# Chambers

## GLOBAL PRACTICE GUIDE

Definitive global law guides offering comparative analysis from top ranked lawyers

# TMT

**China**
DaHui Lawyers

chambers.com

2019

# Law and Practice

*Contributed by DaHui Lawyers*

## Contents

**DaHui Lawyers** has a TMT team of ten partners and 58 fee earners based in China, with particular strength in new economy industries as well as complex cross-border transactions. The firm combines in-depth knowledge of China's legal and business landscape with extensive international experience, enabling it to assist multinational companies in the Chinese technology, media and internet/telecoms sectors. DaHui's expertise in these highly regulated sectors attracts clients of all types and sizes in China's emerging but challenging market, and the team provides these clients with effective and solution-oriented services tailored to their diversified business needs.

## Authors


**Cloud Li** is a partner in the firm's TMT practice who has represented European and North American multinationals, large Chinese state-owned and privately held companies, and numerous private equity funds in various TMT-related M&A, investment, dispute, compliance and general corporate matters. He has represented some of the largest and most established participants in China's TMT sector.

**Jonathan Pfister** is a senior member in DaHui Lawyers' TMT and transaction teams, and has advised numerous clients across various sectors of the TMT landscape. He handles a range of issues for companies seeking to operate and invest in China's highly regulated TMT market, as well as Chinese companies looking to invest abroad. His primary practice areas include cross-border M&A, outbound investment, general corporate matters, and private equity and venture capital financing.

**Michael Wang** is an associate in the TMT team with extensive experience in equity financings, market entry and regulatory/compliance issues, and has represented several multinational and domestic TMT clients.


## 1. Cloud Computing

### 1.1 Laws and Regulations

There are no laws or legal regulations in the PRC specifically relating to cloud computing. However, cloud computing service providers are subject to various general bodies of legislation and regulations, including the Telecommunications Regulations of the People's Republic of China (see **8 Scope of Telecommunications Regime**, below), the Cybersecurity Law of the People's Republic of China ('PRC Cyber Security Law', see **6 Key Data Protection Principles**, below), the Counterterrorism Law of the People's Republic of China, and the Administrative Measures for the Licensing of Telecommunications Business and Administrative Measures for Internet Information Service, among others. Moreover, there have been more than 20 non-binding recommended standards published by the Standardisation Administration of China (SAC) relating to cloud computing. Such standards relate to topics ranging from security guidance, data centre requirements and file service application interfaces.

There are also no industry-specific PRC laws or regulations providing for stricter cloud computing regulations in particular industries. In practice, however, banks and financial institutions will typically require various risk-focused arrangements in their cloud systems, such as asking their cloud computing service providers to only install cloud services onto the bank's Local Area Network (LAN) and for the service provider to forgo access to client data.

Cloud computing service providers generally must comply with the requirements of the PRC Cyber Security Law in respect of the collection and use of personal information. This includes obtaining user consent before collecting personal information, and disclosing internal rules for personal information collection, the intended use of such information, its purpose and the means and scope of collection.

In addition, the PRC Cyber Security Law also sets out more strict obligations on 'Key Information Infrastructure Operators' (KIIOs – see **6 Key Data Protection Principles**,below, for more details), which are defined broadly to include

companies heavily connected to industries implicating PRC sovereignty or the economy, or the well-being of PRC citizens, where the collapse of such entities would likely have an adverse impact on the PRC government or its citizens. Although there is no express law or regulation in effect currently identifying cloud services as key information infrastructure, the scale and importance of some cloud computing operators could conceivably cause them to fall within this definition. Indeed, draft guidance from the Cyberspace Administration of China (CAC), which was issued for public comment in July 2017 (not yet promulgated) specifically includes cloud computing service providers among its listed types of entities that may be deemed as KIIOs.

Therefore, subject to the specific data stored or processed on a cloud computing service, a cloud computing service provider could be required to comply with the more stringent obligations placed on an operator of key information infrastructure under the PRC Cyber Security Law, such as local data hosting and offshore data transfer restrictions. This may result in a cloud computing network with offshore components (eg, servers hosted outside China, or networks between a PRC subsidiary and foreign parent company) having to undergo restructuring to comply with the PRC Cyber Security Law and/or undergo a (currently vaguely defined) security assessment procedure prior to utilising such cloud services.

### 1.2 Regulations in Specific Industries

See **1.1 Laws and Regulations**.

### 1.3 Processing of Personal Data

See **1.1 Laws and Regulations**.

