

Data Protection Widened by China's Consumer Law Changes

Graham Greenleaf, Professor of Law & Information Systems University of New South Wales and George YiJun Tian, Senior Lecturer in Law, University of Technology, Sydney

(2013) 126 *Privacy Laws & Business International Report*, pgs 127-28, December 2013

China's National People's Congress (NPC) Standing Committee (its second-highest legislative body) has amended the PRC's *Law on the Protection of Consumer Rights and Interests* to include provisions on protection of personal information, along with other amendments. These are the first significant amendments to China's consumer protection law since its passage in 1993. The Amendments were passed on 25 October 2013, and will come into effect on 15 March 2014.

These Amendments apply to the use of consumers' personal information by all industries (companies that provide goods or services within China), in both online and offline situations, whereas laws and guidelines made in the last two years (by both the Ministry of Industry and Information Technology (MIIT) and the NPC Standing Committee itself) were largely confined to Internet and telecommunications services.

Principles for consumer transactions

Article 29 of the revised law now provides that¹:

The operators, collecting and using consumers' personal information, shall follow the legal, legitimate and necessary principles, express the purposes, methods and scope of using information, and obtain the consent of consumers. When collecting and using personal information of consumers, operators shall make public their rules for information collection and use, and use personal information only in accordance with agreements with consumers, or in accordance with applicable laws.

Operators and their staff shall treat the collected consumer personal information in a strictly confidential manner, must not disclose, sell or illegally provide to others. Operators shall take technical measures and other necessary measures to ensure information security, and to prevent disclosure or loss of consumer personal information.

In the circumstances that the information disclosure or loss occurs or may occur, immediate remedial measures shall be taken.

If operators have not received consent or request from consumers, or if consumers have expressed rejection explicitly, the operators shall not send commercial information to such consumers.

The content of the information privacy provisions in Article 29 can be broken down into nine requirements (principles) that companies covered by the Consumer Law must apply in relation to consumers:

- (i) Collect and use personal information only where legal, legitimate and necessary;
- (ii) Collect personal information only with consent;
- (iii) Expressly notify consumer of the purpose, method and scope of intended use;
- (iv) Make public their rules for information collection and use;
- (v) Use personal information only in accordance with agreements with consumers, or in accordance with applicable laws
- (vi) Not disclose or sell or illegally provide personal information to others;

¹ Unofficial translation by George YiJun Tian.

- (vii) Provide necessary security measures;
- (viii) Not send commercial communications without consent, and comply with express requests not to send such communications.
- (ix) Take immediate remedial measures when information leakage occurs or may occur.

These are conventional (if rather general) data privacy principles, with the notable absence of such user rights as access, correction and deletion, the omission of which is the weak point of most Chinese laws on data privacy. The principles are also unclear in that they do not refer to the purpose of collection as an explicit limit on subsequent use and disclosure, referring only to user agreement and applicable laws as limitations. Nor are they very clear on whether only the minimal amount of information necessary for a stated purpose can be collected.

What is the significance of the principles set out in Article 29 compared with the previous Chinese regulations of the last two years?

- (a) Almost every expression used in Article 29 can be found in the 2012 Decision of the Standing Committee of the NPC (dealing with the Internet and telecommunications sectors), in clauses 2, 4, 5 and 7 (see (2013) PLBIR Issue 121, 1 and 4-6). On the one hand they are ‘nothing new’ but on the other hand China’s second highest legislative body is being completely consistent in the data privacy principles it applies in different sectors.
- (b) This law applies to all consumer transactions, not only to those in the Internet and telecommunications sectors where the MIIT regulations apply.
- (c) These principles do not add anything new to the principles found in the various MIIT regulations, which are stronger on some points (see (2013) PLBIR Issue 125, 18-19; (2012) PLBIR Issue 116, 1-5).

Administration and enforcement

There are other important aspects of the Amendments which will affect the information privacy provisions.

Article 50 provides for civil liability for infringements of these principles:

Operators, who have infringed consumers' personal dignity, liberty, or right of personal information protection in accordance with law, shall stop such infringements, restore consumers' reputation, offer apologies, and pay damages.

Official consumer associations will also now be able to commence court actions on behalf of consumers, including where the rights of very large numbers of consumers are infringed, such as in large-scale data breaches. A form of class action will therefore be more likely.

Administrative enforcement is also provided for exactly the same types of infringement as can give rise to civil actions under Article 50 (Article 56(9)), requiring the ‘department in charge of industrial and commercial administration or other relevant administrative departments’ to take one or more of the following forms of enforcement (‘based on the circumstances’):

- (a) order the operators to rectify their acts;
- (b) issue a warning;
- (c) issue a fine of up to 500,000 yuan (US\$82,250) (where there are no illegal earnings);
- (d) confiscate illegal earnings (or impose a fine 10 times the illegal earnings);

- (e) order the operators to suspend operations for rectification; or
- (f) rescind their business licences if the circumstances of their offences are serious.

The State Administration of Industry and Commerce (SAIC), which regulates China’s consumer market, will now have a role alongside MIIT in regulating information privacy. Their jurisdictions will overlap in relation to consumer e-commerce, and how they will coordinate remains to be seen.

China approaches private sector coverage

For the first time, the cumulative effect of these laws is that China is approaching having a data privacy law for its whole private sector. Some principles, particularly data subject rights, are still missing or not explicit. Its laws generally only apply to the operation of commercial activities involving consumers and users of Internet or telecommunications facilities, and do not cover employees, but some such exclusions also occur in the laws of other countries such as Japan, Australia, Singapore and Malaysia. Similar ‘cumulative’ sectoral coverage is occurring in Vietnam (see (2013) PLBIR Issue 125, 22-25).