

Data Protection and Privacy in China

March 2012

China does not currently have a comprehensive legal framework to regulate the use and disclosure of personal data or a national level law that delineates how a company can legally collect, process and retain personal data. However, there are important rules scattered in diverse laws, regulations and local ordinances that should be considered when doing business in China.

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 has yet 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 courts, notary public, social security authorities, statistics bureaus, 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 out 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, for the first time in Chinese legislation, prohibited from asking consumers to provide any personal information unrelated to the business transaction at hand. The Information Ordinance of Henan Province also provides that if an entity or individual uses and develops information of any citizen, legal entity or organisation, such citizen, legal entity or organisation has the right to understand the situation and request the amendment or deletion of untrue information.

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:

- 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.
- For any person to obtain such information by means of theft or other unlawful means.



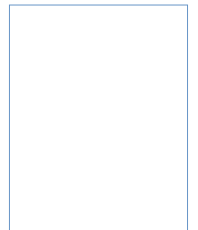
Ashley Winton
Partner, London



Alex Zhang
Partner, Shanghai



Suzanne Innes-Stubb
Counsel, Helsinki



Lucy Xu
Associate, Shanghai

This article was first published in the PLC GC Agenda China March 2012 and is reproduced with the permission of the publisher, Practical Law Company. For further information please contact jane-may.cross@practicallaw.com.

If the circumstance of the violation is severe, the individuals found guilty of either offence will be subject to three years' imprisonment and/or a monetary fine. In January 2010, a court in Zhuhai (a city in the southern part of China) handed down the first criminal sentence for illegal acquisition of personal information under the amended PRC Criminal Law. The case involved a Chinese individual who bought a log of telephone calls made by 14 high-ranking governmental officials and subsequently sold it to fraudsters for RMB16,000 (about US\$2,500). The fraudsters then used the information to impersonate the officials and extracted RMB830,000 (about US\$132,000) from their families and friends. The individual who bought and resold the telephone log to the fraudsters was sentenced to 18 months' imprisonment with a fine of RMB2,000 (about US\$320) for breach of the Criminal Law.

In addition to that, if any organisations and institutions, either public or private, commit either one of these offences, the amended Criminal Law specifically provides that these organisations and institutions are also be subject to a monetary fine and the responsible person in charge may be personally liable for criminal charges.

Apart from the Criminal Law which establishes criminal liabilities, the PRC Tort Liability Law (Tort Law, which is effective as of 1 July 2010) establishes data protection violations as a tort claim which can give rise to private civil actions. The Tort Law recognises that the right of privacy is a unique type of private right and any party whose right to privacy is infringed can claim against the tortfeasor for actual losses, profits arising from the breach, as well as damages for emotional distress.

However, both the amended Criminal Law and the Tort Law fail to provide important details such as what constitutes personal data under the Criminal Law and what standards are taken into account in determining whether the violation amounts to emotional

distress under the Tort Law. So far, no implementing regulations have been issued or published in this regard, nor any interpretation given by the Supreme People's Court.

There are news reports concerning 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 January 2011, a draft of the *Information Security Technology – Guide for Personal Information Protection* was published to regulate the management and processing of personal information carried out by information administrators such as website operators. The China Academy of Social Science (the premier and highest academic research organisation in the fields of philosophy and social sciences and the think-tank of the China State Council) also drafted a PRC Personal Data Protection Law a few years ago in an attempt to establish the first comprehensive legislation in China concerning privacy and data protection. However, such legislation has yet to be adopted at national level.

Pending the adoption of a single comprehensive data privacy law in China, companies doing business in China should still review and evaluate their internal systems relating to the collection, retention, processing and transfer of customer data to ensure that they are adopting best practice and avoiding the privacy and data protection risks described above.

Similarly, companies that have in place outsourcing arrangements with Chinese service providers may wish to review their outsourcing contracts to ensure that the service providers are obliged to comply with the myriad of existing laws concerning privacy and personal data in China and to ensure that they are held harmless from the consequences of any service provider's failure to comply with these laws.