WILMERHALE

China Issues Draft Guidelines on Online Privacy, Announces New Agency to Supervise the Internet

2011-05-19

China on February 10, 2011 issued the draft Information Security Technology – Guidelines for Personal Information Protection (the "**Guidelines**," or the "**Draft**") for comment. The purpose of the Guidelines, according to the preamble, is to "guide and standardize information-processing activities using information systems" in light of the "increasing use of the Internet and increasingly central role of personal information in social and economic activities." This action indicates the central government's intent to step up its efforts to regulate online data transactions in response to the rapid growth of e-commerce and the slow progress of the long-awaited *Personal Information Protection Law* (the first draft of which was completed in 2005). In addition, establishment of the State Internet Information Office parallel to the State Council Information Office announced on May 4, 2011 signifies that there will be tighter control of the Internet generally.

Non-binding "Guiding Technical Document". The Draft takes the form of a standard rather than a regulation and as such was issued by the Administration of Quality Supervision, Inspection and Quarantine ("**AQSIQ**") and the Standardization Administration of China ("**SAC**"), the latter of which is responsible for the formulation of standards. In fact, the

Draft was published on the website of the Ministry of Industry and Information Technology ("**MIIT**") which is responsible for industrial policy and information technology but is not known to have a strong concern regarding privacy protection.

The Guidelines were drafted by the China Software Testing Center ("**CSTC**," an administrative and research unit under MIIT) together with major technology industry associations and internet companies closely related to MIIT. The governing authority for the finalized guidelines will be the Technical Committee on the National Standardization of Information Security under SAC. The Draft also indicates that the Guidelines when finalized will be non-binding. Specifically, they will constitute a "Guiding Technical Document," one of three categories of documents issued by SAC. Of the other two categories, "Mandatory Standards" govern key industries affecting public health and safety as well as individual property rights and must be observed by all relevant parties; while "Recommended Standards" cover less critical areas and are made available for voluntary adoption by private parties in business transactions. The "Guiding Technical Documents" category includes guidelines for on-going efforts to standardize new and still-developing technologies for which formal standard-making is premature. Guiding Technical Documents are for voluntary reference and unenforceable against the targeted subjects. In practice, however, they may induce compliance by participants concerned about competition and reputation.

Not constituting legislation or regulations, the Draft does not address such issues as legal causes of action, administrative remedies, enforcement, or indeed if there will be an enforcement body. Nor does it shed any light on the question of whether the protection of online privacy would affect access by security authorities to personal data based on privacy concerns.

Nevertheless, because the Draft reflects MIIT's current state of mind with respect to regulation of the collection, processing, transfer, maintenance, use, and deletion of personal information on the internet for privacy purposes, its issuance is significant for internet service providers ("ISPs"), internet content providers ("ICPs"), ad networks, market information collectors and processors, and other players in China's fast-growing internet economy. As the Draft prohibits the export of regulated data unless specifically allowed by law or regulation or as agreed by the industry regulator (MIIT), it could also affect multinationals' centralized HR management and even the processing of student information by foreign universities. Should a substantially unchanged final version be adopted, especially if it is reflected in legislation or regulations, it is likely to increase the cost of compliance and risk management.

Definition of "Personal Information". The Draft defines "Personal Information" as "any knowable information relating to a natural person that can be used, either alone or in combination with any other information, to specifically identify such natural person." Thus, despite its name, the underlying concept is more akin to the business-centered concept of PII (personally identifiable information) than the privacy-oriented PI (personal information). It would not cover any information used for profiling and targeting advertisements if such information is used to contact or locate individuals without uniquely identifying them. On the other hand, "alone or in combination" signifies a potentially very broad scope. Without "alone or in combination," the definition would exclude most behavioral attributes of an individual (i.e., online browsing history), although such behavioral attributes when combined with demographic (e.g., address, date of birth, and gender) or other behavioral information may be sufficient to identify an individual.

