Internet Regulation and Data Privacy in China

A Brief Overview for Compliance Officers

China is the world's second largest economy, with an annual growth rate of more than eight percent and a rapidly growing middle class. Foreign investment into China routinely exceeds US$100 billion a year. Businesses from all over the world must have a China strategy to remain competitive and succeed in the global marketplace.

This brief will cover the key corporate compliance issues for companies using the Internet as part of their business in and with China. More detail is available at any time from our China Team. Your attention is called to the disclaimer at the foot of this brief.

DOES PRC LAW APPLY?

PRC regulation of the Internet is not applied extraterritorially. As a practical matter, however, all Internet traffic in China is monitored by and subject to interruption by the PRC authorities. Compliance officers therefore need to be aware of PRC sensitivities with regard to Internet operations even if PRC law does not technically apply to their companies.

The principal means by which the PRC regulates the Internet is through its jurisdiction over value-added telecommunications service providers whose operations or servers are located in the PRC. It exerts this jurisdiction through approval, licensing, permitting, inspection and reporting obligations imposed on Internet content and service providers in the PRC.

Thus, a business which maintains its servers and stores all of its information outside of China is technically not subject to regulation by the Chinese authorities. However, the PRC's total control over information passing over the Internet in China permits it to restrict or block altogether communications as well as entire domains at will, and it frequently does, even where the operator and all its servers are located outside of China. Companies therefore should be aware of what is, and what is not, considered permissible for companies using the Internet in China.

"INTERNET SERVICE PROVIDER"

PRC law regulates all parties who engage in "the service activity of providing information to Internet users through the Internet."

These parties are referred to as "Internet service providers," although we would use the term "Internet content provider" in this situation, reserving the ISP reference to companies providing access to the Internet rather than service over the Internet. This brief will occasionally use the term "ICP" to refer to what the PRC regulations call "Internet service providers."

This is an intentionally broad definition. A conservative view would be that any company maintaining a server in the PRC, which permits third parties to access information on that server or transmit information through that server, is an "Internet service provider" and covered by PRC regulations.

COMMERCIAL INTERNET SERVICE PROVIDERS

Commercial Internet service providers are subject to a complex approval, permitting and licensing scheme in the PRC, described below. "Commercial" Internet activity is not well defined, but a good rule of thumb is that any activity which involves the exchange of information or services over the Internet for compensation is "commercial." Clearly, a subscription-based service is "commercial," for example. Merely providing corporate information on a company website is probably not. It is not clear whether a company providing links to online technical support or other items and services is engaged in "commercial" activity, since those services could be seen as part of the product or service being sold.

NON-COMMERCIAL PROVIDERS

Non-commercial Internet service providers are subject to a notice filing requirement, but not an approval and licensing requirement. "Non-commercial Internet information services" are defined as "the provision of public and shared information services to Internet users through the Internet without compensation."

PERMIT AND LICENSING SYSTEM

The 2002 basic regulatory scheme in China establishes a permitting system for all commercial Internet information service providers.

Any person wishing to provide Internet information services must apply to the local office of the Ministry of Industry and Information Technology for a license. This is generally a provincial-level office, but in areas under the direct supervision of the central government (such as Beijing and Shanghai), the application is to municipal authorities. The local MIIT office is required to act within 60 days of the application; if the permit is denied, a written explanation of the reasons must be provided.

Among other things, an applicant must maintain a business development plan; maintain network and information security procedures, including measures to ensure user privacy; and obtain permits from sector-specific ministries, where applicable.

The operator must also obtain a business license from the relevant office of the State Administration of Industry and Commerce (AIC).

There may be separate local licensing requirements, as there are in Shanghai and Guangzhou. There may also be separate permitting and licensing requirements for given industries, such as media (State Administration of Radio, Film and Television [SARFT], the Ministry of Culture, the General Administration of Press and Publication [GAPP], and the State Secrecy Bureau). More than 20 different national-level government agencies and ministries have promulgated regulations relating to the Internet.

