DechertOnPoint

June 2012 / Special Alert

A legal update from Dechert LLP

# Latest Trends in Cloud Computing in China

Cloud computing continues to be an area of significant interest and investment for many companies. Current forecasts predict IT and cloud computing spending to total $112 billion in 2012, a 15% increase over 2011. Some companies view cloud computing as a potential bridge to bringing well-established business practices into emerging markets with huge opportunities for expansion. Given the size of the current and future market in China, companies are now evaluating whether and how to engage in "cloud" businesses in China. In this *DechertOnPoint*, we discuss a number of key issues that need to be considered in making thoughtful business decisions about cloud computing in China.

## Have Your Servers Located in China: How Censorship and the Great Firewall Affects Service

Censorship is and will likely remain a major stumbling block for the development of internet services in China, including cloud computing. For example, Google Docs, a well-known cloud-based program, is from time to time totally inaccessible in China. Technically, cloud services supported by servers outside China can (and do) work in China, but the risk of being blacklisted can create major continuity issues for the business. Censorship is based on a complex interpretation of a variety of laws that can lead to unpredictable blocking and potential service interruptions. One of these screening processes is known as the Great Firewall (GFW). Apart from implementing censorship, this process also impacts the speed of the cloud due to the additional layer of data analysis by Chinese authorities. There are also a number of problems with basic internet infrastructure: cloud computing only functions as a useful commodity when used with a high-speed broadband connection. However, China's average rate of data transfer is just 1463 kbps. In contrast, the average internet connection speed in OECD countries is about five times faster (source: Akamai – State of the Internet report Q4 2011).

## Be China Law Savvy While Structuring Your Business in China: Finding Your Way In the Chinese Regulation Jungle

Currently, the only major players in Chinese cloud computing services are foreign companies that have paired up with Chinese domestic companies. The Japanese company NEC has set up a joint venture with Chinese company Neusoft and IBM is working with Chinese company Range Technology. Neusoft and IBM are developing a huge 6.2 million square foot 'computer city' that will be primarily for cloud computing and office space. Notably, there are very few domestic companies providing cloud computing services. This may be the product of uncertainty in the market.

That uncertainty may, in part, be a product of the complexity of Chinese law in the area commonly referred to value-added telecom services (VAS). To operate SaaS business, a company needs an Internet Content Provider (ICP) license. Operating an IaaS business requires an Internet Service Provider (ISP) license or a much more difficult to obtain basic

telecom services license. There are foreign ownership restrictions for basic telecoms license and stringent licensing requirement for VAS licenses. Most entrants to the VAS market elect to do so by entering into a partnership with a domestic Chinese licensee, with varying degrees of operational control of the business. We often observe that such arrangements, even if valid, often trigger uncertainties which the foreign investor should do its best to manage by way of various co-operation agreements.

## Monitoring Privacy: Coping with China's Data Protection Framework

Even though a draft law has been in discussions for over a decade now, there is for the time being no dedicated data protection law in China. Foreign companies must instead deal — again — with a collection of various regulations even if China's Tort Law recognizes the right to privacy as a stand-alone legal principle. In particular, cloud computing companies need to be aware of a provision of the Tort Law which states that if an ISP knows a user's privacy rights are being infringed by content posted on its website, or is warned of such infringement by an injured party but fails to take appropriate measures (i.e., removing the content, disconnection, etc.), it is jointly and severally liable with the party that posted such content. In addition, if the injured party requests registered information about the party that posted the infringing content and the ISP refuses to divulge such information, the ISP itself becomes liable for the infringement. Similarly, the Labor Law contains broadly worded provisions that require employee information be treated confidentially. If employee information is placed on the cloud, the strength of the conditional access system will be relevant to assessing whether the employer has complied with these requirements.

More specifically, to deal with issues arising in the banking sector, in 2011 the People's Bank of China (PBOC) issued the Notice to Urge Banking Institutions to Protect Personal Financial Information (the Notice). Chinese banking institutions (including foreign invested commercial banks) (the Banks) are required to observe the provisions of the Notice when collecting, processing and storing personal financial information (PFI) during the course of their business and while accessing the PBOC's credit reference system, payment system or other systems.

