Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

VOLUME 15, NUMBER 8 >>> AUGUST 2015

China's Draft Network Security Law: Implications for Data Privacy and Security

By Eric Carlson and Sheng Huang, of Covington & Burling LLP, Beijing.

On July 6, 2015, China's National People's Congress ("NPC") released a draft of the Network Security Law ("Draft Law," referred to in some press articles as the draft Cybersecurity Law) for public comment. Comments could be submitted through the NPC website or by mail by August 5, 2015.

The release of the Draft Law follows closely on the heels of the new National Security Law that entered into effect on July 1, 2015 (*see report in this issue*).

The Draft Law, initially reviewed by the NPC in June 2015, would apply broadly to entities or individuals that construct, operate, maintain, and use networks within the territory of China, as well as those who are responsible for supervising and managing network security. A number of the provisions in the Draft Law, if enacted in their current form, are likely to significantly impact information and communications technology and other companies with business operations or interests in China.

The provisions that most merit the close attention of companies are those that relate to 1) the "secure" operations of networks and "critical information infrastructure," and 2) data protection.

This article focuses on those provisions that relate to data protection.

Provisions Affecting Data Privacy

The Draft Law would impose a series of obligations on network operators. Network operators are defined to include operators of basic telecommunications networks, Internet information service providers, and key information system operators.

Consistent with other existing laws and regulations, the Draft Law would reiterate the following obligations of network operators:

- protecting personal information, privacy, and trade secrets of users;
- notifying and obtaining the consent of users when collecting and using personal information;
- refraining from leaking, tampering with, stealing, or reselling personal information;
- setting up systems to handle complaints, reports, and requests to amend erroneous personal information;
- policing the network to prevent the dissemination of false or unlawful information; and
- maintaining records of relevant activities.

Violations could result in penalties, including warnings, rectification orders, fines or confiscation of illegal gains, suspension of the business, or revocation of the business license. Like many Chinese laws, the Draft

Law contains general, open-ended penalty provisions proposing that any violation of this law that causes damage to others should result in civil liability, and any violation of this law that constitutes a crime should result in criminal liability.

A number of the provisions in the Draft Law, if enacted in their current form, are likely to significantly impact information and communications technology and other companies with business operations or interests in China.

The obligations listed above are already set out in other laws and regulations in the field, such as the Decision on Strengthening Information Protection on Networks (*see WDPR, January 2013, page 24*), the Provisions on Protecting the Personal Information of Telecommunications and Internet Users (*see analysis by Eric Carlson and Scott Livingston, of Covington & Burling LLP, Beijing, at WDPR, April 2013, page 7*), and the Consumer Protection Law (*see analysis by Eric Carlson and Scott Livingston, of Covington & Burling LLP, Beijing, at WDPR, November 2013, page 11*).

The Draft Law would consolidate these obligations, but would leave many questions unanswered.

For example, the Draft Law would provide that "network products and services" that collect user information must notify users of such functions and obtain consent for collection. It would not, however, provide further clarity on what types of notifications and consents would be deemed sufficient. Also, the Draft Law does not mention how long a network operator must keep records of activities and how it can determine whether the information it has been provided is authentic.

New Privacy-Related Requirements Proposed

Although the majority of the proposed rules would reiterate provisions of existing laws and regulations, there are several new privacy-related rules proposed in the Draft Law:

Notification of Data Breach Must Be Sent to Users

The Draft Law would expressly require network operators, in addition to reporting to the relevant government authority, to notify users when there is an actual or possible data breach. Existing law explicitly requires network operators to report data breaches only to government authorities and take remedial action, though some governmental authorities do, in practice, require network operators to inform users through a government notice.

These proposed new rules reflect a recent trend of tightening rules regarding cross-border data transfers.

The new requirements of the Draft Law would require network operators to spend more resources and pay more attention than was previously the case in handling data breaches and the potential public relation crises and civil claims that may consequently arise.

Certain Data Must Be Stored in China, with International Transfers Subject to Security Assessments

Although certain laws and regulations expressly require certain types of personal information (such as personal health information and personal credit reference information) to be kept in China, the Draft Law would significantly expand the scope of personal information subject to such a data localization requirement. Specifically, personal data collected by operators of "critical information infrastructure" would have to be stored within Chinese territory.

The draft defines "critical information infrastructure" to include the following types of systems:

- basic networks for public communications and radio and television transmission services, and
- critical information systems for:
  - key industries such as energy, transportation, water conservancy, and finance;
  - public service sectors such as power, water and gas utilities, health care, social security, *etc.*;
  - military networks and government networks; and
  - networks and systems with a "very large" number of users.

If the operators of such systems must transfer personal information offshore for operational reasons, a "security assessment" would have to be conducted by national network administration authorities. It is unclear whether the personal data of foreign citizens collected in China would be covered by this obligation, and whether this provision would apply only prospectively to future collection of personal information, or if data already collected would also be affected. The procedures for the "security assessment" are unclear. Pursuant to the Draft Law, an implementing rule for "security assessment" is to be separately promulgated in the future.

These proposed new rules reflect a recent trend of tightening rules regarding cross-border data transfers. It would be more burdensome for multinational companies operating critical information infrastructure in China to transfer personal data internationally, whether intra-group or to third parties (such as data processing contractors).

   ISSN 1473-3579

Broader Definition of Personal Information

For the first time, the Draft Law would identify "personal biometric information" as a separate type of personal information. It would not, however, define "personal biometric information."

Currently, "personal biometric information" is generally understood to include fingerprint and genetic information, which have already been explicitly listed as personal information in several Chinese laws and regulations.

Comment

In China, high-level laws such as the Draft Law are drafted using broad language, with implementing rules subsequently issued by regulating government agencies filling the gaps.

To the extent possible, companies with an interest in these issues should carefully monitor the development and promulgation of such implementing rules and ensure that their interests are taken into consideration by regulating agencies.

The text of the draft Network Security Law is available, in Chinese, at http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm.

Eric Carlson is a Partner and Sheng Huang is an Associate at Covington & Burling LLP, Beijing. They may be contacted at ecarlson@cov.com and shuang@cov.com. ***The authors wish to acknowledge the contributions of Ashwin Kaja, of Covington & Burling LLP, Beijing, to this article.***