Evolving landscape for international cloud providers in China: why US technology giants are pairing up with local partners

Foreign investment in cloud services is heavily restricted in China. For years, international cloud operators have been struggling to identify structures that address regulatory concerns, but at the same time enable a service delivery model that is consistent with international offerings. Teaming up with Chinese companies is not something new, but it has become a more prominent feature in the cloud space following certain regulatory developments in 2017, notably new licensing requirements issued by the Ministry of Industry and Information Technology ("MIIT"), China's telecommunications industry and internet regulator, as well as the implementation of PRC Cyber Security Law (the "Cyber Security Law").

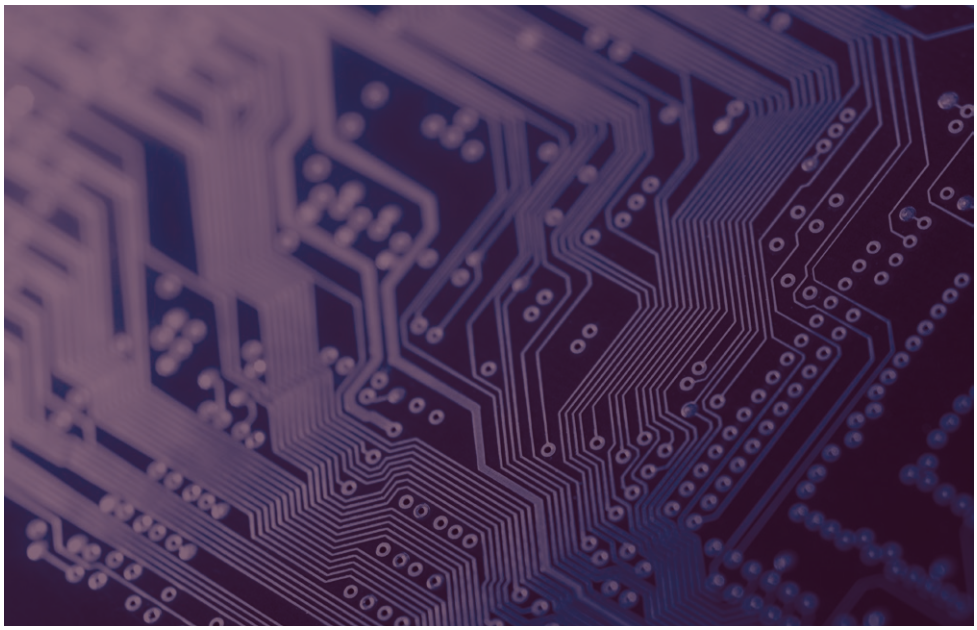
In the past few months, multiple US technology companies have announced their partnerships with Chinese cloud license holders, naming such Chinese partners as "operators" of their cloud services in China. These cross-border partnerships represent the latest trend in China's cloud industry. This note examines how these US-based technology giants are structuring their China service delivery models, which may provide guidance to others that are looking to enter the Chinese cloud services market, a market which is expected to grow 30% year on year for the next five years, with a value exceeding USD 100 billion by 2020.

> “The Chinese cloud services market is expected to grow 30% year on year for the next five years.”

Licensing requirements for cloud operators in China

To understand this somewhat challenging area and to put it into context, you have to go back to China's liberalisation commitment in this sector when it joined the World Trade Organisation ("WTO"). The resulting commitments allowed foreign investment of up to 50% in Value-Added Telecoms Services ("VATS") and up to 49% in Basic Telecoms Services ("BTS"). However, what is less well understood is that when the section in the WTO accession schedule setting out China's sector-by-sector commitments on VATS (which reads "Value-added telecoms services, including the following [...]" and then lists certain VATS services) was being negotiated, those on the other side of the negotiating table to China interpreted "including" to be the lawyer's "including, without limitation", while MIIT has consistently taken the view that "including" means "namely", so China has no obligation to liberalise any sector not expressly included in the WTO text. Internet Data Centres ("IDC") are classified as a VATS, but are notably absent from the WTO schedule. Hence as far as MIIT is concerned, there is no commitment to open up this sector to foreign investment. The classification of services into VATS and BTS is set out in the Catalogue for the Classification of Telecoms Services, the latest iteration of which took effect on March 1, 2016 (the "Telecom Catalogue").