## 2. Blockchain

### 2.1 Risk and Liability

Chinese regulators have materially divergent attitudes towards blockchain technologies versus cryptocurrency. The use of blockchain technologies and their integration into the overall Chinese economy is permitted and even encouraged, while government officials have taken a hard line against cryptocurrencies and initial coin offerings (ICOs). In 2017, both cryptocurrency exchanges and ICOs were banned in China, and offshore websites relating to cryptocurrency trading and ICOs have been blocked.

Blockchain technologies, however, are generally permitted and even encouraged. Notably, a white paper published in October 2016 by the China Blockchain Technology and Industrial Development Forum, under the guidance of the Ministry of Industry and Information Technology (MIIT), analysed the current state of blockchain technology in China and its potential future applications, while setting out a roadmap for blockchain development in China and calling for a formal set of national blockchain standards to provide industry guidance to existing and potential market players. To date, however, no blockchain-related standards have been released.

China is now arguably among the vanguard in the application of blockchain technology. Blockchain technology is already adopted and used by China's e-commerce giants, such as JD and Alibaba, both of which have announced further plans to apply blockchain technology to their logistics services to better allow suppliers and consumers to trace products through production, transportation and storage. Also, China's Ping An bank and Ant Financial both announced blockchain-based applications to maintain ledgers for cross-border transactions. The Nanjing local government even established a RMB10 billion investment fund to invest in blockchain projects.

Additionally, various PRC arbitral tribunals have announced their intention to apply blockchain technology to arbitral proceedings. For instance, there have been reports that the Guangzhou Arbitration Committee worked with WeBank and other parties to develop a blockchain system for arbitration. Under that system, if a borrower defaults on a loan, the Guangzhou Arbitration Committee can automatically issue an arbitral award/ruling based on the information stored via blockchain to all parties involved in the loan's underlying contract. The Nanjing Arbitration Committee also launched a test version of a blockchain-based online ruling system, which allows disputing parties to view digital evidence. The system is reportedly aimed at facilitating the rapid conclusion of arbitration proceedings.

On 10 January 2019, the CAC promulgated the Provisions on Administration of Blockchain-based Information Services('Blockchain Services Provisions'), which represent the first administrative guidelines for providers of non-crypto currency, blockchain-based services in China. The Blockchain Services Provisions define blockchain-based service providers as entities or nodes that provide blockchain-based information services, or any institution or organisation that provides technological support to such entities ('Blockchain Service Providers').

Under the Blockchain Services Provisions, Blockchain Service Providers are responsible for information security and should build internal management systems for user registration, information censorship, emergency response and security protection. The Blockchain Services Provisions require Blockchain Service Providers to conduct a record-filing with the CAC or its provincial-level branch to report certain key information, such as the type and scope of services, application sectors and server addresses, within ten business days after launching their services. Blockchain Service Providers are also required to undertake a security evaluation administered by the CAC or its provincial branches.

Furthermore, Blockchain Service Providers are required to authenticate the identities of their users based on ID card numbers, organisational codes (for PRC entities) or mobile phone numbers before providing services to such users in accordance with the Cyber Security Law.

The Supreme People's Court of China (SPC) has also supported the use of data contained in blockchains in Chinese Internet courts. Under the Provisions of the SPC on Several Issues Concerning the Trial of Cases by Internet Courts, issued on 6 September 2018, Internet courts are required to recognise data submitted as evidence that has been stored on a blockchain. Such blockchain-stored data, however, must have been collected and stored via blockchain with digital signatures and the party wishing to use the evidence must establish the authenticity of the technology used.

### 2.2 Intellectual Property

A blockchain-based application will typically be in the form of computer software, which may make it subject to copyright protections under PRC law. If the application is sophisticated enough (eg, if it includes sufficient technical elements in addition to being mere computer algorithms or business method), and if the application constitutes a solution to a technological problem, then it could be considered patentable under China's patent law. It is reported that in 2018 alone, more than 1,000 patent applications relating to blockchain technology have been filed in China. That said, many blockchain technologies are based, at least partially, on open source software, which will generally be governed by the terms of an open source licence. That licence may impose restrictions on patent applications or contain provisions jeopardising patent enforcement.

### 2.3 Data Privacy

There are no specific PRC rules on data privacy that relate to blockchain technologies specifically. However, an operator of blockchain services would be subject to various other PRC laws and regulations relating to data privacy, such as under the PRC Cyber Security Law. This may require a provider of blockchain services or operator or blockchain technologies to obtain consent before collecting personal information from users, and disclose internal rules for personal information collection, the intended use of such information, its purpose and the means and scope of collection.

