A landmark year for consumer privacy protection in China

Jieni Ji and Eugene Chen (Shanghai) look back on a year of significant change in the area of consumer privacy protection in China. As they point out, in response to these recent developments, multinational companies should revisit their data privacy policies to ensure they comply with the various legal requirements, particularly with respect to the maintenance and usage of customer data.

CHINA

A landmark year for consumer privacy protection in China

INTRODUCTION

2013 was a landmark year for consumer privacy protection in the People's Republic of China. To address the many privacy issues associated with new technologies and business models, a body of new privacy legislation was introduced in the past year. These laws aim to regulate the collection, processing, retention and use of personal information by internet service providers (ISPs), data brokers and business operators. In parallel with these legislative developments, there was also a significant increase in the number of enforcement actions taken. The central public security authority undertook three large-scale national clampdowns on personal data violations since 2012, and over 1,200 arrests were made. Among the most prominent of these was the widely reported arrest in August 2013 of a forensic investigator, a British national, for illegally obtaining Chinese citizens' private information in the course of commercial due diligence projects. More recently, two individuals launched a private, civil action against a number of hotels for allegedly leaking guests' personal information and visit records.[1] If the court decides to accept the case, this will be the first civil action for data breach in China.

HISTORICAL LEGAL BACKDROP

The notion of the right to privacy is a relatively new legal concept in China, where it has traditionally received short shrift compared to the data protection laws of the European Union and other western economies. Prior to 2012, a citizen's right to privacy was only recognised in a few, very high-level pieces of legislation. Until very recently, there were no detailed regulations or implementing guidelines on personal data protection.

The PRC Constitution of 1982 generally protects a citizen's personal dignity, freedom of communication, and privacy of communications. The PRC Tort Liability Law of 2010 generally recognises a "right to privacy" as one of the protected civil rights, based upon which a civil party can file a claim. In 2009, Amendment VII to the PRC Criminal Law created a new offence for "government or private sector employees in the financial, telecommunications, transportation, healthcare or other like sectors to sell or otherwise unlawfully provide personal data that has been obtained by them in the course of carrying out their duties to their parties, or for any person to obtain such information by means of this or other unlawful means".

AN OVERVIEW OF THE NEW DATA PRIVACY LAWS

While the PRC Personal Data Protection Law, which is expected to be China's single most comprehensive data protection law, is still pending, China has, in the interim, released a number of important regulations on personal data protection during 2013.

On 1 February 2013, China's first personal data protection national standard, the Information Security Technology – Guideline for Personal Information Protection within Information Systems

[1] A report of the case is available at: http://news.sina.com.cn/s/2013-11-25/142028805065.shtml. As of the time of this article, the case name and docket number of the case have not been made public.

for Public and Commercial Services ("Guideline for Personal Information Protection"), was released. It followed the Decision on Strengthening the Protection of Online Information, a significant piece of legislation issued at the end of 2012 which sets out the personal data protection framework and high-level principles. The Ministry of Industry and Information Technology also promulgated the Provisions on Protecting the Personal Information of Telecommunications and Internet Users, which came into effect on 1 September 2013. The Administrative Regulations on Credit Reporting Business, promulgated by the State Council, took effect on 15 March 2013. And on 25 October 2013, the Standing Committee of the National People's Congress passed the Amendment to the Consumer Rights and Interests Protection Law ("Consumer Law"). One of the highlights of this Amendment is that the law now protects consumers from unlawful collection, use, and retention of their personal data by business operators.

The Guideline for Personal Information Protection

The Guideline for Personal Information Protection is not legally binding. However, as a recommended national standard, it does provide an outline of best practices in the area of personal data protection. The guideline defines "personal data" as "any computer data relating to a specific natural person which can be processed by an information system and which is capable of identifying such natural person, either individually or together with other information". It classifies "personal information" into two types: general personal information and sensitive personal information. Information, such as identification card numbers, cell phone numbers, race, religion, genetic information, fingerprints and political views, falls into the category of sensitive personal information. The purpose of collecting personal information, and the way in which it is to be used, should be specific, certain, and reasonable. An express consent from the data subject is required for the collection of personal sensitive information, while a tacit consent is required for the collection of general personal data.

