

Morrison & Foerster Client Alert.

February 23, 2012

China's Online Data Privacy Rules Coming into Effect; Other Recent Data Privacy Developments in China

By Paul McKenzie and Jingxiao Fang

China, like many jurisdictions, continues to grapple with the issue of whether and how to protect personal information in light of new technologies and services designed to collect and use personal information in new and different ways. An omnibus privacy law in China continues to be elusive but, as [prior Morrison & Foerster alerts](#) have reported, various government authorities in the People's Republic of China ("PRC"), both at the central level and in some localities, are gradually putting in place laws and regulations in an attempt to address these new issues.

One of the more far-reaching legislative efforts in recent months is new regulations issued by the Ministry of Industry and Information Technology ("MIIT") governing the collection, storage and use of personal information by Internet companies. This alert discusses these new regulations, which come into effect next month. It also discusses privacy regulations recently issued by Jiangsu Province, as well as a number of other recent privacy law developments in China.

INTERNET REGULATIONS

Last July, MIIT issued for public comment a draft entitled *Provisions for Administration of Internet Information Services* (《互联网信息服务管理规定 (征求意见稿)》) setting out basic rules governing online operations of so-called "Internet Information Service Providers" in respect of their collection, storage and use of personal information of users.

Final promulgation of these draft provisions became a particular priority after a series of high profile cases at the end of 2011 involving unauthorized disclosure of user information by a number of well-known Internet companies, including Dangdang, Jingdong and Alipay. The information disclosed included names, addresses, telephone numbers and email addresses of users. Certain information was even traded on the black market. MIIT officials strongly criticized the disclosures and required the Internet companies concerned to take remedial actions.

Beijing

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

Brussels

Joanna Łopatowska 32 2 340 7365
Karin Retzer 32 2 340 7364

Hong Kong

Eric Dickinson 852 2585 0812
Gordon A. Milner 852 2585 0808

London

Ann Bevitt 44 20 7920 4041
Deirdre Moynihan 44 20 7920 4164
Anthony Nagle 44 20 7920 4029

Los Angeles

Michael C. Cohen (213) 892-5404
David F. McDowell (213) 892-5383
Purvi G. Patel (213) 892-5296
Russell G. Weiss (213) 892-5640

New York

Madhavi T. Battiboi (212) 336-5181
John F. Delaney (212) 468-8040
Matthew R. Galeotti (212) 336-4044
Sherman W. Kahn (212) 468-8023
Mark P. Ladner (212) 468-8035
Michael B. Miller (212) 468-8009
Suhna N. Pierce (212) 336-4150
Marian A. Waldmann (212) 336-4230
Miriam H. Wugmeister (212) 506-7213

Northern Virginia

Daniel P. Westman (703) 760-7795

Palo Alto

Anna Ferrari (650) 813-5681
Christine E. Lyon (650) 813-5770
Bryan Wilson (650) 813-5603

San Francisco

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

Tokyo

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

Washington, D.C.

Nicholas A. Datlowe (202) 887-1590
Richard Fischer (202) 887-1566
D. Reed Freeman, Jr. (202) 887-6948
Julie O'Neill (202) 887-8764
Obrea O. Poindexter (202) 887-8741
Cynthia J. Rich (202) 778-1652
Kimberly Strawbridge Robinson (202) 887-1508
Robert A. Salerno (202) 887-6930
Andrew M. Smith (202) 887-1558
Nathan David Taylor (202) 778-1644

Client Alert.

Having completed a public consultation process, MIIT formally promulgated the *Several Regulations on Standardizing Market Order for Internet Information Services* (《规范互联网信息服务市场秩序若干规定》; “Internet Regulations”) on December 29, 2011.

