the “data controller rule”, i.e. the United States Government now has express legal authority to seek electronic data in the possession, custody or control of U.S. companies and enterprises regardless of where the data is physically stored.

Secondly, Section 3 of CLOUD Act contemplates a channel to defend the disclosure request. The new Section 2703 (h) permits the network service provider which receive the disclosure request to file a motion to object to such request made by the enforcement authorities on the conditions that: (a) the customer or subscriber (i.e., the data subject) is not a U.S citizen or does not reside in the United States; (b) the required disclosure may create a material legal risk that the provider would violate the laws of a “qualified foreign government”; and (c) the motion was filed within 14 days since the receipt of the disclosure request pursuant to legal process.

Irrespective of other conditions to the ‘defence’, it is a demanding and arbitrary procedure for a state to be recognized as a “qualified foreign government” (“QFG”) under CLOUD Act. According to the CLOUD Act, the QFG is determined by the Attorney General together with the Secretary of State, which has been required to demonstrate that “the domestic law of such foreign government, including the implementation of that law, affords robust substantive and procedural protections for privacy and civil liberties.”

To be specific, the foreign government needs to enter into an executive agreement and satisfy requirements which, among others, include “whether the foreign government has adequate substantive and procedural laws on cybercrime and electronic evidence, as demonstrating by being a party to Convention on Cybercrime (Budapest)” and “whether the foreign government has demonstrates a commitment to promote and protect the global free flow of information and the open, distributed, and interconnected nature of the Internet.”

Lastly, Section 4 of CLOUD Act provides for a legal framework in which a QFG is able to raise a request to U.S government for getting access to data located or stored in the territory of US. However, it remains uncertain how and to what extent it will provide for an effective data sharing channel because of the strict conditions to be admitted as a QFG and the complicated verification procedure to access the data in U.S firms’ possession.

3. Impacts on Chinese Market and Chinese Companies

CLOUD Act is with no doubt a powerful weapon for the U.S government to maintain its advantageous position in the cyberspace by taking advantage of dominant position in Internet industry contributable to its network service providers operated worldwide. Chinese government and enterprises need inevitably to take actions in response to CLOUD Act. In particular, the standards for being recognized as QFG under

Cloud Act: Risks vs Opportunities

CLOUD Act contradict to China's principle standpoints and without doubt, Chinese government is unlikely recognized as a "qualified foreign government" under the CLOUD Act.

Firstly, the Chinese government currently stands on a prudent position in relation to foreign investment in the business of offering Internet information services, email services, as well as data centre services. It is foreseeable that the Chinese government, after the issuance of CLOUD Act, will continue restricting the investment in these sectors by foreign investors. This is because, should foreign investors (especially US investors) be allowed to invest in these sectors in China, U.S government would have the right to get access to data processed or stored in China disregarding the restrictions of PRC laws and the objections of relevant data subjects.

Secondly, China government is likely to strengthen the control over data exportation. This is not surprising because any data and information stored outside of China is not only difficult for the Chinese government to censor but also exposed to the risks that the U.S government may obtain such data at its own wishes under CLOUD Act.

Thirdly, some companies be facing conflicting legal requirements. Both "General Data Protection Rules" issued by European Union and "Cyber Security Law" and its implementation rules issued by Chinese legislators impose material obligations on network operators that they must respect the intention of data subjects and follow a strict security procedure when exporting data. Such legal requirements is contrary to the U.S law enforcement agencies' extraterritorial right under CLOUD Act, which means , for those whose business operated in both America and EU/China, the performance of one jurisdiction's legal obligations constitutes a violation of the other's requirements.

Additionally, giving the accessibility of U.S authority under the CLOUD Act to trade secrets and other confidential information, Chinese companies are recommended not to procure cloud services from U.S firms or those services on U.S. cloud. Otherwise, their business secret or other confidential information may be accessed by U.S governments.

Last but not the least, CLOUD Act could be a good news for Chinese Internet service providers or any other countries except for United States. The fact that, if their business has no ties to or presence in the United States, they are not subject to any legal obligations to disclose client's information to US government under CLOUD Act could be a good selling point, by which they may receive market advantage comparing to U.S firms which operate in the similar business.

Cloud Act: Risks vs Opportunities

Contact Details

If you would like to know more information about the subjects covered in this publication, please feel free to contact the following people or your usual Llinks contact.

Author	
Xun Yang Tel: (86 21) 3135 8799 xun.yang@llinkslaw.com	
Shanghai	
David Yu Tel: +86 21 3135 8686 david.yu@llinkslaw.com	Bernie Liu Tel: +86 21 3135 8678 bernie.liu@llinkslaw.com
Selena She Tel: +86 21 3135 8770 selena.she@llinkslaw.com	Nicholas Lou Tel: +86 21 3135 8783 nicholas.lou@llinkslaw.com
Dali Qian Tel: +86 21 3135 8676 dali.qian@llinkslaw.com	Kenneth Kong Tel: +86 21 3135 8777 kenneth.kong@llinkslaw.com
David Wu Tel: +86 21 6043 3711 david.wu@llinkslaw.com	David Pan Tel: +86 21 3135 8701 david.pan@llinkslaw.com
Elyn Jiang Tel: +86 21 6043 3710 elyn.jiang@llinkslaw.com	
Beijing	
David Yu Tel: +86 10 8519 2266 david.yu@llinkslaw.com	Bernie Liu Tel: +86 10 8519 2266 bernie.liu@llinkslaw.com
Yuhua Yang Tel: +86 10 8519 1606 yuhua.yang@llinkslaw.com	
Hong Kong (in Association with Vivien Teu & Co LLP)	
David Yu Tel: +86 21 3135 8686 david.yu@llinkslaw.com	Sandra Lu Tel: +86 21 3135 8776 sandra.lu@llinkslaw.com
London	
Yuhua Yang Tel: +44 (0)20 3283 4337 yuhua.yang@llinkslaw.com	