Client Update
China's Network Security Law Takes Effect

NEW YORK
Jeremy Feigelson
jfeigelson@debevoise.com

Jim Pastore
jjpastore@debevoise.com

HONG KONG
Mark Johnson
mdjohnson@debevoise.com

SHANGHAI
Philip Rohlik
prohlik@debevoise.com

WASHINGTON, D.C.
Jeffrey P. Cunard
jpcunard@debevoise.com

Luke Dembosky
ldembosky@debevoise.com

On June 1, 2017, China's new Network Security Law (the "Law") officially came into force. When the Law was first passed in November 2016, we noted that this first-ever law devoted solely to cybersecurity in China would impose substantial obligations on businesses operating in China. Most significant were obligations of the operators of "critical information infrastructures" ("CII Operators") to store data within Mainland China, conduct security assessments for cross-border data transfer, and purchase only network products or services which have been subject to a security review.[1] We also noted that the Law potentially would affect multinationals' IT infrastructure and their ability to transfer data abroad.

At that time, there was significant doubt about the vague and broad terms of the Law, and some hope that these might be clarified by additional implementing regulations.[2] While the Law is now in effect, there has been little clarification, and one of the significant implementing regulations will not go into effect for another 18 months.

Earlier this year, the Cyberspace Administration of China ("CAC")—China's top internet regulator—released two implementing regulations related to the Law for public consultation. One of them, the *Measures for Security Review of Network Products and Services (For Trial Implementation)* ("Security Review Measures"), offers guidance on security standards, and outlines a government-led security

[1] Under the Law, CII Operators are defined as "entities involved in a wide range of sectors including public communication and information services, energy, transportation, water conservancy, finance, utilities and e-government" as well as "other important sectors and fields" whose damage could harm "national security, people's livelihoods and public interest." See Network Security Law, Art. 31.

[2] "China Passes Network Security Law", Debevoise Client Update (Nov. 10, 2016), http://www.debevoise.com/insights/publications/2016/11/china-passes-network-security-law.

review process to be implemented for certain network products and services.[3] The other regulation, *the Measures on Security Assessment of Cross-Border Data Transfer of Personal Information and Important Data* ("Data Transfer Measures"), governs cross-border data flow and delineates a security assessment process on transfer of data abroad.[4] Both the Data Transfer and the Security Measures were slated to take effect on June 1st, although many businesses which routinely transfer data abroad found both to be lacking in clarity.

Last month, a coalition of dozens of global business groups called on China to delay implementing the Law and regulations, complaining that the Law would hamper market access and conflict with World Trade Organization regulations. Subsequently, the CAC decided to delay implementation of the Data Transfer Measures until December 31, 2018. The Security Review Measures, however, became effective on June 1st.

SECURITY REVIEW MEASURES

The stated purpose of the Security Review Measures is to implement Article 35 of the Law, which requires CII Operators to ensure that "network products and services" they purchase have passed a "security review."

The network security review requirement focuses on whether the products and services are "secure and controllable." A number of specified risks must be assessed during the review—for example, the risk of products or services being unlawfully controlled, interfered with or otherwise hacked.[5] The CAC has set up a Cybersecurity Review Commission (the "Commission") responsible for adopting relevant policies relating to security reviews. A Cybersecurity Review Office will be set up to handle the actual review.[6] In addition, the Commission will assemble expert panels to assess security risks.[7] Specific review methods will

---

[3] In February 2017, the first draft of the Security Review Measures was released for public comment. On May 2, 2017, the final version of the Measures was released, a copy of which in Chinese is available http://www.cac.gov.cn/2017-05/02/c_1120904567.htm.

[4] On April 11, 2017, the first draft of the Data Transfer Measures was released for public comment, a copy of which in Chinese is available at http://www.cac.gov.cn/2017-04/11/c_1120785691.htm. On May 19, 2017, the Cyberspace Administration of China ("CAC") invited international stakeholders to attend a seminar to discuss an updated version of the Data Transfer Measures. References here are made to this updated version of the Data Transfer Measures, although this version has not been official published yet.

[5] Security Review Measures, Art. 4.

[6] Security Review Measures, Art. 5.

[7] Security Review Measures, Art. 6.

include lab testing, on-site inspection, online monitoring, and background check.[8]

The Security Review Measures lay out general principles rather than specifying practical guidelines. For example, these Measures do not specify any timeframe for the review process, nor do they make it clear how the security risks will be assessed. Such lack of clarity provides substantial discretion to the regulators.