The Notice, among other things, prohibits Banks from storing, processing or analyzing outside China any PFI which has been collected in China, or providing PFI collected in China to an offshore entity. Banks outsourcing their data outside of China need to pay special attention to this requirement, especially as the Notice defines PFI very broadly.

PFI includes:

- personal identity information
- personal property information
- personal account information
- personal credit information
- personal financial transaction information
- derivative information; and
- other personal information acquired or stored in the process of developing business relationships with individuals.

Banks hiring outsourcing service providers to deal with their data are advised to examine and evaluate such providers' ability to protect PFI. Any service agreement entered into between the service provider and the Bank must impose obligations on the service provider to protect the confidentiality of the PFI and to destroy the PFI upon termination of the service contract.

Violation of the Notice requirements authorize the PBOC to order the relevant Bank to rectify its non-compliance and require the Bank to punish its responsible officers and any non-permitted disclosure constitutes a crime.

To address these legal requirements, Banks should consider:

- providing adequate training to their employees about the importance of PFI security and confidentiality;
- tracking and restricting access to PFI, including appointing a PFI compliance officer to respond quickly to data security breaches and audit internal procedures; and
- reviewing PFI related practices and documents and outsourcing service contracts to ensure compliance.

## Make Sure You Don't Deal With State Secrets

Another significant issue that needs to be considered by cloud computing companies is the protection of State secrets. The gathering of information in an on-line database might be deemed to violate Chinese State secrets regulations. The Chinese State secrets legal framework was revised in 2010 by two important pieces of regulation, the Law of the People's Republic of China on Guarding State Secrets and the Interim Provisions on the Protection of Trade Secrets of Central Enterprises (together, the State Secrets Laws).

Chinese authorities are usually extremely concerned by the types of data transferred on the internet and the potential threats such transfers may cause to State security.

Thus, the production, reproduction, access, dissemination and transfer out of China of data that may disclose state secrets are strictly forbidden by the State Secrets Laws.

One challenge foreign companies may encounter in China is that Chinese authorities have broad discretion to determine the scope of State secrets. As such, information related to the business operations of certain state-owned enterprises may be classified as State secrets. Therefore, disclosure of information from a database containing such information may violate the provisions of the State Secret Laws. Consequences of such potential breaches must be studied carefully, as criminal punishments are attached to such violations, and individuals employed by foreign companies in China have been known to be imprisoned as a result.

Additionally, the State Secrets Laws also require an ISP to cooperate with the authorities in case of investigation, by immediately ceasing transmission of information involving State secrets, maintaining records of the information transmitted, reporting them to the authorities, and deleting such information when requested. As previously discussed, as the definition of State secrets is uncertain and may vary from time to time, ISPs may face an additional burden when requested to serve as a de facto agent of the Chinese government.

In summary, all foreign corporations dealing with cloud computing in China must assess the impact on themselves (and their staff) of the latest Chinese regulations in this respect and particularly pay special attention to regulations on state secrets and data privacy. Doing so in advance may help take advantage of the benefits of cloud computing while mitigating potential risks.

■ ■ ■

This update was authored by Jingzhou Tao (+8610 5829 1303; jingzhou.tao@dechert.com) and Gregory Louvel (+8610 5829 1315; gregory.louvel@dechert.com).

## Practice group contacts

For more information, please contact the author, one of the attorneys listed or any Dechert attorney with whom you regularly work. Visit us at www.dechert.com/privacy_and_data_protection.

**Jingzhou Tao**
Beijing
+8610 5829 1303
jingzhou.tao@dechert.com

**Gregory Louvel**
Beijing/Hong Kong
+8610 5829 1315
gregory.louvel@dechert.com

Sign up to receive our other *DechertOnPoints*.

Dechert LLP

www.dechert.com