The Internet Regulations cast a relatively broad net. They apply to Internet Information Service Providers (“IISPs”). This is a term drawn from regulations issued by the State Council in 2000 that simply refers to parties providing information to Internet users over the Internet. As such, not only Chinese Internet companies whose principal business is online (and whose operations require a license from MIIT) but also other Chinese companies whose online activities are more limited are required to comply with the Internet Regulations in their online operations. Morrison & Foerster has prepared an unofficial English translation, a copy of which can be requested by email to chinamarketingteam@mofocom.com. The Internet Regulations will take effect on March 15, 2012.

Highlights

- The Internet Regulations provide a definition of personal information, where privacy provisions in prior PRC legislation commonly do not define the term. Personal information is defined as information relating to a user that, alone or in conjunction with other information, is sufficient for a third party to identify the user.
- IISPs must obtain users’ prior consent when collecting users’ personal information or providing such information to others.
- IISPs must properly keep users’ personal information and take immediate remedial measures (the scope of which is not explained) in case of information leakage.
- IISPs may only collect users’ personal information as necessary to provide their services.
- IISPs must expressly inform users of the method, content and purpose of the collection and processing of their personal information and must not use their personal information beyond the stated purpose.
- IISPs breaching these requirements are subject to sanctions that include rectification orders, warnings and penalties ranging from RMB10,000 to RMB30,000.

The issue of online data privacy has been widely discussed in the media and in official circles in recent months. Promulgation of the Internet Regulations comes at a time of greater activism on the part of the public security authorities and other government agencies in dealing with cases of data theft. The MIIT has a record of relatively aggressive exercise of its jurisdiction over the Internet. For all of these reasons, it is expected that the privacy provisions of the Internet Regulations will be actively enforced. Companies in China will need to review their privacy policies to ensure compliance with the consent, confidentiality and non-use requirements of the Internet Regulations. The privacy provisions of the Internet Regulations are broadly drafted, leaving important compliance questions unanswered. It will also be important to monitor MIIT policy with respect to the implementation of such provisions.

RESIDENT IDENTITY CARDS LAW AMENDED

Every Chinese citizen 16 years of age and older who is resident in China must have a valid identity card. Identity card numbers and other information contained on identity cards represent important personal information that can be misused if obtained by unauthorized third parties. With unauthorized disclosure and sale of personal information having become a serious social problem, the Standing Committee of the National People’s Congress on October 29, 2011 promulgated an amendment to *the Law on Resident Identity Cards* (《中华人民共和国居民身份证法》; “Identity Card Law”) to heighten protection of information contained on identity cards.

Client Alert.

Highlights

- Information displayed on an identity card includes the holder's name, gender, ethnicity, date of birth, permanent domicile ("hukou"), ID number and photograph. Identity cards include a digital microchip that includes this same information in digital form. The amendment to the Identity Card Law implements a requirement that the individual's fingerprints be registered and recorded in digital format in the card.
- Entities that have access to personal information of citizens that is contained on identity cards, as well as employees of those entities, are subject to an express obligation under the amended Identity Card Law to keep that information confidential.
- Breaches of the confidentiality requirement under the law are subject to sanctions that include detention of 10 to 15 days and penalties ranging from RMB100,000 to RMB500,000 for breaches by entities and of RMB5,000 for breaches by individuals.

DEVELOPMENTS IN JIANGSU AND OTHER LOCALITIES

While efforts to enact an omnibus privacy law have foundered at the national level, some local governments, especially in localities seeking to develop outsourcing and other industries dependent on robust data-privacy protection, are moving ahead with legislative efforts.

An example is the *Jiangsu Province Informatization Measures* (《江苏省信息化条例》; "**Jiangsu Measures**"), which were passed on September 23, 2011 by the Standing Committee of the Jiangsu Provincial People's Congress and took effect on January 1, 2012.

