MORRISON | FOERSTER

Morrison & Foerster Client Alert.

April 11, 2011

China Issues New Guidelines on Data Privacy Protection

By Paul D. McKenzie, Arthur F. Dicker, and Jingxiao Fang

The PRC General Administration for Quality Supervision, Inspection, and Quarantine ("GAQSIQ") and the Commission for the Administration of Standardization (the "Commission") have circulated a draft *Information Security Technology Guidelines for Personal Information Protection* (the "Guidelines"). The Guidelines, if issued, would represent another in a series of recent efforts by Chinese authorities to address their citizens' personal data protection concerns in the absence of a comprehensive regulation on this issue.

HIGHLIGHTS

Notable highlights from the Guidelines include:

- Clarification on the definition of personal information to include any information that (i) is able to be collected and processed; (ii) relates to individuals; and (iii) by itself or in combination with other information could disclose the identity of the individual;
- An overarching principle that the holders of personal information keep such information confidential, and a specific requirement that express consent be obtained for all third-party disclosures of personal information;
- A set of more specific principles to be observed during the collection, processing, use, transfer, and maintenance of personal information;
- Application of such principles specifically to personal data on *computer networks* (as opposed to other data storage media in hard-copy form);
- Restrictions on outsourcing the handling of personal information; and
- Prohibition on the export of personal information unless expressly permitted by law or otherwise approved by government authorities.

BACKGROUND

As we discussed in previous client alerts in 2009 and 2010, China lacks a comprehensive national law focusing exclusively on the regulation of data privacy. A draft *Personal Information Protection Measures* (the "Measures") was prepared by a group of legal scholars commissioned by the

Beijing

Paul D. McKenzie 86 10 5909 3366
Jingxiao Fang 86 10 5909 3382

Brussels

Karin Retzer 32 2 340 7364
Joanne Lopatowska 32 2 340 7365

Hong Kong

Gordon A. Milner 852 2585 0808
Nigel C.H. Stamp 852 2585 0888

Los Angeles

Mark T. Gillett (213) 892-5289
Michael C. Cohen (213) 892-5404
David F. McDowell (213) 892-5383
Russell G. Weiss (213) 892-5640

London

Ann Bevitt 44 20 7920 4041
Anthony Nagle 44 20 7920 4029
Chris Coulter 44 20 7920 4012

New York

Joan P. Warrington (212) 506-7307
John F. Delaney (212) 468-8040
Madhavi T. Batliboi (212) 336-5181
Suhna Pierce (212) 336-4150
Marian A. Waldmann (212) 336-4230
Miriam Wugmeister (212) 506-7213
Sherman W. Kahn (212) 468-8023

Northern Virginia

Daniel P. Westman (703) 760-7795
Timothy G. Verrall (703) 760-7306

Palo Alto

Bryan Wilson (650) 813-5603
Christine E. Lyon (650) 813-5770

San Francisco

Roland E. Brandel (415) 268-7093
James McGuire (415) 268-7013
William L. Stern (415) 268-7637
Jim McCabe (415) 268-7011

Tokyo

Daniel P. Levison 81 3 3214 6717
Gabriel E. Meister 81 3 3214 6748
Jay Ponazecki 81 3 3214 6562
Toshihiro So 81 3 3214 6568
Yukihiro Terazawa 81 3 3214 6585

Washington, D.C.

Andrew M. Smith (202) 887-1558
Cynthia J. Rich (202) 778-1652
Julie O'Neill (202) 887-8764
Nathan David Taylor (202) 778-1644
Obrea O. Poindexter (202) 887-8741
Reed Freeman (202) 887-6948
Richard Fischer (202) 887-1566
Kimberly Strawbridge Robinson (202) 887-1508

Chinese government but has not been adopted to date. Amendments to the *Criminal Law* (the "Criminal Law Amendments") adopted in 2009 attempted to address unlawful disclosure or acquisition of certain kinds of personal data and have since been used by courts in deciding cases during the last two years. After several drafts spanned over seven years, the *Tort Law* finally came into effect in 2010 with one of the most notable developments being recognition of a private right of action of an individual to bring a tort claim for damages based on a breach of his or her right to privacy.

The drafters of the Guidelines have attempted to pick up the proverbial regulatory "baton" by preparing the Guidelines as a "national standard" under China's GB ("*guobiao*") standardization system, but only as a voluntary guideline (GB/Z) lacking the force of law. By contrast, China has issued numerous mandatory standards, particularly of a technical nature, which are enforced by relevant administrative agencies concerning the protection of human health, personal property, and safety. Examples of non-mandatory standards (GB/Z, GB/T) include standards for book numbering, codes for representing the names of countries, and use of punctuation marks. Examples of mandatory standards include road traffic signs and markings, civil engineering codes for seismic design of buildings, and names of various Chinese nationalities.

PRINCIPLES

The Guidelines provide a general principle requiring that the holders of third-party personal information keep such information confidential. The individual should be notified as to the manner of collection, processing and disclosure of his or her personal information, and should have a right and opportunity to object to such collection, processing and disclosure. The individual should also have the right to request that his or her personal information be corrected or removed from the holder of such information.

The Guidelines also set forth more specific principles on how personal information may be collected, processed, used, transferred and maintained.

COLLECTION, PROCESSING, AND USE OF DATA

With respect to the collection, processing, and use of personal information, these principles state:

- In order to collect and process the personal information of an individual, the individual should be notified about the purpose of collecting such information, the contact information of the entity collecting it, and the rights that the individual has (for example to object to such collection), and information on how to raise a complaint;
- Personal information should only be used for the purpose stated to the individual when the information was collected, unless otherwise stipulated in law or clearly agreed to by the individual;
- The collection of certain types of personal information is prohibited if not relevant to the stated purpose provided to the individual at the time of collection, in particular information related to religious beliefs, ethnicity, fingerprints, and genetics;
- In order to collect the personal information of an individual under the age of 16, consent from a custodian should be obtained.

