
Protecting Personal Data in China: An Update

By Woon-Wah Siu and Julian Zou


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 two years have witnessed a series of laws, administrative regulations and standards, which are aimed at tightening control over involuntary dissemination of personal data.

National Law

General Rules

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.¹ 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 have 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

 ¹ There are also national statutes relating to protection of state secrets and archives, such as the State Secrets Law, the Archives Law and the Overseas Securities Confidentiality Provisions. Protection of state secrets, however, will not be discussed here.

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.

2013 Consumer Protection Law

On October 25, 2013, the legislature in China adopted the second amendment to the Consumer Protection Law (2013 Consumer Protection Law), which explicitly addresses the issues relating to collection and use of consumer personal information. The 2013 Consumer Protection Law prohibits businesses from disclosing, selling or otherwise providing consumer data to any third parties and businesses must take all reasonable measures to keep consumer data in strict confidence. In response to high-profile distribution of spam mobile messages and emails, the 2013 Consumer Protection Law also prohibits distribution of marketing pitches to a consumer without the consumer's explicit consent.

The statutory requirements under the 2013 Consumer Protection Law apply to any business entities that provide products or services to the general public, and, therefore, will function as the last resort absent specific rules applicable to particular industries.

Several Provisions on Regulating Market Orders of Internet Information Services

On March 15, 2012, the Ministry of Industry and Information Technology of the PRC (MIIT) published Several Provisions on Regulating Market Orders of Internet Information Services (MIIT Provisions) as its first attempt to regulate the protection of personal information in the Internet industry. The MIIT Provisions apply to internet service providers (ISPs) that 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.

Provisions on Protecting the Personal Information of Telecommunications and Internet Users

The Decision has only 12 articles and is broadly worded. To implement and interpret the rules under the Decision, the MIIT published the Provisions on Protecting the Personal Information of Telecommunications and Internet Users on July 16, 2013 (Personal Information Protection Provisions).²

The Personal Information Protection Provisions clearly defines “Personal Information” as information that, in itself or together with other information, can be used to identify the individual user, such as the name, birth date, ID number, residential address, telephone number, account number and password, and the time when and the location where the individual user is using the services of telecommunication service and Internet service providers.

Under the Personal Information Protection Provisions:

- A service provider must establish rules for collecting and using Personal Information and publish them on its website or at its service location(s);
- The service provide must expressly tell the owner of Personal Information the purpose, method and scope of collection of Personal Information, and how it corrects discrepancies in the collected data;
- The Service Provider may not:
 - collect or use Personal Information without consent of the owner of the Personal Information;
 - collect Personal Information that is not necessary for provision of their services; or
 - use the collected Personal Information other than for the disclosed purposes.
- The service provider and its employees must keep Personal Information in strict confidence and may not modify, damage, disclose, sell or otherwise provide to any third party, the Personal Information;
- The service provider must publish the contact information for processing customers' complaints and has to respond within 15 days after receiving any complaint;

² 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 provides detailed personal information protection requirements on data collection, data possessing, data transfer and data retention. However, the Guidelines have no legal binding effect and, most likely, will be incorporated into some industry self-regulatory data protection rules. As of this writing, the China Software Evaluation and Test Center under MIIT is planning on establishing a “Personal Information Protection Alliance”—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 on personal data protection.

- The service provider must establish reasonable internal policies and rules to secure the confidentiality of the collected Personal Information, including internal audit and training of relevant employees at least once a year; and
- If the service provider engages agents to collect, store or analyze Personal Information, the service provider must supervise the agents and ensure that its agents comply with the same requirements for collection, storage and use of Personal Information.

Regulations on Online Transaction and Postal Services

Following the 2013 Consumer Protection Law and the Personal Information Protection Provisions, the Online Transaction Administration Rules published by the State Administration of Industry and Commerce, issued on January 26, 2014, and the Protection of Personal Information in Postal Services published by the State Post Bureau, issued on March 26, 2014, all incorporate same or similar rules for protection of personal information.

We expect to see more regulations, general law or industry-specific rules published in 2015 and in the near future, which will incorporate protective measures for personal information.

Local Law

In response to the increasing occurrences of inappropriate collection and use of personal data on a massive scale, and inspired by the efforts of the central government to strengthen the protection of personal information, many provinces in China have adopted or are considering adopting personal data protection regulations. For example, Jiangsu province enacted data protection regulations in 2013 that prohibit the sale, illegal use or disclosure of personal data; the Jiangsu regulations also prohibit theft or purchase of personal data.

Employment-Related Personal Data Protection

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 alert, 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 [\(bio\)](#)
Silicon Valley
+1.650.233.4057
julian.zou@pillsburylaw.com

About Pillsbury Winthrop Shaw Pittman LLP

Pillsbury is a full-service law firm with an industry focus on energy & natural resources, financial services including financial institutions, real estate & construction, and technology. Based in the world's major financial, technology and energy centers, Pillsbury counsels clients on global business, regulatory and litigation matters. We work in multidisciplinary teams that allow us to understand our clients' objectives, anticipate trends, and bring a 360-degree perspective to complex business and legal issues—helping clients to take greater advantage of new opportunities, meet and exceed their objectives, and better mitigate risk. This collaborative work style helps produce the results our clients seek.

This publication is issued periodically to keep Pillsbury Winthrop Shaw Pittman LLP clients and other interested parties informed of current legal developments that may affect or otherwise be of interest to them. The comments contained herein do not constitute legal opinion and should not be regarded as a substitute for legal advice.

© 2015 Pillsbury Winthrop Shaw Pittman LLP. All Rights Reserved.