Highlights

- Repetitive collection of the same personal information by different government agencies is prohibited.
- In order for parties other than government agencies to collect personal information, consent from the individual must be obtained, and the use that will be made of the information must be explained. Though requiring consent, Jiangsu Measures are unclear on the definition of personal information and the mechanism to obtain consents from individuals. Any future reported cases of enforcement will help to address such uncertainty.
- Unlawful disclosure of obtained information is prohibited. Entities and individuals breaching this prohibition are subject to penalties ranging from RMB100,000 to RMB500,000.

More local governments are expected to follow Jiangsu's lead in enacting local regulations to deal with protection of personal information. One example is the Shenzhen Government which, on December 27, 2011, indicated its intention to promulgate a local personal information protection regulation. A legislation research report, written by a group of senior members of the Shenzhen Bar Association, has been submitted to the Shenzhen Provincial People's Congress for review and discussion.

Some local governments have taken legislative initiatives to protect privacy in public areas. In the latter part of 2011, the Changsha Municipal and the Shanxi Provincial Governments both enacted local *Measures for the Administration of Public Surveillance Systems* (《公共安全图像信息系统管理办法》), which expressly forbids installation of surveillance cameras in places such as hotels, public bathrooms, dressing rooms and work areas in finance, insurance and securities companies. In issuing measures to regulate use of surveillance cameras, Changsha and Shanxi have followed the example of many other local governments—including the Beijing government which issued measures back in 2006.

Client Alert.

JUDICIAL DEVELOPMENTS

A few recent court decisions and guidance opinions should also be noted by China privacy watchers, including:

- On October 14, 2011, just prior to the amendments to the Identity Card Law having been promulgated, the local People's Court in the Longgang District of Shenzhen Municipality rendered a judgment in the first personal information breach case in Longgang District. The defendant in that case had obtained photocopies of the identity cards of 2,000 people either through illegal purchase or exchange on the Internet, and then sold the information. The defendant was found guilty of the crime of unlawfully accessing personal information of third parties and sentenced to a one-year prison term and a fine of RMB1,000, applying provisions of the PRC Criminal Law.
- The *Provisions on Several Issues regarding the Hearing of Administrative Cases Involving Public Government Information* (《最高人民法院关于审理政府信息公开行政案件若干问题的规定》) were issued by the Supreme People's Court and came into force on August 13, 2011; ("**Provisions**"). The Provisions stipulate that a citizen, legal person or organization can file an administrative lawsuit against the government if it considers that government publication of information infringes upon its individual privacy or trade secrets. Where the breach is proven, the court is required to render a judgment that the disclosure of such information is illegal and may order the government to take remedial measures.
- On August 5, 2011, the Beijing Second Intermediate People's Court issued a judgment in one of the biggest personal information breach cases to date in Beijing. The 23 defendants in the case, employees of a telecommunications company, illegally sold personal information such as personal phone numbers of the company's subscribers. The court found that the sale infringed the legitimate rights and interests of the subscribers and caused serious damages and imposed jail terms ranging from 6 to 30 months.

PRACTICAL IMPLICATIONS FOR ORGANIZATIONS OPERATING IN CHINA:

- Don't assume that you have no privacy obligations in China. Although there is no omnibus privacy legislation, bit by bit the protection of personal information is growing.
- Remember that there are provincial and local laws as well as national laws. For the time being; the focus on privacy is being taken up by the local and provincial governments. That patchwork of laws and regulations is expected to expand.
- While privacy is not viewed as a fundamental "human right" in China quite the same way as in some other jurisdictions, due to the highly publicized cases relating to the theft and misuse of personal information, individuals are becoming more aware of and concerned about protection of personal information.
- Consider implementing privacy best practices to put your organization in a strong position as the regulations continue to develop.

Contact:

Paul McKenzie
(86) 10-5909 3399
pmckenzie@mof.com

Jingxiao Fang
(86) 10-5909 3399
jfang@mof.com

Client Alert.

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 eight 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/> and "like" us on Facebook at <http://www.facebook.com/MoFoPrivacy>.

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. Prior results do not guarantee a similar outcome.