Further, blockchain service providers who are engaged in certain industries could be deemed to be operating 'key information infrastructure', making them subject to more strict obligations under the PRC Cyber Security Law. In particular, this may include operators of blockchain services in financial or real estate sectors. If such a service provider qualifies as an operator of key information infrastructure, any personal information collected through a given blockchain could not be transmitted outside of China without undergoing additional security assessment procedures, which may require that all nodes of the blockchain be located within China as well.

### 2.4 Service Levels

Currently, there are no specific PRC laws or regulations on any service levels or service level agreements (SLAs) for an operator of blockchain services. That said, the SAC recently promulgated recommended national standards on SLAs for cloud computing as prepared by the China National Information Technology Standardisation Committee (CNITSC), ie, Information technology – Cloud computing – Basic requirements of cloud service level agreement (CSLA) (GB/T 36325-2018). The CNITSC has also promulgated an industrial standard on SLAs, ie, Information Technology Service – Guidelines on Service Level Agreement (SJ/T 11691-2017). While none of these standards are compulsory standards, there appears to be an increasing number of Chinese Internet and software service providers adopting some level of SLAs. As such, SLAs are expected to evolve primarily in light of technical and commercial considerations between blockchain service providers and users.

### 2.5 Jurisdictional Issues

Because the nodes of a blockchain could potentially be dispersed across servers located in multiple countries and jurisdictions, the question of which laws the blockchain will be subject to is complicated and has not been specifically addressed by PRC law within the blockchain context. However, because the definition of Blockchain Service Providers under the Blockchain Services Provisions covers 'nodes', the rules provided by the Blockchain Services Provisions should at least be applicable to hosts of Chinese nodes used for blockchain information services (defined as information services provided to the public using blockchain-based technology and in the form of Internet websites, mobile applications etc). That said, since the Block Services Provisions are only an administrative provision, under current PRC law and in the absence of an agreement among relevant blockchain parties on governing law and forum selection, whether or not a blockchain is subject to PRC law will be governed by standard PRC choice of laws and forum selection rules under the PRC Civil Procedure Law and the Law of the People's Republic of China on Application of Laws to Foreign-Related Civil Relationships. Even under these laws, there remain uncertainties; for instance, whether having a single blockchain node located on a server in the PRC will be sufficient to subject the entire blockchain to PRC jurisdiction, or whether something more is required.

## 3. Legal Considerations for Big Data, Machine Learning and Artificial Intelligence

### 3.1 Big Data

Currently, there are restrictions on foreign investment into big data companies. The Telecommunications Business Catalogue, published in 2015 by the MIIT, lists the operation of an Internet data centre (IDC) as a business that requires a value-added telecommunications operating permit. Currently, as this permit cannot be obtained by a foreign-invested entity, generally foreign entities are required to outsource their data storage and data analysis services to local PRC IDCs. Indeed, since 28 February 2018, the Apple iCloud service in mainland China (which formerly operated via an offshore service provider) has been transferred and operated by Guizhou-Cloud Big Data Industry Development Company, a PRC IDC.

Beyond these foreign investment restrictions, there are no laws or regulations in the PRC specifically applying to 'big data' companies or providers of 'big data'-type services, such as big data analytics and consulting services. As such, there are no statutory limitations or allocations of liability or insurance requirements applicable to duly established big data companies.

Generally, big data companies will be subject to the requirements of the PRC Cyber Security Law, which will require that informed consent be procured from users or data subjects before a company can collect and process their personal information. In the case of a big data service provider, such consent should indicate that the user's personal information will be used specifically to produce data analytics or provide consulting services.

Moreover, a big data service provider may be deemed an operator of key information infrastructure and therefore subject to stricter compliance requirements, including the requirement to store all personal information within the PRC and the restrictions on transmitting such data outside the PRC without performing certain security assessment procedures. That said, if a big data service provider undertakes anonymisation (ie, technologically processing personal information to make the personal information subject unidentifiable and non-recoverable) when processing personal information, the ultimate analytics and consulting services may not be subject to the restrictions of the PRC Cyber Security Law on divulging personal information without the data subject's consent.

### 3.2 Machine Learning

There are no PRC laws or regulations specifically pertaining to the creation, development or use of machine learning algorithms or technologies. As such, there is no PRC legislation on the allocation of liability or setting insurance requirements on companies providing products or services employing machine learning algorithms or technology.

As the operation of machine learning algorithms tend to require large data sets, service providers obtaining such data will be subject to the requirements of the PRC Cyber Security Law. As such, for any personal information obtained directly from data subjects, informed consent must be obtained, and such consent should indicate that the data subject's personal information will be used specifically for machine learning purposes. If such data is obtained from a third-party source, care should be taken to ensure that appropriate consents were obtained by the entity that collected any personal information, or that such personal information is anonymised.