This definition appears to be responsive to the most common privacy concern in China today. Consumers complain that they start to receive marketing calls and/or text messages after they buy a house or a car, open a bank account or purchase insurance. A few recent criminal prosecutions for the illegal appropriation, sale, and provisions of citizen personal information under Art. 7 of the Criminal Law have traced such unsolicited advertisements to the unauthorized sale of electronic customer files by employees of entities that keep customer files on their computer networks. To date privacy complaints voiced by consumers in the media typically do not implicate the use of sophisticated behavioral tracking software or the act of pushing advertisements through to computers without uniquely identifying their users.

Definition of "Personal Information Administrator". The Draft defines "Personal Information Administrator" ("**PIA**") as "a natural or legal person who has actual power to administer personal information." The term "actual power" extends the reach of these Guidelines beyond ISPs or ICPs to include such third-party data collectors as ad networks and market research firms, even firms that install tracking software hidden in free software offered to websites.

Guidelines on handling personal data online. In essence the Guidelines would adopt the notice-based model and non-technological privacy protection methods commonly used in the past two decades of industry self-regulation in the West. The core principles and requirements in the Guidelines require that personal data may be collected only directly from the individuals indicated, with notice of the purpose and scope of the prospective use of such data, and require consumer consent with respect to the collection, use, and disclosure of their personal data. Other requirements include: consumers can request access to their personal data retained by a

PIA by contacting its designated personnel; processing and use may not exceed the scope of stated purposes; consumers with a "proper reason" can request that a PIA delete their personal data; and retention of data is limited to fulfillment of the stated purpose.

Prohibition of transfer of personal data out of China. The Draft prohibits transfer of personal data out of China without the express consent of the "governing administrative authority." Its enforcement would mean that foreign data collectors and consumer intelligence providers must form a subsidiary in China for data processing and may not transfer collected data to processing centers outside China without the prerequisite consent. This would arguably constitute a trade restriction, but MIIT has a history of protectionism.

Although the context suggests that the targets of the Guidelines are Internet data collectors and processors, technically such a prohibition could become an obstacle to integrated HR management for multinationals with operations in China. For example, the enforcement authorities could prohibit multinationals from transferring employee data outside China. For multinationals that maintain centralized HR functions, this could mean that they must obtain consent from authorities before sending information on employees in China to central files. This will cause unnecessary cost and inconvenience to multinationals doing business in China. Even foreign universities could be entangled with respect to the administration of Chinese student and employee data and study-abroad programs. Such prohibition would also, and presumably unintentionally, reduce the international competitiveness of Chinese information service outsourcers if they are restricted in their ability to transfer data outside of China.

Conclusion

China as yet does not have a comprehensive law on Internet privacy. Although China in October, 2009 amended its *Criminal Law* to include crimes relating to the handling of personal data and introduced administrative measures on the handling of such sensitive information as personal financial and health information, it has generally been cautious in its approach to comprehensive regulation of online privacy. Contrary to widespread anticipation, the 2009 *Tort Law* does not address privacy protection, and the pending amendment to the *Consumers Rights Protection Law* proposes to protect only the most basic demographic attributes plus financial and health information. This, together with the non-binding status of the Guidelines indicates that the central authorities are undecided about the balance between protecting privacy online and ensuring that the Internet remains a platform for economic growth, but the decision to establish a new State Council Office with supervisory responsibility over the Internet signifies an intent to increase regulatory scrutiny and capability. Maintaining access to personal information for national security reasons may also be a factor. It remains to be seen which of the Guidelines will be transformed into regulations, or whether the central authorities will let the Guidelines serve as a benchmark for self-regulation of the online-ad industry as technology continues to develop.

Authors

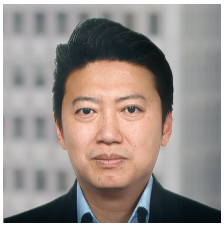
Lester Ross

PARTNER

Partner-in-Charge, Beijing Office

lester.ross@wilmerhale.com

+86 10 5901 6588



Kenneth Zhou

PARTNER

kenneth.zhou@wilmerhale.com

+86 10 5901 6588