Client Alert

January 2017

China Looks to Tighten the Regulation of Cloud Services

By Gordon Milner, Chuan Sun and Paul McKenzie[1]

What You Need to Know:

China has issued a new draft law tightening the regulation of cloud services. The draft:

- covers onshore hosted SaaS and PaaS (but possibly not IaaS)
- imposes new restrictions on cross-border partnerships that may render some current arrangements unworkable
- imposes obligations on cloud service operators to monitor and police users of their platforms
- increases data security and breach reporting requirements

While the law is only in draft form, its key components are consistent with other recent Chinese Internet-related regulation and seem unlikely to change materially. In order to minimize potential business impact when the final form of the law is enacted, participants in the space should start reviewing their current operating structures and practices now.

Background

The market for cloud services in China has seen substantial growth in recent years. Homegrown services such as Aliyun have been joined by well-known international service providers, which have set up Chinese-hosted operations in conjunction with local partners.

As a relatively novel industry, cloud services were not specifically addressed under Chinese law until December 2015 when the Ministry of Industry and Information Technology (MIIT) updated the *Telecommunication Catalogue* (the "Catalogue") to include "Internet resource collaboration services" (IRCS) as a new subcategory of Internet Data Center services. While clarifying that the provision of cloud services requires a value-added telecoms license, the Catalogue did not provide detailed guidance regarding how cloud services would be regulated.

On November 24, 2016, MIIT issued a draft *Circular on Regulating the Operations of the Cloud Service Market* (《关于规范云服务市场经营行为的通知》, the "Draft") for public comment. While the final formal circular has not yet been issued, the Draft clearly indicates MIIT's intent to impose strict restrictions on the ability of foreign cloud service providers to participate in the Chinese market.

[1] The authors thank Shanghai consultant Liwen Zhang for her assistance in preparing this client alert.

Definition of Cloud Services and License Requirements

In defining "cloud services," the Draft adopts the concept of IRCS from the Catalogue. The Catalogue defines IRCS rather broadly as:

> [the use of] equipment and resources installed in a data center to provide users with data storage services, development environments for internet applications, and deployment and operation management of internet applications via the Internet or other networks, using sharing of resources to allow users to scale as fast or as much as needed.

In this note, we refer to the operators of IRCS as "Operators".

This definition is somewhat broad and would almost certainly capture most platform as a service (PaaS) and software as a service (SaaS) offerings. As such, an Operator of PaaS or SaaS hosted in China will require an Internet Data Center value-added telecom service license ("IDC License") specifically covering IRCS.

On its face, this definition would arguably not include pure infrastructure as a service (IaaS) offerings and the applicability of the Draft to such services is therefore uncertain at this stage. To the extent that they are not covered by the Draft, it seems likely that MIIT will treat IaaS offerings hosted in China as falling within the broader category of Internet Data Center services. As such, operators of IaaS will still likely require an IDC License (although perhaps without specific coverage of IRCS).

The Draft prohibits telecommunications companies from providing network infrastructure or services to any cloud services Operator lacking the necessary IDC License.

Tighter Restrictions on Foreign Participation

Investment and Partnership Models

Foreign investment in the telecommunications industry is restricted under Chinese law. The *Administrative Provisions on Foreign-Invested Telecommunications Enterprises (amended in 2016)* (《外商投资电信企业管理规定》(2016 年修订)) provides that an onshore foreign invested telecommunications enterprise (FITE) is eligible to hold an IDC License only if the foreign investor's equity share does not exceed 50%.[2] In practice, so far as we are aware, MIIT has not issued any IDC Licenses to FITEs regardless of whether they meet this requirement. The Draft does not affect these restrictions on foreign investment.

Foreign cloud service providers have implemented a variety of structures in order to participate in the Chinese market notwithstanding these restrictions. Typically, the foreign party:

(i) licenses its brand and provides specialist cloud technology and other resources to a local telecoms value-added license-holding Operator;

(ii) exerts a degree of contractual control over the cloud service (for example, the service packages offered, marketing, quality control, hardware and software platform used, and data); and

[2] An exception exists under the *Closer Economic Partnership Agreement* between mainland China and Hong Kong/Macau (CEPA) pursuant to which qualifying Hong Kong or Macau incorporated data center providers are able to hold up to a 50% equity interest in a FITE that is eligible to hold an IDC license. In practice, such arrangements remain relatively rare and it is unclear whether such a joint venture would be eligible to hold an IDC License specifically covering IRCS, as would be required to operate SaaS and PaaS.

(iii) extracts value from the Operator through license, rental, and/or consulting fees.

The net effect of these partnership models is to produce a business which, from a customer-facing perspective, is essentially indistinguishable from the foreign service provider's offering outside of China.