Operating cloud services in China generally requires a VATS business operating permit (a "Permit") issued by the MIIT, although there is some debate over whether certain elements of Software-as-a-Service ("SaaS") models require a VATS Permit. A Permit is clearly required for IDC services, a category more meant to cover the hardware aspects of cloud services, in particular the operation of Internet data centers. Beginning March 1, 2016, a separate license was, *de facto* required for Internet Resource Collaboration ("IRC") services, which is set out as a subset of IDC in the Telecoms Catalogue. MIIT has confirmed that this sub-category under IDC covers "cloud services", in the draft Circular on Regulating Business Activities in the Cloud Services Market, issued for public comment in November 2016 ("Draft Cloud Circular"). Please refer to the



detailed discussion of this circular in our client note of January 2017 (see our briefing http://www.hoganlovells.com/en/publications/draft-legislation-to-affect-china-cloud-services-market-access).

"Cloud services" were not defined in the Draft Cloud Circular, and may, based on recent market practices, be broadly interpreted to cover three types of services: Infrastructure-as-a–Service ("IaaS"), Platform-as-a-Service ("PaaS") and SaaS. Based on a circular issued by MIIT in January 2017 ("2017 Circular")[28], cloud businesses established after March 1, 2016 must now obtain an IRC Permit as well as an IDC Permit before going into operation. Cloud businesses with IDC Permits that were operational prior to March 1, 2016 (subject to a notice requirement) had until December 31, 2017 to obtain an IRC Permit in addition, failing which they had to cease engaging in the business.

On January 12, 2018, MIIT issued another circular to reconfirm its position on the requirement for an IRC Permit to engage in cloud business, together with a list of more than 100 companies that have obtained IRC Permits ("IRC License Holders List"), including major Chinese cloud players such as Alibaba and Tencent, as well as local partners of overseas cloud operators, as well as listing those who did not requalify for on IRC Permit.

Foreign participation in cloud services

As noted above, MIIT takes the view that IDC, and hence by extension IRC, services are not open to foreign investment, and by making IRC a subset of IDC in the Telecoms Catalogue, MIIT effectively made IRC off-limits to foreign investment as well, thereby severely limiting direct equity participation options in the cloud space. There are, however, several potential options that foreign investors can consider when seeking to participate in the cloud space in China. None of these are a panacea and each has its own pros and cons. Sometimes it may be necessary to mix and match.

Investing through a Hong Kong entity qualified under the Mainland China / Hong Kong Closer Economic Partnership Arrangement ("CEPA")

In strict legal terms, this is the only option for foreign investors to access the Chinese cloud market (primarily IDC as it does not expressly cover IRC) through equity ownership. Under the relevant rules, a CEPA-qualified Hong Kong service provider entity is allowed to establish an equity joint venture with a local Chinese company to engage in IDC business, with the level of Hong Kong ownership capped at 50%. The ownership of Hong Kong companies is not subject to foreign investment restrictions in this sector, meaning that the Hong Kong joint venture partner can be 100% foreign-owned. However, the arrangements remain subject to approval by MIIT, which in practice is not always supportive of equity joint

ventures based on a CEPA arrangement, and, consistent with its restrictive interpretation of China's WTO commitments, has interpreted CEPA as only applying to investors where the ultimate shareholder is from Hong Kong, notwithstanding the fact that this restriction is not set out in CEPA itself.

VIE structures

The well-known variable interest entity ("VIE") structure typically involves a foreign investor entering into a series of contractual arrangements with a Chinese VATS Permit holder that enables the foreign entity to exercise effective control over the licensed business, and seeks to achieve an equity-like return in a sector restricted to foreign investment. VIE structures are popular in industry sectors restricted for foreign investment, including the telecoms and internet sectors, as well as those where in many cases foreign participation is prohibited, such as many media-related sectors, but do involve substantial risks to foreign investors.

