Advisory

pillsbury

China

Corporate & Securities

Corporate & Securities - Technology

Privacy, Data Security & Information Use

April 2, 2013

Protecting Personal Data in China

By Woon-Wah Siu and Julian Zou

This advisory is one of a series prepared by Pillsbury's China Practice on questions frequently asked by our clients doing business in China. In June 2012, we published an advisory on personal data protection in China in which we also suggested some best practices. Here, we are updating that advisory to reflect new regulations adopted in the past six months.

Personal data protection legislation has been a widely discussed topic in recent years in China, mainly because employees of institutions that amass personal data of users and clients in the course of their business (such as internet companies, hospitals, phone companies, banks and insurance companies) are selling the personal/client data for profit or disclose the data to third parties inappropriately. In extreme cases, databases of personal information can even be downloaded online freely.

Despite cries for a comprehensive national personal data protection law, no such law is in place yet. However, the past six months have witnessed a series of administrative regulations and standards, which are aimed at tightening control over involuntary dissemination of personal data.

National Law

Several Provisions on Regulating Market Orders of Internet Information Services

For a long time, the laws at the national level that provide personal data protection were the PRC Criminal Law and the PRC Tort Liability Law. The PRC Criminal Law prohibits employees of government agencies or institutions in the financial, telecommunication, transportation, education or medical sectors from selling or otherwise unlawfully providing to third parties personal data of any Chinese citizen to which these employees have access in the course of performing duties or services at any such agency or institution. The PRC Criminal Law also prohibits any person from obtaining personal information of any person by means of theft or other unlawful means. A person whose personal data has been unlawfully used or disclosed may also file a civil claim under the PRC Tort Liability Law for infringement of privacy. However, due to the lack of detailed interpretations or implementing regulations on the application of the relevant provisions in the PRC Criminal Law or the PRC Tort Liability Law, the impact of these laws on prevention of misuse of personal information has been relatively insignificant.

On March 15, 2012, the Ministry of Industry and Information Technology of the PRC took a first concrete step, and published *Several Provisions on Regulating Market Orders of Internet Information Services* (MIIT Provisions). The MIIT Provisions apply to internet service providers (ISPs) which normally collect large amounts of personal information, such as email service providers, and web and blog operators or hosting service providers. The Provisions do not focus on data protection, but include two articles that regulate how these ISPs may collect and use personal data of their users. Among other things, the articles impose the following requirements on the collection of user personal information that, in itself or together with other information, is sufficient to identify the user.

- The ISPs must inform users of their services of the method and content of and the purpose for collecting and processing the personal information and may not provide personal information to a third party without the user's prior consent.
- The ISPs may collect such personal information as is necessary for provision of their services.
- The ISPs must securely maintain personal information and must take measures promptly to mitigate possible harm resulting from any actual or suspected leak of personal information. If a leak of personal information results in actual or potential material adverse consequences, the ISP must inform the authorities and be cooperative during an investigation by the authorities.

An ISP who violates any of the MIIT Provisions may be subject to a fine ranging from RMB 10,000 to RMB 30,000, together with a public warning.

Decision on Strengthening Online Information Protection

In December 2012, the Standing Committee of the National People's Congress published the *Decision on Strengthening Online Information Protection* (the Decision). The Decision tries to fill the gaps in the MIIT Provisions by requiring ISPs to keep confidential any personal information collected in the course of their business operation and to abstain from disclosing, revising, selling or illegal providing any such personal information to any other person. The Decision further gives Chinese citizens the right to require ISPs to delete and to take any necessary measures to prevent any unpermitted dissemination of their personal information. The Decision only applies to personal information in digital form.

The Decision also applies to governmental agencies, which must keep confidential the personal digital information obtained in the course of their performing their duties and must not divulge, falsify, damage, sell or illegally provide such information to others. The Decision also directs governmental authorities to take necessary measures to prevent illegal collection of personal digital information through stealing or other unlawful means; selling or illegally providing personal information to others; or other criminal activities relating to online information.

The Decision only has 12 articles and is broadly worded. Thus implementation of the Decision will have to wait until detailed implementation or interpretive rules have been adopted.

The Guidelines

In January 2013, MIIT issued the first national standard on personal data protection, the *Information Security Technology – Guidelines for Personal Information Protection within Public and Commercial Information Systems* (Guidelines). The Guidelines, for the first time, clearly defines what might be considered as "personal information" and "sensitive personal information," and provides detailed personal information protection requirements on each of data collection, data possessing, data transfer and data retention phases.

However, the Guidelines has no legal binding effect, so its effectiveness in protection personal data will depend on further rules and regulations. Most likely, the Guidelines will be incorporated into some industrial self-regulation rules that will form the basis for protecting private data and personal information. As of this writing, the China Software Evaluation and Test Center under MIIT has announced its plan of facilitating the formation of a "Personal Information Protection Alliance" by a coalition of major internet companies, industry associations and standards testing and evaluation centers, which is expected to play a consultative role in future legislation in the personal data privacy protection.

Local Law

In response to the increasing occurrences of inappropriate collection and use of personal data on a massive scale, and in view of the lack of comprehensive personal data protection legislation at the national level, many provinces in China have adopted or are considering adopting personal data protection regulations. For example, Jiangsu province enacted data protection regulations last year that prohibit the sale, illegal use or disclosure of personal data; the Jiangsu regulations also prohibit theft or purchase of personal data.

Best Practices

Foreign companies doing business in China often ask what the requirements are on how to collect, process and use personal information of their employees in China for administrative and business purposes. Chinese law is silent in this regard. In the absence of clear legal guidance, companies doing business in China may consider the following practices to reduce possible misuse of personal data and claims of infringement of privacy rights:

- Informing each employee what personal data the company will be collecting and the purpose for collecting such data.
- Requesting the employee to sign an acknowledgement and consent to the company's collection, processing, and use of personal data.
- Implementing measures to maintain the confidentiality of personal data by, for example, limiting access to personal data to specified employees on a need to know basis.
- Limiting personal data collected to the information necessary for the relevant administrative or business purposes.
- Providing the employee with the option of not disclosing certain sensitive personal information (such as medical history).

In general, the Chinese subsidiary should adopt the same procedures as those used by the parent company to protect employee personal data, especially if the procedures have been designed to comply with more developed data protection laws in other jurisdictions.

If you have any questions about the content of this advisory, please contact the Pillsbury attorney with whom you regularly work, or the authors below.

Woon-Wah Siu (bio)
Shanghai
+86.21.6137.7924
woonwah.siu@pillsburylaw.com

Julian Zou (bio)
Shanghai
+86.21.6137.7923
julian.zou@pillsburylaw.com