Asian Data Privacy Updates

1. China

China’s Personal Information Protection Law Proposal was submitted to the State Council in 2008, which was followed by the Ministry of Industry and Information Technology’s non-binding Internet Information Services Market Order Provisions of 2011. However, little direct progress was made until the standing committee of the National People’s Congress (NPC) introduced its Decision on Strengthening Internet Information Protection (the Decision) on December 28, 2012. Echoing Directive 95/46/EC in the EU by stipulating that the collection and use of information will be “legitimate, proper, and necessary,” the Decision seeks to protect network information security; the lawful interest of citizens, legal persons, and other organizations; and safeguard China’s security and social order through its Articles.

The Decision’s first Article states that “[n]o organization or individual may steal or obtain in other illegal manners [ ] citizens’ individual electronic information, sell or illegally provide citizens’ individual electronic information to other persons.” Instruction to Internet Service Providers (ISPs) continues, where providers must, among other activities:

- Clearly indicate the purposes, methods, and scope of collection and use of citizens’ data;
- Obtain agreement from citizens before collecting their data;
- Publicize rules for the collection and use of personal data;
- Preserve the secrecy of collected data;
- Not divulge, distort, or damage the data;
- Refrain from selling or otherwise illegally providing the data to others; and
- Adopt technical measures and other methods to ensure information security and prevent damage to or loss of the data.

Among the provisions of the Decision is Article Six, specifically directed at network service providers, whereby users of the services must “provide real identity information” prior to “website access,” “fixed telephone, mobile telephone,” “other surfing formalities,” or “information publication services.” In response to criticism that Article Six would be used to discourage whistleblowers and other Chinese dissention, the government-sponsored Xinhua News Agency argued that the Decision “will help, rather than harm, the country’s netizens.”
2. Japan

On May 24, 2013, the LDP-led ruling coalition directed the passage of the “Common Number” Bill through both Diet chambers. The Common Number Bill plans to assign every Japanese resident, including mid-to-long-stay foreigners and special permanent residents, a personal identification number beginning in January 2016. Additionally, a portal site through which people can check their social security records and other information via the Internet is planned for 2017. The numbering system was originally proposed in 2009, but remained quiescent until the LDP-New Komeito ruling coalition mustered sufficient support based, in part, on a philosophical foundation for fair social welfare and tax systems.

To oversee some aspects of the ID system, a third-party independent committee with independent authority will oversee allegations of data mishandling by public officials. Those who leak or illegally commercialize ID information will face up to four years in prison or a ¥2 million fine. While the use of a single number system has raised some concerns, including the potential for “forcible data-matching,” the government push for support has focused on efficiencies in administration and easier detection of tax evasion and welfare fraud.

3. Malaysia

On November 15, 2013, the Personal Data Protection Act (PDPA) of 2010 was entered into force, introducing an omnibus privacy regime in Malaysia for the first time. This new regulation carries a host of requirements, including registration with the Personal Data Protection Department of Malaysia (PDPD) for a number of industries, including (among others) banking and financial institutions. The PDPA also includes the threat of severe consequences for non-compliance, including “fines for companies and/or fines and imprisonment for directors and officers of the company.”

4. Kazakhstan

On November 26, 2013, Kazakhstani Law No. 94-V on Personal Data and its Protection came into force, defining such concepts as “personal data” among others, but left some ambiguity in how data might be transferred and/or stored internationally. It also contained a number of limitations: Law No. 94-V does not extend to the collection of personal data for personal and family needs; the use of information for the Kazakhstani National Archive; the collection, processing, and protection of personal data related to Kazakhstani state secrets; or the use of information related to intelligence, counter-intelligence, and criminal activities, within legal limits.

5. South Korea

Article 16 of South Korea’s Personal Information Protection Act (effective September 30, 2011) was amended on August 6, 2013 to incorporate an affirmative obligation on the part of a personal information processor, requiring notification to data subjects that data subjects may deny consent for the collection of any personal information other than for any purposes under Article 15(1). This continues South Korea’s stringent efforts to promote data privacy, and provides another instance of South Korea’s articulation of a minimum data collection regime.

6. Singapore

Singapore’s Personal Data Protection Act (PDPA), passed in 2012, went into effect on January 2, 2013, the same day Singapore’s Personal Data Protection Commission (PDPC) was established; some portion of PDPA does not come into full effect until July 2, 2014. The PDPC followed-up the implementation of the PDPA with a further guidance note on September 24, 2013 which, among other topics, gave direction to organizations regarding notification requirements for the collection, use, or disclosure of personal data as well as the anonymization of personal data. This guidance outlined the use of ‘cookies’ for internet user’s online activity, distinguishing in part
between active consent on one hand, and “the mere failure of an individual to actively manage his browser settings” on the other.

7. Hong Kong

Revisions to Hong Kong’s Personal Data (Privacy) Ordinance – Code of Practice on Consumer Credit Data – took effect on April 1, 2013. These revisions require consent prior to the use of personal data in the context of targeted, direct advertising, and instruct individuals that, while direct marketers must notify individuals of their opt-out right prior to using personal data for the first time, individuals may choose to opt out at any time at no cost to the individual opting out. The Ordinance also provides for the following penalties: if “the transfer of personal data to third parties [is] for gain, the maximum penalty is a fine of HK$1,000,000 and imprisonment for 5 years. For other direct marketing contraventions, the maximum penalty is a fine of HK$500,000 and imprisonment for 3 years.”

8. India

While India currently adheres to the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (Rules) enacted in 2011, the Centre for Internet and Society presented a new Privacy (Protection) Bill, 2013 (Bill), on September 30, 2013. The Bill seeks to further refine provisions of the Rules, with a focus on protection of personal data through limitations on use and requirements for notice. The collection of personal data would be prohibited unless “necessary for the achievement of a purpose of the person seeking its collection,” and, subject to sections 6 and 7 of the Bill, “no personal data may be collected under this Act prior to the data subject being given notice, in such form and manner as may be prescribed, of the collection.” The Bill acknowledges the collection of data with and without consent; the regulation of personal data storage, processing, transfer, and security; and discusses the different types of disclosure.