The following information needs to be given to data subjects in plain language upon collection: purpose(s); nature of the personal data collected, collection methods and retention period; scope of potential uses, including whether it will be disclosed to third parties; security measures; data processor's name, address and contact information; potential data risks; consequences if data subjects refuse to provide the personal data; and channels for filing a complaint.

Principles for the Collection of Personal Information under the Administrative Regulation on Credit Reporting Business

The Administrative Regulation on Credit Reporting Business designates the People's Bank of China ("PBOC") as the top credit-reporting regulator in China. The regulation empowers the PBOC with the authority to monitor credit report business and to issue penalties for non-compliance. We expect that the PBOC will play a major role in data protection. The regulation sets out the administrative and civil obligations and liabilities of data brokers, data collectors, and data users. The key legal requirements under the regulation include the following

- the collection of personal information requires the prior consent of data subjects
- personal information, such as religion, genetic information, fingerprints, blood type, disease and medical history, is prohibited from collection by data brokers[2]
- data holders need to notify data subjects in advance if they transfer unfavourable personal credit information to data brokers[34]

[2] Information relating to a company's directors, supervisors, and senior management in relation to the performance of their duties is not deemed to be personal information.

- data brokers should guarantee data subjects access to information concerning themselves (each individual is entitled to up to two free credit reports each year)
- data users shall not use or transfer data to a third party in breach of the agreements between the parties
- data brokers should maintain the reasonable accuracy of data and
- data brokers should process and store the information collected in China within the territory of China.

Business operators' obligations under the Consumer Law

The Consumer Law provides another layer of legal protection to consumers' personal data. A consumer may file a civil action against a business operator if the latter fails to comply with the data protection requirements under the Consumer Law. The possible remedies include stopping infringement, restoring consumers' reputation, eliminating negative effects, issuing apologies, and recovering economic losses. It is worth noting that the Consumer Law recognises the principle of "proportionate (or necessary)" as one of the principles in terms of the collection and use of consumer data, although the law does not provide more details on the principle. However, the expectation is that businesses should collect only the data they need to satisfy a specific business purpose, and data collection practices should be limited and consistent with the context of the transaction. In addition to this principle, business operators also need to comply with data provisions under the Consumer Law, including the following

- obtaining consumers' prior consent on the collection of personal information
- expressly informing consumers of the method, content, and purpose of collecting personal information
- taking reasonable security measures to keep consumer information confidential
- immediately taking remedial measures to mitigate the impact where data has been or may be leaked or lost and
- refraining from sending commercial information to consumers without their consent or request, or after they have expressly declined to receive such information.

COMMENT

In response to these recent developments in China’s data privacy laws, we expect that many multinational companies will need to revisit their data privacy policies to ensure compliance with the various legal requirements, particularly with respect to the maintenance and usage of customer data. Companies doing business in China will have to pay closer attention to establishing a comprehensive set of data management procedures throughout the life-cycles of their products and services. In our view, companies should consider the following measures (while bearing in mind that the new privacy regime is still very general and subject to interpretation)

---

[3] Unfavourable personal credit information refers to information that could adversely affect the credit standing of a data subject, including information that the data subject fails to perform obligations under contracts in activities such as borrowing, purchase on credit, guarantee, leasing, insurance, and use of credit cards; information on administrative sanctions against the data subject; information contained in judgments or rulings rendered by people's courts ordering the data subject to perform obligations or ordering compulsory enforcement against the information subject; and other misconduct information prescribed by the PBOC.

[4] The statutory retention period for unfavourable personal credit information is five years.

- identify themselves to consumers, describe how they collect and use consumer data, and obtain prior consent from consumers upon collection
- provide reasonable security for consumer data and other types of data generated from business operations
- make sure that access to the relevant database is limited to authorised personnel only, and closely monitor access to the database
- obtain sufficient legal and technical protections when engaging a third party to maintain the relevant database
- seek legal advice before transferring data to a third-party vendor or a party located out of the country, including to corporate headquarters
- adopt a security scheme to respond to accidental data breach
- implement a robust data privacy and retention programme and provide data privacy training to employees.

Eugene Chen

Shanghai

eugene.chen@hoganlovells.com

Jieni Ji

Shanghai

jienni.ji@hoganlovells.com

Article reprinted with permission from Hogan Lovells' International Product Liability Review - Issue 53, December 2013, page 2.