A software program employing machine learning technology likely will be subject to copyright protections under PRC law. However, machine learning algorithms themselves will be very difficult to patent in the PRC. Moreover, any machine learning software that is based on open source software will generally be governed by the terms of an open source licence. That licence may impose restrictions on patent applications or contain provisions jeopardising patent enforcement.

### 3.3 Artificial Intelligence

There are no PRC laws or regulations specifically pertaining to the creation, development or use of artificial intelligence (AI). As such, there is no PRC legislation specific to the use of AI on the allocation of liability or setting insurance requirements on companies providing products or services employing AI.

As the operation of AI tends to require large data sets, service providers obtaining such data will be subject to the requirements of the PRC Cyber Security Law. As such, for any personal information obtained directly from data subjects, informed consent must be obtained, and such consent should indicate that the data subject's personal information will be used specifically for AI purposes. If such data is obtained from a third-party source, care should be taken to ensure that appropriate consents were obtained by the entity that collected the personal information or that the personal information is anonymised.

With respect to the ownership of intellectual property rights, under the Copyright Law of the People's Republic of China ('PRC Copyright Law'), only natural persons, legal persons or organisations can be entitled to copyrights. As a result, PRC law currently appears to suggest that any works and content created by AI cannot currently be protected under the PRC Copyright Law.

## 4. Legal Considerations for Internet of Things Projects

### 4.1 Restrictions Affecting a Projects' Scope

Chinese legislators have taken a relatively broad view of the concept of 'Internet of Things' (IoT). The Guiding Opinions of the State Council on Promoting the Orderly and Healthy Development of Internet of Things (Guo Fa [2013] No 7, the 'IoT Opinion') describes IoT as technologies "based on the intensive integration and comprehensive application of a new generation of information technology" and designated IoT as an important strategic emerging industry of the country. The IoT Opinion further emphasises the co-ordinated overall development of IoT applications, technologies, industry and standards.

Although China has yet to promulgate a comprehensive legislation on the security and regulation of IoT, recent legislation on IoT-related issues, such as data security, data privacy, cloud computing, protection of critical infrastructure, classified levels of security protection, information security etc., are all applicable to IoT and a number of different government departments and regulatory bodies have been involved in the regulation and standardisation of the IoT sector. These government bodies include the MIIT, which is the key regulator for the telecoms sector and about 20 other industries, and the CAC, which acts as the main watchdog for information security and content administration, as well as others such as the National Development and Reform Commission (NDRC), the Ministry of Science and Technology (MOST) and the SAC. When contemplating an IoT project, the following legal issues and relevant rules of PRC law should be considered.

**Operating Permits**

The Telecommunications Regulations of the People's Republic of China apply to all types of 'telecommunications' services. 'Telecommunications' is defined broadly as the "act of using wired or wireless electromagnetic or optoelectronic systems to transmit or receive voice, text, data, image or other forms of information". Under PRC law, telecommunications services are divided into two categories: basic and value-added telecommunications services. The former generally covers important telecommunications infrastructure, while the latter covers the services working in conjunction with that infrastructure; eg, VPN services, Internet data service centres, call centres, etc. In light of this, any infrastructure services for IoT connectivity and networks would likely fall within the definition of 'basic telecommunications services', while other IoT products or services would likely be categorised as 'value-added telecommunications services'.

Therefore, depending on the type of services being provided, a business operator may need to obtain either a Basic Telecommunications Service Operating Permit or a Value-Added Telecommunications Services Operating Permit before bringing an IoT product or service to market. Each permit will require a telecommunications services operator to meet different requirements, which may include an absence of foreign investment, which could make a particular IoT service or product effectively prohibited to foreign investment.

**Information Security and Data Protection**

While there is no specific law on the information security of IoT, the general rules of the PRC Cyber Security Law are generally applicable to the IoT sector; in particular, the rules regarding confidentiality and safekeeping of personal information of consumers, and protection of privacy (further elaborated in relevant sections below). If an IoT service provider is deemed as operating key information infrastructure, then it will be subject to more stringent compliance requirements.

**Standardisation**

The SAC has been working with various governmental bodies and industrial associations to devise national standards in the IoT sector. From 1 January 2019, ten IoT standards will be implemented to cover the information sharing, security, network connectivity etc, including GB/T 36478.1-2018 (Internet of things. Information sharing and exchanging. Part 1: General architecture), GB/T 36478.2-2018 (Internet of things. Information sharing and exchanging. Part 2: General technical requirements), GB/T 36468-2018 (Internet of things. General principles of stipulation on evaluation indicator system), etc. While the national standards in the IoT sector are mostly recommended standards (GB/T standards) rather than mandatory standards (GB standards), IoT device manufacturers and service providers will need to consider if their products/services are compatible with the relevant national standards.