Essentially, the foreign investors have to control the nominee shareholders that own the domestic capital VATS Permit holder. If these nominees turn against the foreign investor and claim outright ownership, they may use, among others, threats of reporting the VIE structure to the regulators because the structure has never been expressly recognized by the Chinese government. Indeed some recent arbitration cases resulted in it being successfully challenged on the basis it was a circumvention of the requirement for the foreign investor to obtain a VATS Permit (with MIIT approval) through a foreign-invested enterprise in China.

In February 2015, the PRC Ministry of Commerce proposed a draft Foreign Investment Law, in which it cast doubt on the legality and sustainability of VIE structures involving control by a foreign investor in restricted sectors (such as all telecoms/internet sectors, including IDC/IRC). This could have a far-reaching impact on many VIEs in China, resulting in challenges for those who have made use of it. However, this proposal has not yet been made law, and there is some expectation that there will be some form of grandfathering or transition for existing VIE structures, as billions of dollars have been invested in PRC businesses through VIE structures, with the businesses listed in Hong Kong and the US. Expectation is not always the same as what transpires in practice, as those who watched the unwinding of the predecessor Chinese-Chinese-Foreign structures can bear witness. The difference this time around is the personal fortunes of many Chinese entrepreneurs are in the mix too. Notwithstanding the well-known risks, *faute de mieux* the VIE structure is still the most commonly used structure for foreign investors to enter restricted sectors in China.

> Multiple US technology companies have announced their partnerships with Chinese cloud license holders.

However, MIIT appears to take the view that cloud and IDC services are too sensitive to be controlled by foreign investors through VIE structures, and so the apparent administrative tolerance for VIE structures in other restricted sectors does not generally extend to this space. In practice, MIIT may exert pressure on the foreign investor's Chinese partner or VATS Permit holder to remove control elements that are viewed as too aggressive. As things stand now, a full-on version of the VIE structure as seen in the venture capital world in other telecoms/Internet sectors, for example, seems to be a non-starter for large-scale cloud businesses in China.

Technical cooperation with a domestic Chinese company that is a license holder

Currently MIIT seems to be more comfortable with technical cooperation models for delivery of cloud services in the PRC, in which (1) a PRC domestic capital VATS Permit holder enters into customer-facing contracts, and (2) the foreign cloud service provider enters into cooperation agreements to provide technical support to the VATS Permit-holding domestic capital company. This model is supported by the Draft Cloud Circular, which acknowledges that licensees may enter into technical cooperation arrangements provided that the PRC VATS Permit holder reports its technical cooperation to MIIT in writing. The Draft Cloud Circular has still not become law, but in practice MIIT is implementing most of its provisions. As noted in our note of January 2017 (see our briefing http://www.hoganlovells.com/en/publications/draft-legislation-to-affect-china-cloud-services-market-access), the following activities are not permitted during the course of collaboration:

a) the leasing, lending or transfer of a telecommunications services operating license to a partner in a disguised manner by any means, or providing to any partner the resources, venues, facilities or other conditions for unlawful operations;

b) a partner entering into contracts directly with users;

c) using only the trademark and brand of a partner to provide services to users;

d) unlawfully providing to any partner user personal information and network data; and

e) other activities which violate laws and regulations.

Items (b) and (c) are particularly challenging to branded overseas cloud service operators, as this means you cannot 'own the customer' and can only co-brand the cloud services.

Cyber security law implications

On June 1, 2017, the Cyber Security Law came into effect. This is a law with

profound implications for global companies doing business in China. See our bulletin on this (http://www.hoganlovells.com/en/publications/china-passes-controversial-cyber-security-law). The cloud services sector is impacted in a number of important ways. Among other things, the Cyber Security Law requires:

a) **Data localization:** Operators of "critical information infrastructure" must store personal information and "important data" collected during its operations within mainland China, unless the transfer offshore has been approved. The State Council has yet to come up with a final definition for "critical information infrastructure operator".

b) **Obligations to provide law enforcement assistance:** Network operators are required to maintain weblogs for six months and provide technical assistance and support to law enforcement investigations.