DRAFT DATA TRANSFER MEASURES

The Data Transfer Measures remain in the draft form issued on May 2, 2017. They are to be enforced from December 31, 2018. The Data Transfer Measures aim to clarify the data localization and transfer provisions under the Law. Article 37 of the Law provides that CII Operators must store "personal information and important data" collected and generated during operation within Mainland China, and cross-border data transfer will be subject to a "security assessment."

The Data Transfer Measures expand the scope of "security assessment" under the Law to cover not only CII Operators, but also general "Network Operators."[9] "Network Operators" are defined under the Law as "owners or managers of a network, or network service providers,"[10] terms so broad they could cover virtually every entity that uses networks to conduct business, regardless of the industrial sector. This means, for example, that a company merely operating a local area network to collect employee information may also need to conduct a security assessment for intra-company data transfer abroad.

Two types of data will be subject to the security assessment requirement: "personal information" and "important data." "Personal information" refers to information that can be used to identify a person's identity alone or in combination with other information, such as name, date of birth, identity document number, etc.[11] "Important data" does not mean data that are important to the corporation, but those "closely related to national security, economic development, and social and public interests".[12]

---

[8] Security Review Measures, Art. 3.

[9] Draft Data Transfer Rules, Art. 2.

[10] Network Security Law, Art. 76(3).

[11] Data Transfer Measures, Art.15; Network Security Law, Art. 76(5).

[12] Data Transfer Measures, Art. 15.

The Data Transfer Measures provides for two types of assessment processes: self-assessment and regulator assessment. In general, Network Operators are obliged to conduct security assessments for their cross-border data transfer.[13] However, an industry regulator will conduct the security assessment if the transfer contains a "huge" amount of personal information (defined as relating to over 500,000 Chinese citizens), or if the transfer involves data related to sensitive matters (*e.g.*, nuclear facilities, national defense, marine environment, etc.) or involves data related to cybersecurity information of CII Operators, or if the transfer involves other data that may potentially affect national security and public interests.[14] The Data Transfer Measures also lay out the substantive criteria applied to both self-assessment and regulator assessment, including the aspects to assess (for example, amount, scope, type, level of sensitivity of personal information involved), as well as the circumstances under which cross-border transfer will be prohibited (for example, the transfer poses risks to China's national security or public interests).[15]

Notably, the Data Transfer Measures offer strong protection on personal information. According to Article 4 of the Data Transfer Measures, to transfer personal information abroad, the data subject must be notified of "the purpose, scope, type and the country or region where the recipient is located," and consent to the transfer. The only exception to this requirement is when urgent circumstances occur under which the security of citizens' lives and properties are endangered. The Data Transfer Measures also emphasize that absent the data subject's consent, no cross-border transfer of personal information is allowed.[16] The lack of any stated exceptions to this rule, combined with the broad definition of "personal information," would appear to make any data transfer particularly burdensome. This breadth will hopefully be addressed before the Data Transfer Measures take effect in 18 months.

LOOKING FORWARD

Although the Law and the Security Review Measures have already taken effect, there is a lack of clarity as to how to comply with both documents. It is unclear as to when the Draft Data Transfer Measures will be officially adopted and whether they will be adopted in the current near final version. It is also unknown

[13] Data Transfer Measures, Art. 6.

[14] Data Transfer Measures, Art. 7.

[15] Data Transfer Measures, Arts. 8 and 9.

[16] Data Transfer Measures, Art. 9(2).

what the regulator's enforcement priorities will be or exactly how security reviews will be carried out, although businesses that operate in or supply critical industries should be more alert than others.

It is to be hoped that additional implementing regulations or guidelines will be issued in the near future. In the meantime, corporations subject to the Law can consider:

- Continuing to work with Chambers of Commerce and other business groups in China to encourage greater clarity;
- Evaluating whether they meet the definition of CII Operators, based on the business nature, the industries that they supply, and the nature and amount of data collected and processed during business operation;
- Reviewing current IT infrastructure deployments and data compliance programs, and assessing whether they could comply with the requirements on data localization, cross-border data transfer, and product or service security review;
- Consulting with legal professionals to identify improvements necessary to increase cyber compliance; and
- Planning ahead for potential interaction with regulators, and mapping out crisis management strategies.

* * *

Please do not hesitate to contact us with any questions.