## 5. Challenges with IT Service Agreements

### 5.1 Specific Features

By and large, the PRC legal framework concerning IT service agreements presents many of the same common issues found in other jurisdictions. In particular, provisions dealing with indemnification and liability caps for data breaches, service outages and other service malfunctions tend to be among the most heavily negotiated clauses of IT service agreements in China. Another routinely contested contractual issue concerns a service provider's reporting obligations to its customers in the event that it discovers discovered breaches, attempted intrusions, actual intrusions and data leaks. Maintenance timetables and service-level credits, as well as IP ownership of customised software applications are also potential points of discussion. Taken together, these general issues of IT service agreements tend to be deal specific and their resolution is often subject to the risk profiles of the parties involved.

In addition, similar to the practice in the IoT sector, the SAC, the MIIT and the China Communication Standards Association (CCSA) have drafted several national and industrial standards for cloud services (eg, GB/T 36325-2018 (Information technology – Cloud computing – Basic requirements of cloud service level agreement (CSLA)), SJ/T 11691-2017 (Information Technology Service – Guidelines on Service Level Agreement) and YDB 144-2014 (Cloud service agreement reference framework)). These standards are not mandatory but represent official recommendations of PRC government authorities and industry associations.

There are also some considerably unique features and considerations applicable to IT service agreements in the PRC. In light of the rigid regulatory framework and complex operating permit regime in China's telecoms sector (see **8 Scope of Telecommunications Regime**, below), many companies may find that engaging or partnering with an IT service provider is a regulatory necessity, so that an entity can use one or more permits held by the service provider to indirectly provide services or content that would otherwise be restricted. Indeed, this may result in some market players contracting with IT service providers even if they do not technically need some types of third-party IT services or would prefer to handle such activities internally, as doing so may be more convenient and efficient. Because these arrangements may entail a longer-term and more substantive relationship between IT service providers and their customers than would otherwise be the case, such customers should be careful in selecting a local IT service provider to ensure that not only they can provide the necessary IT services, but also to ensure they hold all necessary permits.

Some IT service providers also effectively serve as de facto 'gatekeepers' of Chinese IT and telecoms regulations. According to the Administrative Measures for the Licensing of Telecommunications Business, value-added telecoms operators that provide access services to their customers are prohibited from equipping such customers with the means to conduct restricted activities if the customers lack necessary telecoms operating permits. As such, some service providers may require their customers to hold certain permits to use their services in a given manner. For instance, an Internet service provider may require a customer to hold a value-added telecom service permit to use its Internet access services in conjunction with the customer's e-commerce website. As the interpretation of these licensing requirements may vary among service providers, different services providers may have different requirements for their customers. Therefore, it is recommended that users should be clear from the outset as to the range of services they wish to use, and the IT service provider's requirements for providing those services.

### 5.2 Rules and Restrictions

See **5.1 Specific Features**.

## 6. Key Data Protection Principles

### 6.1 Core Rules Regarding Data Protection

There is no single definitive piece of legislation in the PRC governing data protection. Instead, there are a range of laws and regulations containing data protection provisions that apply to specific parties in a variety of circumstances. Some of the most notable include the PRC Cyber Security Law, the Criminal Law of the PRC (revised in 2015) and the Law of the PRC on the Protection of Consumer Rights and Interests ('PRC Consumer Protection Law'). For example, under the PRC Consumer Protection Law, business operators are required to notify consumers of the purpose, method and scope of information collected from users/customers, as well as how such information will be used, and to obtain consumers' consent prior to collecting such data or transferring it, whether such transfers are made onshore or offshore. These consumer protection restrictions also require business operators to keep any personal information of consumers confidential, and to take technical and other measures to safeguard such information. Additionally, various sources of legislation also provide that PRC nationals have a general right to privacy under PRC law, which includes the right to have their information kept private.

In recent years, the most significant data protection development to impact both domestic and multinational companies operating in China has been the roll out of the PRC Cyber Security Law, which contains various rules applicable to data collected and/or stored on a company's networks. After taking effect on 1 June 2017, the PRC Cyber Security Law is intended to serve as the comprehensive and definitive law governing cyber security in the PRC. In its current form, the law contains many broad provisions and uncertainties that are intended to be clarified by subsequent legislation.