c) The Security Assessment for Personal Information and Important Data Transmitted Outside of the People's Republic of China Measures (Amended) **("Draft Rules on Overseas Data Transfers")**: issued in connection with the Cyber Security Law (see our bulletin here http://www.hoganlovells.com/en/publications/chinas-draft-data-localisation-measures-open-for-comment) *de facto* widen the net by imposing a variant of the data localization measure (i.e. you cannot transfer overseas without clearing the security review) on "network operators" , which is a very broad concept that is thought to includes cloud service operators in the PRC, so as to make overseas transfers of personal information and important data collected by network operators subject to a security review by the Chinese government and consent from the data subject. These rules were meant to come into effect at the same time as the Cyber Security Law, but were put on hold as they proved to be hugely controversial, especially as the scope went beyond the scope of the Cyber Security Law.

As noted above, although uncertainties exist as to scope of the Cyber Security Law and its applicability to cloud services providers and operations, it appears likely that cloud service providers with operations in mainland China will be required to:

a) locate their service facilities and network data within mainland China, where such services are provided to customers in China; and

b) ensure that any cross-border data transfers comply with relevant rules, including the Draft Rules on Overseas Data Transfers (when they become law).

Analysis of shared model and conclusions

Recently announced cases involve US technology companies providing different types of cloud services, including IaaS, PaaS and SaaS on a large scale. Nevertheless, broadly speaking, they appear to have taken a similar approach to providing cloud services in China, as follows:

a) Local VATS Permit holder(s) will enter into contracts with end customers and provide cloud services in their own name;

b) Cloud services are co-branded;

c) The local VATS Permit holder will operate the cloud services, while receiving technological support from its foreign partner; and

d) Data centres to support the service offering and store the cloud service data are either owned by the local VATS Permit holder or leased from licensed third party vendors, and are located in China.

These all seem to be driven by the Draft Cloud Circular and the Cyber Security Law. However, in reality, customers are choosing to purchase these cloud services not because of the local VATS Permit holding entity that fronts the business, but the technology provided by, and the brand or co-brand of the big name behind it. Essentially, it has to be the global technology provider that will take the lead in managing the core functions of the business, so that people can get comfortable with the quality of the services provided to customers in China, many of whom are Chinese subsidiaries of their global clients. This is not easily achievable in the light of the laundry list of restrictions for such cooperations, not to mention those imposed by MIIT when the cooperation is reported to MIIT. With this in mind, the cooperation relationship must be structured properly, which means satisfying regulatory requirements while granting a minimum level of operational control that is acceptable to the global cloud services provider.

The cooperation structure may also take on board certain elements of a VIE structure. As discussed above, it is virtually impossible to adopt all the elements of a typical VIE, which will result in full control, and such attempts have in our experience been resisted by MIIT. Local partners on the other hand may be willing to accommodate a lot of onerous terms, as they are primarily incentivised by the financial benefit generated from the cloud operations. However, technical cooperations need to be reported to MIIT, which may review the terms of cooperation, so overly aggressive terms will not necessarily work.

For new-comers to the China market, no matter you are providing IaaS, PaaS or SaaS, unless you can get comfortable your model of SaaS does not require on IDC/IRC VATS Permit, you will likely need to team up with a Chinese VATS Permit holder, and structure the cooperation relationship in such a way as to strike a delicate balance between meeting regulatory requirements and achieving

operational autonomy. With our deep, practical, hands-on experience in this area, we are ideally placed to help you achieve that balance and to guide you through what can often be a tricky negotiation with your Chinese partner and/or the MIIT.

Liang Xu
Partner, Beijing
T +86 10 6582 9577
liang.xu@hoganlovells.com

Roy Zou
Partner, Beijing
T +86 10 6582 9596
roy.zou@hoganlovells.com

Mo Chen
Associate, Beijing
T +86 10 6582 9555
mo.chen@hoganlovells.com

Andrew McGinty
Partner, Shanghai
T +86 21 6122 3866
andrew.mcginty@hoganlovells.com

Mark Parsons
Partner, Hong Kong
T +852 2840 5033
mark.parsons@hoganlovells.com