New Restrictions on Partnership Models

While the Draft does not *per se* prohibit cloud service partnership models, it does set out several requirements aimed at regulating and limiting the scope of such arrangements, including (*inter alia*):

1. Operators are required to proactively report cloud services cooperation arrangements to MIIT;
2. an Operator's foreign partner must not directly enter into any contract with any user (this could include agreements couched as software licenses as well as service subscription agreements);
3. the relevant cloud services cannot be branded solely with the foreign partner's trademark;
4. an Operator must not illegally provide its foreign partner with users' personal information or network data;
5. an Operator must not provide any resource, site, facility, or other assistance to its foreign partner facilitating any illegal telecoms operations; and
6. an Operator must not lease or transfer its IDC License to its partner in any form.

Restrictions (5) and (6) are couched in very broad language. This reserves considerable latitude to MIIT and creates uncertainty as to how the restrictions would be applied in practice. There is, for example, no bright-line test as to the circumstances in which MIIT would view an IDC License as being leased or transferred to a foreign partner. That said, the language is similar to the wording used in the 2006 *Notice of the Ministry of Information Industry*[3] *on Strengthening the Administration of Foreign Investment in Value-added Telecommunications Services* (《信息产业部关于加强外商投资经营增值电信业务管理的通知》). Based on our experience with the earlier notice, there is at least some risk that if the cloud services are substantially provided by the foreign partner and the Operator is merely providing an optical and contractual front end to the business, MIIT will take the view that the Operator has leased or transferred its IDC License to the foreign partner.

Taken together, these restrictions will present difficulties for the more extreme "thin operator" models which may need to be restructured to clarify branding and provide a more substantial role for the local Operator. That said, the Draft does at least provide a much-needed degree of certainty as to what types of model can be safely operated in China.

Monitoring and Policing Obligations

The Draft imposes a raft of obligations on Operators to monitor and police customers who use their cloud service to host websites and/or applications. These include, *inter alia*:

1. implementing real-name customer registration protocols;
2. actively supervising the use of the platform in accordance with the terms of customer agreements;
3. reporting any unlawful use of the platform to MIIT and taking steps to rectify such use; and

[3] This is the name of the predecessor of MIIT.

4. censoring, keeping records of, and reporting to the authorities, any distribution via the service of information deemed unlawful under Chinese law.

These requirements echo similar stipulations in the more generally applicable *Cyber Security Law* (《网络安全法》) and Anti-Terrorism Law (《反恐怖主义法》) and appear designed to make clear that the recently evolved censorship and control regime also applies to the dissemination of material through cloud service platforms. Given the wide-ranging nature of material hosted via cloud services, cloud service providers may find such active supervision obligations challenging.

Once MIIT publishes the final form of the circular, Operators will need to review and update their policies and customer agreements in order to accommodate such requirements. Given the lead time inevitably required to implement the necessary changes with customers and the likelihood that the administration requirements set out in the Draft seem unlikely to change materially in the final version, we recommend that Operators start reviewing their policies and user agreements now.

Security of Network Data and Personal Information

The Draft requires that Operators locate network data in China when providing services to domestic users and comply with relevant rules and regulations when undertaking cross-border data flows. The Draft also requires Operators to establish robust data management systems to ensure the security of network data and personal information. Specifically, Operators must:

1. establish and notify users of rules for collecting and using personal information;
2. implement protection standards to protect network data and users' personal information against data theft and tampering (note that the Draft is silent as to the specific standards required);
3. report any data beach to MIIT, notify users immediately, and take mitigation measures;
4. stop collection and use of personal information after users cease using the service; and
5. provide at least three months' notice to MIIT and all users before ceasing to provide the services, and accommodate users' requirements regarding data storage.

These requirements are generally consistent with the *Cyber Security Law* and the 2013 *Regulation on Protecting Personal information of Telecom and Internet Users* (《电信和互联网用户个人信息保护规定》). Operators should already be in the process of reviewing their policies and customer agreements for compliance with the *Cyber Security Law* and should consider addressing the additional requirements from the Draft as part of that process.

System Requirements and Internet Gateway

The Draft requires that Operators host the cloud service platform in mainland China when providing services to domestic users.

The Draft requires each Operator to establish several systems to support its cloud services business, including (*inter alia*) a service quality guarantee system, a user complaint handling mechanism, a network information security management system, a security assessment system for new technologies and new business operations, and an emergency response system.

In the event that it needs to connect a server to an overseas network, an Operator must utilize an international business Internet gateway approved by MIIT. The use of other methods such as leased private lines, VPN, or other self-established or third-party channel for international networking is prohibited. The net effect is that international connections will need to traverse China's Golden Shield national firewall. This will typically have a material adverse effect on latency and may need to be taken into account when planning cross-border integration of cloud services.

We will continue to monitor the progress of the Draft and will provide further updates in due course when MIIT issues the formal circular in final form.

Contacts:

Gordon Milner	**Chuan Sun**	**Paul D. McKenzie**
(852) 2585-0808	(852) 2585-0762	86 (10) 59093366
GMilner@mofo.com	CSun@mofo.com	PMcKenzie@mofo.com

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on The American Lawyer's A-List for 13 straight years, and Fortune named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.