COVINGTON

COVINGTON & BURLING LLP

E-ALERT | Global Privacy & Data Security

February 15, 2013

CHINA RELEASES NEW NATIONAL STANDARD FOR PERSONAL INFORMATION COLLECTED OVER INFORMATION SYSTEMS

China's Standardization Administration and the General Administration of Quality Supervision, Inspection, and Quarantine have jointly released a long-awaited national standard related to personal information. Entitled *Information Security Technology -- Guidelines for Personal Information Protection Within Public and Commercial Services Information Systems* (信息安全技术公共及商用服务信息系统个人信息保护指南) ("Guidelines"), the new standard took effect February 1, 2013. The Guidelines are voluntary and lack the force of law. They nevertheless clarify key expectations for relevant actors collecting personal information ("PI") and outline how PI is to be handled in four phases: collection, processing, transfer, and deletion, with voluntary requirements for each phase. The Guidelines also set out eight "basic principles" for handling of PI within China.

The Guidelines apply to PI handled through "information systems," which is defined to refer to computer information systems, including mobile devices, that "collect, process, store, transmit, search, or otherwise handle information." The Guidelines are specifically excluded from applying to government agencies or other institutions exercising "public management" functions.[1] Under the Guidelines, "third-party testing and evaluation agencies" will be created to conduct independent testing and evaluation of company's information systems as well as to provide industry guidance and supervision for all aspects of PI protection.[2]

China has two types of standards: mandatory and voluntary. As a voluntary standard, the Guidelines may impact companies operating in China in two principal ways. First, while the Guidelines lack the force of law, they might serve as a regulatory baseline for PRC judicial and law enforcement authorities to judge a company's data privacy efforts in criminal or civil litigation or in administrative proceedings. The Guidelines also may reflect an evolving consensus by China's policy-makers regarding data privacy that may be further extended in subsequent binding legislation.

At the same time the Guidelines were announced, the government also announced the creation of an industry advisory group, titled the Personal Information Protection Alliance (个人信息保护推进联盟), that could play some role in industry self-regulation. While this group may have a voice in drafting and consulting on future standards or regulation, is it unclear how much influence it will have, particularly in certain industries.

---

[1] Although state agencies are excluded from the terms of the Guidelines, the "illegal provision" of PI by state agencies and other institutions with access to large amounts of personal information is currently prohibited by Article 253(a) of the PRC Criminal Law.

[2] The appearance of this type of third-party agency is not without precedent. In 2007 the *Administrative Measures for the Classified Protection of Information* issued by the Ministry of Public Security required "entities operating and/or using information systems" to select an evaluation agency to audit the security status of their information systems on a regular basis. As of July 2011, more than 100 such agencies had been registered across China, two of which served as drafting advisers for the Guidelines. We understand from consultation with these agencies that they may be tasked with responsibility for supervising PI compliance efforts.

Reports have indicated that the Ministry of Industry and Information Technology (MIIT), China's main internet regulator and a contributor to the Guidelines, is currently in the process of drafting *mandatory* guidelines concerning the protection of user PI, specifically with regard to the telecommunications and internet industries. No clear timeline currently exists for the finalization of this standard.

Companies with operations in China will wish to consider modifying their existing data privacy procedures in light of these recent developments.

Further Guidance Provided on "Personal Information" and Notice Requirements

The Guidelines contain a number of provisions significant to companies assessing the current patchwork of PRC data privacy regulation. Most notably, "personal information," a term long used but never defined in PRC regulation, is defined in the Guidelines as "computer data that may be processed by an information system, relevant to a certain natural person, and that may be used solely or along with other information to identify such natural person." This definition in the Guidelines follows a similar definition of "users' personal information" ("information that is relevant to users and can serve to identify users solely or in combination with other information") contained in the recently MIIT-promulgated *Several Provisions on Regulating the Market Order of Internet Information Services* ("Market Order Provisions"). The similarity of the two definitions suggests that MIIT has coalesced around an official definition for this previously ambiguous term.

The Guidelines divide personal information into "personal sensitive information" and "personal general information," similar to the distinction in the EU data privacy regime. "Personal sensitive information" is defined as information that would have an adverse impact on the subject if disclosed or altered, while "personal general information" is defined as all personal information other than personal sensitive information. The Guidelines instruct that the specific contents of "sensitive" PI "shall be determined in accordance with the industry's unique characteristics and the desires of the data subject," although how this will work in practice, or where final authority rests for this determination, remains unclear. The Guidelines note, however, that sensitive PI may include such items as identity card numbers, race, political viewpoint, religion, or biometric information.

Under the Guidelines, PI may be collected only if the user is notified of the following before collection:

- the purpose of collection;
- the methods and means of collection, specific information collected, and time of retention;
- the scope of use of the collected PI, including the scope of disclosure or provision to other organizations and institutions;
- the PI Administrator's measures for protecting PI;
- the PI Administrator's name, address, and other contact information;
- the potential risks the PI Subject may encounter after providing PI;
- the potential consequences if the PI Subject is unwilling to provide PI;
- the available channels of complaint for the PI Subject; and
- in circumstances where PI is transmitted or entrusted to another organization:
  - the purpose for transmission or entrustment;
  - the specific PI and scope of use of the transmitted or entrusted PI; and
  - the name, address, and contact information of the recipient of the entrusted PI.

If the PI is "sensitive," then the data subject must clearly give their consent prior to collection and keep evidence of their consent. If "general," tacit consent is assumed unless expressly objected to. The Guidelines give no further guidance on how consent is to be obtained.

Previously, notice requirements have been included in regulations targeting internet information service providers, such as the Market Order Provisions, and laws targeting entities handling "personal electronic information," such as the recent *Decision of the Standing Committee of the National People's Congress on Strengthening Online Information Protection*. (See our client alerts here and here.) While these provisions mandate a notice requirement, they fail to describe what specific information should be contained in the notice, which has complicated compliance efforts for companies handling PI in China. The more detailed description of notice content outlined in the Guidelines may therefore be helpful to guide organizations in designing notices and policies.

Significantly, the Guidelines also prohibit overseas transfers of any PI to an entity absent express user consent, government permission, or other explicit legal or regulatory permission. The Guidelines do not explicitly carve out intra-company transfers from this prohibition. This final formulation adds an exception for user consent that was not found in an earlier published draft, although it remains unclear at what time (i.e., prior to transfer or in the original notice) this consent must be obtained.

Potential Next Steps for Companies with Operations in China

The recent uptick in data privacy legislation, and the creation of the self-regulatory group discussed above, indicate that China is increasingly focused on creating a more comprehensive domestic data privacy regime and further legislative activity should be expected. The selection of a voluntary, rather than mandatory, standard indicates that China has decided on an incremental evolution of their data privacy legislation, with present efforts likely to serve an experimental role based on which future more comprehensive legislation may be developed and perfected.

With the release of the Guidelines, companies collecting PI within China may wish to consider revisiting their current online privacy policies to determine:

- whether current notice and consent policies for the company's collection and use of PI accord with the requirements of the Guidelines;
- whether current policies include obtaining special consent for the collection of any PI that may be considered "sensitive", or when any PI is transferred outside mainland China; and
- internally, whether current processing, transfer, and deletion practices accord with the requirements of the Guidelines.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our global privacy & data security practice group:

Daniel Cooper	+44.(0)20.7067.2020	dcooper@cov.com
Eric Carlson	86.10.5910.0503	ecarlson@cov.com
Scott Livingston	86.10.5910.0511	sdlivingston@cov.com