### 6.2 Distinction Between Companies/Individuals

The PRC Cyber Security Law does not make a technical distinction between companies and individuals. However, it does contain important other distinctions both at the level of collectors/handlers of data (typically companies) and at the level of data itself (typically data belonging to consumers/individuals).

At the data collector/handler level, the law distinguishes between 'Network Operators' and the narrower concept of KIIOs. Network Operators are broadly defined as "network owners and administrators, and network service providers." As no further definitions of these three sub-categories is provided, this definition could potentially include any company or individual operating a website or using a company intranet/cloud computing network. KIIOs, on the other hand, are essentially defined to include certain companies heavily connected to industries implicating PRC sovereignty or the economy, or the well-being of PRC citizens, the collapse of which would likely have an adverse impact on

the PRC government or its citizens (eg, major utilities and banks). Different rules and requirements within the PRC Cyber Security Law are applicable to Network Operators and KIIOs, with the restrictions placed on the latter tending to be more onerous.

At the level of data itself, the PRC Cyber Security Law is focused especially on two particular types of network data; ie, 'Personal Information' and 'Important Data'. Personal Information is defined under the PRC Cyber Security Law to include "…all kinds of information recorded by electronic or other means that can be used to identify, independently or in conjunction with other information, a natural person, including name, date of birth, ID numbers, biometric personal information, etc". Important Data is technically undefined under the PRC Cyber Security Law. However subsequent draft guidance sets out many sector-specific types of data deemed as Important Data. For example, for a financial institution, a list of clients would be considered Important Data, if a breach or leak of the list would potentially damage the safety and soundness of that financial institution. Taken together, companies collecting or handling information over a network that could be considered Personal Information or Important Data should take particular caution that they are in full compliance with the PRC Cyber Security Law.

### 6.3 General Processing of Data

In addition to the general data handling and user consent rules noted above in the context of the PRC Consumer Protection Law, the PRC Cyber Security Law also provides data processing rules applicable to all Network Operators in China. For example, Article 10 of the PRC Cyber Security Law requires Network Operators to "take technical and other necessary measures to ensure the secure and stable operation of a network, effectively respond to cyber security incidents, prevent illegal crimes committed on a network, and maintain the integrity, confidentiality and availability of cyber data." Article 21 also provides that Network Operators must formulate internal security management systems and take technological measures to preserve relevant web logs for no less than six months, among other requirements.

Having said that, if a party collecting or handling data in China is deemed as a KIIO, then a collection of more stringent data processing rules will be triggered. Most significant to multinational companies, these heightened data processing rules include a local data-hosting requirement, which requires that all Personal Information and Important Data collected or maintained during business operations in China are hosted on servers physically located in the PRC. Similarly, KIIOs are also restricted from transferring Personal Information or Important Data offshore without performing certain security assessment procedures. Notably, any data transfers between an offshore parent company and a PRC subsidiary that is deemed a KIIO would fall under these local hosting and offshore data transfer restrictions. It is also worth noting that some subsequent draft legislation following the PRC Cyber Security Law has envisioned the expansion of these local hosting and offshore data transfer restrictions to all Network Operators (ie, not just KIIOs); however, this draft legislation has faced significant scrutiny and ultimately it is uncertain whether it will be adopted in the future.

### 6.4 Processing of Personal Data

As noted above, processors of all personal data in the PRC must ensure their compliance with the various consumer protection rules and individual rights to privacy that are generally provided across various sources of PRC law. Typically, the consent of data subjects should be obtained before any personal data is collected, processed, stored or transmitted. Under the PRC Cyber Security Law, Network Operators are required to disclose the intended use and purpose when collecting Personal Information (like Important Data) from data subjects. Moreover, personal information may only be collected if it relates to the services provided by the Network Operator. When processing information, network operators are obligated to not divulge, damage or distort any personal information.

The PRC Cyber Security Law further provides that Personal Information can be provided to third parties, provided that consent of the data subject is obtained in advance. This is generally interpreted to permit the sharing of Personal Information with third-party data processors, with the necessary consent. Indeed, the Personal Information Security Specification (GB/T 35273-2017) addresses delegated processing of personal information and includes compliance recommendations.

The PRC Cyber Security Law also includes a general exception for Personal Information that is anonymised; that is, technologically processed so that the personal information is subject unidentifiable and non-recoverable from the persona information. Anonymised information will not be subject to the restrictions of the PRC Cyber Security Law on divulging Personal Information without the data subject's consent.

## 7. Monitoring & Limiting of Employee Use of Computer Resources

### 7.1 Employees' Restrictions on Computer Use

PRC law provides no rules on the monitoring of employees' use of computer and Internet resources owned by the employer. As such, employers are generally permitted to use various means (eg, monitoring software) to monitor and restrict employees' use of company computer resources.