Operators are strictly limited to the activities set out in their operating permits, and any changes to business scope, website address, etc. must be approved in advance.

ICPs must post their operation license numbers on their websites.

Licenses are domain-specific, so multiple domains will require multiple licenses.

Operators must maintain records for up to 60 days of all content on their websites, subscriber access counts, account numbers of subscribers, and other information—and to submit that information to the relevant government authorities.

RESTRICTIONS ON FOREIGN INVESTMENT

The licenses just described (often called "ICP licenses") cannot be held by a foreign person or company, or by a PRC entity owned more than 50% by a foreign party. It is extremely difficult to obtain an ICP license for a Sino-foreign joint venture, however, so in practice ICP licenses are limited to 100% PRC-owned entities.

VARIABLE INTEREST ENTITY (VIE) STRUCTURES

Foreign companies wanting to use the Internet in the PRC as part of their businesses typically use a "variable interest entity" or "VIE" structure. In a VIE structure, the ICP license is held by a PRC entity controlled by the foreign party, but not owned by it. The legitimacy of this structure has been questioned by some commentators, but it is used by hundreds of companies and has at least the tacit sanction of the Chinese government.

It is essential, however, for compliance officers to be sure the contracts which make up the VIE structure are current, filed with the authorities where appropriate, and that they are complied with in practice.

COMPLIANCE CHECKLIST

Compliance officers should be aware of a range of operational requirements applicable to all Internet service providers.

Data retention

All Internet service providers must maintain records for up to 60 days of all content on their websites, subscriber access counts, account numbers of subscribers, and other information. This information must be submitted to the authorities on request.

In addition, all ICPs that engage in news, publishing and electronic notice services must record the contents of information distributed and the time distributed, as well as Internet addresses or domain names, and record user online

time, user account numbers, Internet addresses or domain names and the telephone numbers of Internet users. These records must be kept for 60 days and made available to the authorities on request.

Network and information security procedures

A number of PRC regulations require operators to establish and maintain "systems of information security and censorship." This is not well-defined, and some operations suggest a greater need for these systems (file sharing, social media, blogging) than others (technical support, travel services). Compliance officers should consider the advisability of having written policies and designated individuals or committees to ensure compliance with those policies.

Content monitoring, self-censorship and mandatory reporting

Any operator which discovers impermissible content being transmitted by or over its website must discontinue the transmission, keep "relevant records" and report the matter to the authorities. "Impermissible content" is broadly defined, see below.

Many companies, especially if they are in the file-sharing or social networking space, employ a significant percentage of their workforce, as well as sophisticated screening algorithms, to comply with this requirement of self-censorship. The PRC authorities inform operators frequently, often on a daily basis, as to what terms, information or content must be deleted or blocked from websites.

Compliance officers should ensure that their companies have in place sufficient measures to comply with PRC censorship requirements.

State secrets

The PRC government takes an expansive view of what might be regarded as "state secrets" or "national security information." For example, the address of police stations as well as the working papers of a company's public accountants have both been treated as state secrets in recent examples.

State secrets may not be published or distributed over the Internet, or transmitted outside of the PRC for any reason.

Music and video

Special licenses are required for the distribution or sharing of music, video, and other audiovisual or cultural information.

News

The publication or distribution of "news" over the Internet is separately and strictly regulated by the PRC government.

Online games

The online gaming industry is complete closed to foreign investment, even through the use of VIE structures.

Data privacy

Regulations published in 2011 and 2012 require operators to adopt and comply with rules for collection and use of electronic personal information, and make such rules known to their users. See more detailed discussion of data privacy, below.

IMPERMISSIBLE CONTENT

The following information is prohibited from being published or distributed over the Internet in China. Any person publishing or distributing this information—including permitting the distribution or transmission of this information over or through a website maintained by a person who is not the author—is subject to potential civil and criminal liability.