The restriction to use data only for the purpose stated to the individual at the time of collection may present certain administrative difficulties for a company. Presumably it could be quite difficult to go back to customers after they have provided personal information in connection with a completed product purchase to obtain further consents to the use of their information. Companies would have to find the right balance in stating such purposes broadly at the outset to capture all potential uses, but not so broadly as to discourage customers from purchasing the underlying products or services.

EXPORT AND OTHER TRANSFERS OF DATA

With respect to the transfer of personal information:

- Express consent from the individual must be obtained in connection with the transfer of personal information to any other organization (within or outside of China);
- The export of personal data is limited to where the law expressly permits it or the export has otherwise been approved by government authorities; and
- The transferring party should specifically ensure the security of the personal information during the transfer process.

The obligation to obtain express consent from an individual in order to disclose his personal information to another organization exceeds disclosure requirements in other jurisdictions such as the European Union. The corresponding EU directive provides specific exceptions to its consent requirement where sharing the information is necessary to complete the contract or satisfy pre-contractual obligations. However, the Guidelines in their current recommended form do not state any such exceptions. The Guidelines also do not define the term "other organizations," and therefore interpreted literally could even preclude transfers to affiliates of the company holding the individual's personal information.

Cross-border transfers of data are prohibited unless an exception is found in the law or they are otherwise approved by government authorities. We are not aware of any Chinese law currently in place that would provide explicit exceptions to this prohibition on the export of such data. Moreover, a literal interpretation of the Guidelines would prohibit the export of personal information even where the individual has consented to such export. However, it is also important to remember that the Guidelines are only to be issued as a recommended "guideline" standard, and would not be mandatory. We expect that the language in the Guidelines prohibiting export may be acting as a placeholder until the Guidelines are actually promulgated with the force of law, if at all. At that time, and presumably after receiving additional feedback from the business community, clearer regulations carving out exceptions to the export prohibition may be adopted.

Of course many companies outsource data processing (including the handling of personal information) to third-party service providers located in China. These companies would be reluctant to outsource such data processing to China-based providers if export restrictions created potential difficulties in having such data returned to them. In this regard, it is important to note that the prohibition on exporting personal data applies to any "administrator" of personal information, defined as "the natural person or legal person with the right to manage the personal information." [There is some room for interpretation, but presumably the prohibition may be understood to apply only to an entity which outsources the data processing since it has the actual right to manage the data under the primary contract with the individual.] Under this interpretation, any subsequent "export" of the data by a Chinese outsourcing company back to the foreign company would not be an export by the relevant "administrator" and thus not subject to the export prohibition of the Guidelines. This conclusion would be consistent with EU law if the concept of a personal information administrator under the Guidelines was analogized to a "data controller" under EU law. We expect that subsequent implementing regulations for the Guidelines, if promulgated, would more explicitly carve out this exception. Otherwise, the export restriction strictly applied would potentially be a fatal blow to certain sectors of the Chinese outsourcing industry.

Other provisions of the Guidelines contemplate the outsourcing of data processing that involves handling personal information, though the Guidelines' requirements are relatively consistent with the requirements of other jurisdictions and existing best practices of most large companies. The Guidelines would place affirmative obligations on the entity outsourcing this function to notify the individual that the handling of his or her personal data has been outsourced to a third party, and to ensure that the third party also complies with the stipulations of the Guidelines. The outsourcing

service contract with the third party should also specify obligations of the third party to provide for security of the personal information. The outsourcing company should also delete the personal information after it has performed the required services.

IMPLEMENTING THE GUIDELINES

If issued, the Guidelines would certainly appear to be an attempt by the Chinese government to fill a regulatory gap where a comprehensive personal information law remains elusive. As the Guidelines would be issued as a recommended "guideline" standard only, we suspect that the authorities may want to "test the waters" to see how these standards are accepted and put into practice by the local business community. The Guidelines only apply to computer networks (generally understood to also include standalone computers and the Internet), and in fact specifically acknowledge the input of major Chinese internet portal site providers such as Baidu, Sina, and Tencent. In fact, we understand that the delay in issuing the Guidelines has been a result of the authorities having been flooded with additional comments from interested parties.

In the interim, we would expect that implementing the Guidelines may prove to be a useful defense for companies operating in China that may be the subject of lawsuits under the Criminal Law Amendments or Tort Law. Where a company is sued for a criminal or tortious act of its employee in making use of personal data housed at the company, it should be helpful (in an attempt to divorce itself from the rogue actions of an employee) to demonstrate that a company has adopted the principles of the Guidelines in its internal control procedures.

We will continue to monitor developments in this field to see if these Guidelines are issued and how they may be further implemented, and update our clients as appropriate. We would also be happy to provide an English translation of the Guidelines upon request.

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials in many areas. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer*'s A-List for seven straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Morrison & Foerster has a world-class privacy and data security practice that is cross-disciplinary and spans our global offices. With more than 60 lawyers actively counseling, litigating, and representing clients before regulators around the world on privacy and security of information issues, we have been recognized by *Chambers* and *Legal 500* as having one of the best domestic and global practices in this area.

For more information about our people and services and the resources we offer such as our free online Privacy Library, please visit: http://www.mofo.com/privacy--data-security-services/.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations.