July 20, 2015

China Proposes Draft Privacy Legislation with Significant Potential Implications

By Paul McKenzie and Wei Zhang

On July 6, 2015, China's legislature, the National People's Congress (NPC), circulated for comment two pieces of draft legislation with significant potential implications for data privacy and data security in China. Comments can be posted via the NPC's website www.npc.gov.cn by August 5, 2015. The key provisions of these two draft laws are summarized below.

DRAFT CYBER SECURITY LAW

Coming closely on the heels of the July 1, 2015 promulgation of a new national security law, the draft Cyber Security Law (网络安全法) has as its stated goal the protection of "cyber sovereignty" and the preservation of cyber security. It includes provisions governing data localization, protection of personal information and other data, and network security.

- *Definition of personal information.* Many Chinese regulations that include provisions governing the protection of personal information are unclear on the scope of the term "personal information". The draft law includes a relatively detailed definition of "citizens' personal information", meaning personal information such as a citizen's name, birth date, ID number, biometric data, profession, residence, or telephone number, recorded electronically or through another method, as well as other kinds of information that, alone or combined with other information, may be used to determine a citizen's identity.

- *Data localization.* Article 31 of the draft law would require an operator of "key information infrastructure" to store personal information and other "significant data" collected and produced in the course of its business operations inside China. It would also require that, before any of that data can be shared with parties overseas or stored overseas, the Chinese company complete a security evaluation in order to evaluate the security risk associated with the data export. The term "key information infrastructure" refers to, among other things, public communications

UNITED STATES

California
Tiffany Cheung (415) 268-6848
Kimberly R. Gosling (858) 314-5478
Rebekah Kaufman (415) 268-6148
Christine E. Lyon (650) 813-5770
David F. McDowell (213) 892-5383
Purvi G. Patel (213) 892-5296
Andrew Serwin (858) 720-5134
Stephanie Sharron (650) 813-4018
William L. Stern (415) 268-7637
Nancy R. Thomas (213) 892-5561
David M. Walsh (213) 892-5262

New York
Cindy Abramson (212) 336-4178
Melissa Crespo (212) 336-4354
John F. Delaney (212) 468-8040
Michael B. Miller (212) 468-8009
Sotirios Petrovas (212) 336-4377
Suhna N. Pierce (212) 336-4150
Marian Waldmann Agarwal (212) 336-4230
Miriam H. Wugmeister (212) 506-7213

Washington, D.C.
L. Richard Fischer (202) 887-1566
Adam J. Fleisher (202) 887-8781
Libby J. Greismann (202) 778-1607
Julie O'Neill (202) 887-8764
Cynthia J. Rich (202) 778-1652
Nathan David Taylor (202) 778-1644

EUROPE

Berlin
Hanno Timner 49 30 72622-1346
Lokke Moerel 44 20 79204054

Brussels
Karin Retzer 32 2 340 7364
Alja Poler De Zwart 32 2 340 7360

London
Susan McLean 44 20 79204045
Alex van der Wolk 44 20 79204074

ASIA

Beijing
Paul D. McKenzie 86 10 5909 3366

Hong Kong
Gordon A. Milner 852 2585 0808

Singapore
Daniel P. Levison 65 6922 2041

Tokyo
Toshihiro So 81 3 3214 6568
Yukihiro Terazawa 81 3 3214 6585

infrastructure and information systems used by public utilities, government at the municipal or higher level; the military, or used in transportation systems, health care, or the financial sector. Notably the term also includes networks and systems owned or managed by network services providers that provide services to "large groups of users", potentially giving the data localization requirements of the draft law a very broad application. Frustratingly, the term "significant data" is not defined in the draft law. We anticipate the intention is to reinforce exisiting restrictions on the export of state secrets, as well as address other information whose export may have an impact on national security, but further guidance will be needed on this issue, as well as on the nature of the security evaluation required in connection with data exports.

- *Data protection*. Chapter 4 of the draft law includes broad provisions governing the protection of network data, including personal information. The term "network data" refers to all kinds of electronic data collected, stored, transmitted, processed, and produced through networks. The personal information protection provisions take a similar approach to personal information protection in sector-specific data privacy rules already in place with respect to the telecommunications sector. The provisions apply to all "network operators". "Network operator" and the term "network" are both defined broadly so that the obligations apply to the owner of any computer information network, as well as to any party who administers a computer information network or provides services over it. As such, the data protection provisions of the draft law apply broadly to a very wide range of parties who either own or use a computer information network (and effectively to all personal information in electronic form), and not only within the limited sectors covered by current rules. The principal requirements include the following:
    - Collection and use of personal information must comply with the principles of legality, legitimacy, and necessity.
    - The purpose, method, and scope of the collection and use of personal information must be expressly disclosed, and the collection and use of personal information must be based on the individual's consent.
    - Network operators may collect and use personal information only in connection with their provision of services and should not collect or use personal information outside the scope agreed by the individual.
    - Network operators should disclose to individuals their policies for the collection and use of personal information.
    - Individuals can demand that personal information collected unlawfully be deleted, and they have the right to demand correction of personal information that is inaccurate.
    - No entity or individual may steal or acquire personal information by other unlawful means, or sell or unlawfully provide personal information to others; language that corresponds to language in the Ninth Amendment to the Criminal Law is also discussed in this update.
- *Security certification/inspection*. Article 19 of the draft law would require that key network equipment and special-purpose network security products comply with applicable security standards and be subject to a security certification or security inspection before being sold in the market. The security certification/inspection requirement builds on a similar requirement contemplated in regard to equipment used in the telecommunications and Internet sectors in the *Guiding Opinions on Strengthening Network Security in the Telecommunications and*

Internet Sectors. Article 19 makes clear that its implementation is subject to the issuance of a catalogue of key network equipment and special-purpose network security products by the "State network information department", a reference to the Cyber Administration of China (CAC).

- *National security review*. Article 30 of the draft law contemplates a vague national security review requirement, requiring the operator of "key information infrastructure" procuring network products or services to undergo a security review process led by the CAC if the procurement "might have an effect on national security". This brief provision does not provide further details but states that the implementing measures for this process will be issued by the State Council. This requirement echoes the announcement made by the State Internet Information Office on May 22, 2014, which stated for the first time that all important technology products and services affecting national security or the public interest will be subject to a "cyber security" review. This provision of the draft law would establish the formal statutory basis for implementing such a national security review process for the procurement of IT equipment and services for important IT infrastructure.

It is difficult to predict how long it will take for the NPC's legislation process to be completed after the period for comments closes on August 5, 2015. The draft law is still subject to two readings before the full NPC or its Standing Committee, and we anticipate that a significant amount of debate within government circles has yet to take place on various aspects of the draft law before the law is formally promulgated. Some commentators are predicting that the draft law will be promulgated before the end of 2015.

In the meantime, various other regulatory efforts continue as part of the Chinese government's campaign to enhance network security, many of which are likely to have an adverse impact on market access by foreign IT companies.

DRAFT AMENDMENT TO CRIMINAL LAW

As we reported previously, the NPC's circulation for public comment Amendment 9 to the Criminal Law of the People's Republic of China (Draft) (中华人民共和国刑法修正案（九）（草案）), which contemplated a significant broadening of the scope of criminal liability under Article 253 of the Criminal Law for misuse of personal information.

The NPC has circulated a second draft of Amendment 9 (刑法修正案（九）（草案二次审议稿)), which while reworking the drafting of the data privacy provisions of the first draft, preserves the scope of criminal liability contemplated in the first draft while increasing related penalties. Now any breach of Article 253 is subject to a prison term of up to three years, with a longer prison term of between three and seven years if the circumstances are especially serious. Under the previous draft, the maximum penalty was three years (two for the new offense of unlawfully "selling or providing personal information to another party" introduced in the first draft).

It is likewise difficult to predict how long it will take for the NPC to complete its legislation process in respect of the Criminal Law amendment completed after the period for comments closes on August 5, 2015. The draft is still subject to one reading before the full NPC or its Standing Committee.

About Morrison & Foerster:

We are Morrison & Foerster — a global firm of exceptional credentials. 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 11 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 treatise setting out the U.S. and international legal landscape related to workplace privacy and data security, "*Global Employee Privacy and Data Security Law,*" or our free online Privacy Library, please visit our practice page and follow us on Twitter @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.