However, if a company uses such means to collect employees' Personal Information, then under the PRC Cyber

Security Law, the employer may be obligated to notify its employees of its collection methods and obtain employee consent before such collection. This can be accomplished by including appropriate language in the company's employee handbook, and obtaining each employee's acknowledgement that he or she has read and understood the handbook's contents.

## 8. Scope of Telecommunications Regime

### 8.1 Technologies within Local Telecommunications Rules

The Telecommunications Regulations of the People's Republic of China ('Regulations') apply to all types of 'telecommunications' services. 'Telecommunications' is defined broadly as the "act of using wired or wireless electromagnetic or optoelectronic systems to transmit or receive voice, text, data, images or any other form of information."

The Regulations categorise telecommunications services as either 'basic telecommunications services' or 'value-added telecommunications services' and require different operating permits to engage in each. Basic telecommunications services include voice communications services, public data transmission and public network infrastructure, while value-added telecommunications services consist of call centre services, Internet data centre services, CDN services, VPN services and others. A complete list of services or business qualifying as basic telecommunications services and value-added telecommunications services can be found in the Telecommunications Business Catalogue, as amended in 2015 by the MIIT.

Therefore, depending on the type of telecommunications services being provided, prior to bringing a service to market, the telecommunication operator will need to obtain either a Basic Telecommunications Service Operating Permit or a Value-Added Telecommunications Services Operating Permit. Each permit requires a telecommunications services operator to meet different requirements, including the following:

- basic Telecommunications Service Operating Permit:
  - (a) the operator must be a legally established company that specialises in basic telecommunications services and in which the state holds no less than 51%;
  - (b) a feasibility study and technical plan for formation of the network must be completed;
  - (c) the operator must have access to funds and specialised personnel commensurate with the business activities to be engaged in;
  - (d) there must be a site and corresponding resources to carry out envisioned business activities;
  - (e) the operator must have the reputation or the capability to provide long-term service to its subscribers; and
  - (f) the operator must comply with other conditions specified by the state.
- value-added Telecommunications Services Operating Permit:
  - (a) the operator must be a legally established company;
  - (b) the operator must have access to funds and specialised personnel commensurate with the proposed business activities;
  - (c) the operator must have the reputation or the capability to provide long-term service to its subscribers; and
  - (d) the operator must comply with other conditions specified by the state.

## 9. Audiovisual Services and Video channels

### 9.1 Main Requirements

China does not maintain a unified regulatory regime for all components of the audiovisual media industry as a whole. Instead, industry sub-sectors are separately regulated through a range of different laws and regulations. With respect to audiovisual media, the key areas of regulation include cable broadcasting, online audiovisual services and Over the top (OTT) services. In general, the broadcasting or online transmission of audiovisual content is highly regulated and in many cases restricted to both foreign and domestic investment.

**Cable Broadcasting**

Cable broadcasting is highly regulated in the PRC, and is not open to foreign participation or even new domestic market entrants. Currently, a broadcasting television station may only be set up and established by the central or local government branches, such as the National Radio and Television Administration (NRTA) or the Ministry of Education. The station's establishment will be subject to the central PRC government's national market plans as well. No individual or other enterprise or organisation is allowed to set up any broadcasting television station in China.

The most central piece of legislation relating to cable broadcasting; that is, offering traditional cable television channels such as CCTV, is the Administrative Regulations for Radio and Television. Among others, all cable broadcasters are required to obtain two key permits: the Radio and Television Broadcasting Institution Permit and the Radio or Television Programme Production Permit. PRC law requires applicants for these permits meet certain requirements, including requirements regarding the applicant's location, equipment, technology and personnel, and to complete an application processes with applicable authorities. No application fees are required. As mentioned, however, it is difficult if not impos-

sible for new entities, domestic or foreign-invested, to obtain either of these permits in China.

**Online Audiovisual Services**
Online audiovisual services are primarily regulated through:

- the Interim Administrative Provisions on Internet Culture, which is central to the so-called 'Internet Culture' sector, regulating online cultural activities;
- the Administrative Measures for the Transmission of Audio-Visual Programs Through the Internet or Other Information Networks;
- the Administrative Regulations on Internet Audio-Visual Program Services; and
- the Administrative Regulations on Audio-Visual Program Services via Private Network and Targeted Transmission,

all of which apply to online audiovisual service activities.