Information which:

- opposes the fundamental principles stated in the PRC constitution;
- compromises national security, divulges state secrets, subverts state power or damages national unity;
- harms the dignity or interests of the state;
- incites ethnic hatred or racial discrimination or damages inter-ethnic unity;
- undermines the PRC's religious policy or propagates heretical teachings or feudal superstitions;
- disseminates rumors, disturbs social order or disrupts social stability;
- disseminates obscenity or pornography, encourages gambling, violence, murder or fear or incites the commission of a crime;
- insults or slanders a third party or infringes upon the lawful rights and interests of a third party; or
- is otherwise prohibited by law or administrative regulations.

DATA PRIVACY

Until very recently, data privacy was only addressed on a piecemeal basis under PRC law. The Ministry of Industry and Information Technology (MIIT) promulgated data privacy regulations in December 2011 (called the *"Provisions"*), and the Standing Committee of the National People's Congress published broad "Resolutions" on the same topic in December 2012.

The 2011 *Provisions* and the 2012 *Resolutions* apply to any person or entity "engaging in the provision of Internet information services and activities relating to Internet information services within the People's Republic of China." (Note the implicit disclaimer of extraterritorial jurisdiction.)

"Personal information" is defined as "any information associated with a user which, either independently or when combined with other information, is able to identify such user."

Under the *Provisions* and the *Resolutions*, all Internet service providers must:

Adopt and comply with data protection rules

- Adopt and comply with rules for collection and use of electronic personal information, and make such rules known *(Resolutions)*;
- Clearly state the purpose, means and scope of their collection and use of electronic personal information *(Resolutions);*
- Expressly inform users of the method, content and purpose of the collection, process and use of personal information *(Provisions);*

Obtain users' consent to collect data, and only use it for limited purposes

- Refrain from collecting users' personal information without their consent, unless otherwise required or permitted by law or regulation *(Resolutions* and *Provisions);*
- Only collect personal information necessary to provide their services *(Provisions);*
- Only use personal information as necessary for the stated purpose *(Provisions);*

Protect the confidentiality of users' personal information

- Adopt information security safeguards to protect the confidentiality of personal information *(Resolutions);*
- Maintain the security of personal information and not disclose it to any third party without the individual's consent, unless otherwise provided by law or regulation *(Resolutions* and *Provisions);*
- Refrain from deceiving, coercing or misleading a user into consenting to the release of personal information to third parties *(Provisions);*

Refrain from trading in users' personal information

- Refrain from misappropriating or otherwise obtaining personal information by unlawful means *(Resolutions);*
- Refrain from selling or otherwise unlawfully providing or divulging personal information to any third party *(Resolutions* and *Provisions);* and
- Refrain from transferring user information, either arbitrarily or by falsely using the user's name *(Provisions).*

Both the *Resolutions* and the *Provisions* are silent on what constitutes a user's "consent." EULAs and standard privacy policies are likely to become a regular feature of PRC websites, with all the uncertainty they bring in other parts of the world.

Preserving personal data

The *Resolutions* and the *Provisions* prohibit operators from altering or destroying personal information obtained in the course of their business *(Resolutions);* or arbitrarily modifying or deleting personal information without justifiable cause *(Provisions).*

Real names

The *Resolutions* contain one provision which seems at odds with "data privacy": a requirement that operators collect the real names of users on all agreements for the provision of access-related or information-related services. This direct rejection of the anonymity which is often cited as a benefit of the Internet has caused considerable debate within China.

DATA BREACHES

The 2011 *Provisions* as well as the 2012 *Resolutions* require all operators to "immediately take remedial measures" in the event of an actual or potential data breach. The *Provisions* exclude any breaches unless "serious consequences" are likely (without defining that term); the higher-ranking *Resolutions* do not provide such an exemption.

In addition to taking remedial measures in the event of a data breach, the operator is required to report the breach to the relevant governmental authorities and cooperate with them in any subsequent investigation or proceeding.

Pillsbury Winthrop Shaw Pittman LLP | 1540 Broadway | New York, NY 10036 | 877.323.4171