A comprehensive privacy regime rising on the Eastern horizon

As China's trickle of data privacy regulation threatens to turn into a cascade, companies operating in China will wish to closely monitor new and developing regulations, and maintain regular compliance checks to ensure internal policies and procedures adhere to this emergent legal framework. In the past year, China's data privacy framework has integrated a trio of developments – a law, regulation, and a voluntary national standard – that suggest the beginnings of a data privacy regime containing many of the common features existing in other jurisdictions. Further legislation, in particular for the mobile space, is expected shortly. Eric Carlson and Scott Livingston, Partner and Associate respectively at Covington & Burling in Beijing, outline these recent legislative efforts.

Legislative Background

Historically, China's regulations on data privacy have been scattered among various industry-specific regulations and typically drafted so broadly as to give little practical guidance for a company's internal compliance efforts. The three new regulations have begun to clarify these otherwise vague contours, and provide key guideposts for companies looking to navigate China's regulatory patchwork.

The Regulation

This current trend of online regulation started in December 2011 with the passage of the Several Provisions on Regulating the Market Order of Information Systems ('Market Order Provisions'), effective 15 March 2012. The Market Order Provisions, promulgated by China's internet regulator, the Ministry of Industry and Information Technology ('MIIT'), apply to 'Internet Information Service Providers' ('IISPs') such as websites and other providers of content through the internet. The Market Order Provisions are the most extensive binding data privacy regulations to date in China and include the following key provisions:

- A definition for 'users' personal information' as 'information that is relevant to users and can serve to identify users solely or in combination with other information'.
- A notice and consent provision requiring IISPs to inform users of the ways they collect and process personal information, the information collected and the purpose for collection, and to obtain users' consent for such collection.
- A minimal collection requirement that limits collection of personal information to only that necessary for the provision of services.
- A use limitation/purpose specification provision that restricts IISPs from using personal information for any purpose outside of the scope of services.
- A data security provision that requires IISPs to 'properly' maintain their users' personal information, with a requirement that IISPs take immediate remedial action in the event of a data breach, and, where serious, report to MIIT.

However, despite its contributions to China's emerging data privacy framework, the Market Order Provisions leave unclear the precise form a company's notice should take or any further guidance on how a user may evidence consent. The Market Order Provisions also do not provide for any form of user rights, such as the ability to access, delete, or revise an individual's personal information held by an IISP.

The Law

China continued to emphasise a more advanced regulatory framework with the passage of the Decision on Strengthening Online Information Protection ('Online Information Decision') by the national legislature, the Standing Committee of the National People's Congress, on 28 December 2012. The Online Information Decision applies to 'network service providers' and all other 'enterprises or public institutions,' a scope significantly broader than the Market Order Provisions' focus on IISPs and implicating any company that handles 'electronic personal information.' [1]

The Online Information Decision contains the following significant data privacy provisions:

- A notice and consent provision similar to the Market Order Provisions by which network service providers and all other enterprises or public institutions must clearly indicate the 'use, method, and scope' of their collection of an individual's 'personal electronic information' and not to collect or use this information without consent.
- A data security provision requiring network service providers, other enterprises or public institutions, or their employees to adopt technological and other measures necessary to protect information security and protect against 'disclosure, damage, or loss of an individual's electronic personal information.' Similar to the Market Order Provisions, collectors of personal information must 'strictly maintain the confidentiality' of information collected during the provision of services.
- A use limitation provision to ensure network service providers, other enterprises or public institutions, or their employees do not 'disclose, distort, or damage' that information. If a collector violates this provision, it must adopt

'immediate' remedial measures.

- A user rights provision asserting that citizens 'have the right to require a network service provider to delete the relevant information or adopt other necessary measures' where the citizen discovers that their 'individual identity has been [illegally] divulged, individual privacy has been disseminated, or other network information infringes their lawful rights and interests.'

Although the Online Information Decision is classified as law, and occupies a higher status in China's legislative hierarchy than the Market Order Provisions, its specific provisions are drafted somewhat broadly, and some are repetitive of provisions found in other regulations. It is likely that the law is meant in part to signal the high priority the Government places on ensuring enhanced online data privacy, as well as to provide further legislative guidance to MIIT. We understand that MIIT is currently drafting implementing regulations for the Decision.

The Standard

Although China continues to lack a comprehensive law, the promulgation of a voluntary national standard entitled Information Security Technology - Guidelines for Personal Information Protection Within Public and Commercial Services Information Systems ('PI Guidelines') in November 2012, effective 1 February 2013, is China's most extensive guidance to date on the expected responsibilities and duties of parties to transfers of personal information carried out over 'information systems.'

The PI Guidelines categorise personal information handling into four phases: collection, processing, transfer, and deletion, with voluntary requirements for each phase. While these requirements represent an authoritative statement on recommended data handling procedures, the fact that the PI Guidelines are a type of voluntary national standard means that they lack the force of law. Our sources indicate a mandatory national standard covering online personal information is currently in development, though there is no word on its expected release date.

A mandatory national standard covering online personal information is currently in development, though there is no word on its expected release date

Although voluntary, the PI Guidelines nevertheless contain a number of key features found in other jurisdictions' data privacy regimes including:

- An enumerated list of eight 'basic principles' for handling of personal information, including purpose specification, minimal collection, data quality warranty, security safeguards, faithful performance, and accountability.
- A notice and consent requirement for the collection of an individual's personal information with an extensive list of content required for inclusion in notice provisions.
- User rights provisions including the duty to verify, revise, or supplement collected personal information, upon request of the data subject, to ensure that it is correct. When the collection of personal information is continual (e.g. information collected via a social network), the collector must provide the data subject with appropriate tools to configure, adjust, or terminate its provision of personal information.
- The division of 'personal information' into 'personal sensitive information' and 'personal general information,' with '[p]ersonal sensitive information' defined as information that would have an adverse impact on the subject if disclosed or altered, and 'personal general information,' defined as all personal information other than personal sensitive information. This distinction is similar to that found in the EU data privacy regime.

Significantly, the PI Guidelines prohibit transfers outside of mainland China of personal information to an entity absent express user consent, government permission, or other explicit legal or regulatory permission. The PI Guidelines do not explicitly carve out intra-company transfers from this prohibition.

Although a voluntary standard, the PI Guidelines are likely to be helpful guidance for design or revision of a company's privacy program, particularly as their voluntary requirements may be integrated into the upcoming regulations discussed below.

The Future

The passage of this regulatory trio signals an increased emphasis on regulating online personal information by PRC authorities. As noted above, we understand that MIIT has begun to issue draft implementing regulations for the Online Information Decision and is also currently drafting a mandatory national standard for online personal information. Chinese regulators also are reportedly drafting other regulations targeting online app stores, mobile devices and mobile applications, and online advertising, each of which may contain significant data privacy provisions.

Eric Carlson
Partner
Covington & Burling
ecarlson@cov.com

Scott Livingstone
Associate
Covington & Burling
sdlivingston@cov.com

Footnotes:
1. The term is undefined in the law but described as information 'by which the individual identity of citizens can be distinguished as well as that which involves a citizen's privacy.'