To operate an online streaming platform – that is, provide video on demand (VOD) services such as Youku – the most important operating permits include an Internet Culture Business Permit ('Online Culture Permit') and an Internet Audio Video Broadcasting Permit ('IAVB Permit'). Both permits require the applicant to meet certain requirements and complete an application process with local- and state-level government authorities. No application fees are required. For the IAVB Permit, it requires the new applicant to be controlled or wholly owned by one of China's State-Owned Enterprises. Neither the Online Culture Permit nor the IAVB Permit may be obtained by an applicant having any foreign investor.

**OTT Services**
The most important operating permit for providers of OTT Services is the Over the top (OTT) licence. To apply for an OTT licence, a qualified applicant must meet certain requirements, including being controlled by a State-owned Enterprise along with other equipment and personnel requirements. Here too, both local and state government approval are needed, which requires submitting an application to local- and state-level authorities. No application fees are required. To date, only 16 OTT licences have been issued.

**Contractual Partnerships/Licensing**
Taken together, directly operating an online video channel in the PRC is highly regulated and requires procurement of operating licences/permits (ie, an Online Culture Permit and an IAVB Permit/OTT licence) that are generally only available to the companies with State-owned Enterprises as shareholders. As such, it is more common for content owners outside China to simply license content to a domestic entity that holds all required permits; eg, the licensing arrangement between iQiyi and Netflix. Such domestic entities will also ensure that licensed content complies with PRC content/censorship requirements and will potentially self-censor any content that may potentially result in an infringement.

## 10. Encryption Requirements

### 10.1 Legal Requirements Governing the Use of Encryption

The use of encryption products is highly regulated in the PRC. While there are some general, affirmative obligations for companies to safeguard/encrypt protected types of data (such as Personal Information and Important Data under the PRC Cyber Security Law), such companies must always ensure that they remain in compliance with the PRC's more tailored legal provisions on encryption such as the Regulation of Commercial Encryption Codes. In this regard, relatively recent regulations promulgated by China's State Council and the State Cryptography Administration (SCA) in 2017 represent a seismic shift in the regulatory landscape governing commercial encryption products in China, which have superseded three prior burdensome regulations, including the Regulation on Administration of the Usage of Commercial Encrypted Products, the Regulation on Administration of the Sales of Commercial Encrypted Products and the Measures for Administration of the Usage of Encrypted Products by Foreign Organisations and Individuals. Back when such regulations were effective, Chinese regulators subjected all companies in China to enterprise-level restrictions on the manufacture, distribution and use of commercial encryption products. Foreign companies and foreign individuals were barred from manufacturing or distributing such products in China, and their use was subject to a burdensome prior-approval process. While foreign-invested Chinese companies (eg, WFOEs or JVs with foreign shareholders) were technically allowed to manufacture and distribute such products, in reality they were also essentially banned.

However, in invalidating these three regulations, the PRC authorities officially retired many of the most burdensome approval requirements of the old regulatory regime. Following these developments, some additional changes could be further triggered in the future. These loosened restrictions will no longer prohibit the manufacture and distribution of approved encryption products solely due to a company's enterprise type, and will also make it easier for foreign entities to adopt best practices in their data security standards without prior authorisation (provided that they use Chinese-manufactured encryption products or specifically approved imported products, as discussed below). Although certain rigid restrictions remain, and even though the new regulations are still subject to implementation at the local administrative level, these regulatory changes will likely prove to be a welcome development for manufacturers, distributors and users of commercial encryption products in China.

In terms of rules governing the use of commercial encryption products (ie, as opposed to their manufacture or distribution), the most notable change brought by the new encryption regulations largely shifts the focus of PRC regulators from the type of enterprise using encryption products (ie, a pure domestic company, foreign-invested company or purely foreign company/individual) and instead focuses on the specific encryption products being utilised. Accordingly, domestic companies, foreign-invested companies and foreign companies/individuals may all now freely use Chinese commercial encryption products that have been manufactured and distributed pursuant to a valid product certificate issued by PRC regulators. Additionally, foreign-invested companies and foreign companies/individuals may also seek regulatory approval to use foreign-manufactured encryption products, provided that such foreign products have obtained a valid and approved import permit from the SCA and Chinese Customs.

**DaHui Lawyers**
Suite 3720 China World Tower A
1 Jianguomenwai Avenue,
100004 Beijing

Tel: +86 10 6535 5888
Fax: +86 10 6535 5899
Email: richard.ma@dahuilawyers.com
Web: www.dahuilawyers.com

### 10.2 Exemptions

The use of encryption does not exempt an organisation from any specific rules under PRC law. However, in practice, the use of certain encryption products as certified/authorised by Chinese authorities will often satisfy certain obligations to safeguard and protect data under PRC law, such as provisions applicable to Network Operators under the PRC Cyber Security Law.