

# Insight: Privacy

February 2012

## Data Protection and Privacy in China

China does not currently have a comprehensive legal framework to regulate the use and disclosure of personal data nor a national-level law that delineates how a company can legally collect, process and retain data together with legal remedies for specific violations. The relevant rules are scattered in diverse laws, regulations and local ordinances.

The right to privacy is upheld in principle by the PRC constitution and Civil Law Principles. The PRC Constitution provides that a citizen's personal dignity is specifically protected as a fundamental right. Although the Constitution fails to define what constitutes personal dignity, most Chinese legal scholars take the view that personal dignity should include certain privacy rights. Despite the fact that the term privacy is referenced in certain PRC laws and judicial interpretations, the scope of privacy protection (including the right to restrict public access to personal information) has not yet been expressly codified or addressed in detail by the PRC courts.

A number of diverse laws and regulations refer in general terms to the right to privacy. For example, relevant laws and regulations impose duties on inter alia courts, notaries, social insurance authorities, statistics authorities, hospitals, tour guides, real estate brokers, life insurance companies and internet retail platforms to keep confidential personal information that they obtain in the course of their work or business.

In addition, some local governments have also passed ordinances setting forth more detailed rules for the protection of consumer information. For example, Shanghai's Consumer Protection Rules provide that a business is not only prohibited from disclosing to a third-party a consumer's personal information (including name, gender, employment status, education, contact information, marital status, income, assets and health history), but also prohibited from asking consumers to provide any personal information unrelated to the business transaction at hand.

Due to the increasing awareness of the public of their right to privacy and also the problem that personal information is routinely collected and sold on a large scale, in 2009, the PRC Criminal Law was amended in a variety of areas, including defining certain acts relating to data collection and privacy as criminal offenses. For example, it is now a crime:

- (i) For employees of government institutions or institutions/organisations in the financial, telecommunications, transportation, education or medical sectors, to sell or otherwise unlawfully provide to third parties the personal data of any citizen that has been obtained in the course of performing duties or services at such institution/organisation; or
- (ii) For any person to obtain such information by means of theft or other unlawful means.



For more information please contact:

### Ashley Winton

Partner, London

+ 44 20 7532 2514

awinton@whitecase.com

### Alex Zhang

Partner, Shanghai

+ 86 21 6132 5966

azhang@whitecase.com

### Suzanne Innes-Stubb

Counsel, Helsinki

+ 358 9 22864 339

sinnes-stubb@whitecase.com

### Lucy Xu

Associate, Shanghai

+ 86 21 6132 5909

lxu@whitecase.com

*This publication is prepared for the general information of our clients and other interested persons. It is not, and does not attempt to be, comprehensive in nature. Due to the general nature of its content, it should not be regarded as legal advice.*

White & Case LLP  
5 Old Broad Street  
London EC2N 1DW  
Tel: + 44 20 7532 1000  
Fax: + 44 20 7532 1001

If the circumstance of the violation is severe, the individuals found guilty of either offense will be subject to imprisonment or criminal detention of up to three years and/or a monetary fine. The amended Criminal Law also specifically provides that organisations and institutions, either public or private, that commit either offense shall be subject to a monetary fine and the responsible person in charge may be personally liable for criminal charges.

However, the amended Criminal Law fails to provide important details on what constitutes personal data or unlawful provision, or what circumstances will be relevant in determining whether a violation is severe. Such definitions are usually embedded in the implementing regulations of the Criminal Law or the Supreme People's Court's interpretations as a response to comments from legal scholars and professionals and cases that emerge in this area.

In addition to the Criminal Law, there are news reports regarding the Chinese authorities' desire to draft a privacy and data protection law to regulate the collection, retention and use of personal information. For example, in 2011, a draft of the Information Security Technology - Guide for Personal Information Protection was published for the purpose of regulating the management and processing of personal information carried out by information administrators. However, such legislation has yet to be adopted at national level.

In the meantime, companies operating in China, especially those in the financial, telecommunications, transportation, education, or medical sectors, would be well advised to review their internal systems relating to the collection, retention, processing and transfer of customer data, including taking appropriate security measures to protect data collected, inform employees who handle personal data of their confidentiality obligations, and conduct necessary due diligence to assess the nature and sources of personal data to be acquired.