On April 11, 2017, the Cyberspace Administration of the People’s Republic of China (CAC) released a draft of the *Measures for the Security Assessment of Personal Information and Important Data to be Transmitted Abroad* (Draft Measures) for public comment. The Draft Measures mark a step forward in the implementation of the security assessment system called for under the Cybersecurity Law, which was promulgated on November 7, 2016 and took effect on June 1, 2017.

**Overview and Definitions**

Article 2 of the Draft Measures provides that, “Personal Information and Important Data generated or collected by a Network Operator during its operation within the territory of the People’s Republic of China shall be stored domestically. If it is necessary to transmit data abroad due to commercial needs, a security assessment shall be conducted according to the requirements hereunder.”

**TAKEAWAYS**

- Cyberspace Administration is promulgating standards to implement elements under the new Cybersecurity Law.
- “Personal information” has a straightforward definition; “important data” does not.
- Foreign invested network operators may face difficult decisions about information they currently retain outside of China.
1. **Personal Information.** “Personal Information” is defined under the Draft Measures as all information, recorded in electronic form or otherwise, which can be used, solely or together with other information, to determine the identity of a natural person, including but not limited to the name, date of birth, ID card number, personal biometric information, and address and phone number of the nature person. This definition is consistent with that provided under the newly promulgated Cybersecurity Law. Under the *Information Security Technology—Guidelines for Personal Information Protection within Public and Commercial Information Systems* issued by the Ministry of Industry and Information Technology in January 2013, Personal Information may also include race, political opinion, religion, genetic information and fingerprints. (See *Protecting Personal Data in China: An Update* for detailed discussions of the definition of Personal Information and the protection measures adopted in some other national or local laws and regulations.)

2. **Important Data.** “Important Data” is defined under the Draft Measures as data closely related to national security, economic development, and social and public interests. Unlike the definition of Personal Information, “Important Data” is loosely defined under the Draft Measures and government authorities therefore have more discretion to include or exclude certain information from the definition on a case-by-case basis. The Cybersecurity Law does not adopt the concept of “Important Data”, but uses the concept of “Critical Information” and “Critical Information Infrastructure”, which cover information relating to public communication and information services, power, traffic, water, finance, public service, electronic governance and other critical information that, if destroyed, suffered a loss of function or was leaked to the public, might seriously endanger national security, the national welfare, the people’s livelihood or the public interest. Although the Cybersecurity Law uses a different defined term (Critical Information is translated from “关键信息”, while Important Data is translated from “重要数据”), it is reasonable to conclude that “Important Data” and “Critical Information” both target information closely related to national security and social welfare.

3. **Network Operator.** “Network Operator” is defined under the Draft Measures to include network owners, network managers and network service providers. The same definition is used in the Cybersecurity Law. Before the publication of the Cybersecurity Law, Chinese laws and regulations used the concept of “Internet Service Provider” or “ISPs” to refer to the party principally responsible for the protection of Personal Information. (See, for example, the *Administrative Measures on Internet Information Services* published by the State Council on September 25, 2000, the *Several Provisions on Regulating Market Orders of Internet Information Services* published by the Ministry of Industry and Information Technology on March 15, 2012, and the *Decision on Strengthening Online Information Protection* published by the Standing Committee of the National People’s Congress in December 2012.) The common understanding is that an “Internet Service Provider” is a party who actually operates websites, and does not include the owners of the websites. The use of the term “Network Operator” in the Draft Measures, and the expansion of the parties included in that term will tighten the government’s control over the dissemination of Personal Information via the Internet.

**Security Assessment upon Transmission of Personal Information outside China**

The Draft Measures expressly provide that Personal Information and Important Data generated or
collected within China must be stored in China. Although neither the Draft Measures nor the Cybersecurity Law provides a clear explanation, our understanding, which has been confirmed informally by competent government authorities, is that “People’s Republic of China” or “China” here only refers to mainland China and does not include Hong Kong, Taiwan or Macau.

If, due to commercial reasons, Personal Information or Important Data needs to be transmitted outside of China, a security assessment must be conducted with regard to any such transmission.

What is a “security assessment”?

In accordance with the Draft Measures, a “security assessment” is used to evaluate the potential risks to national security, social and public interests and personal legitimate interests arising from transmitting the data abroad. A security assessment must include the following aspects:

1. the necessity of the outbound transfer
2. the quantity, scope, type and sensitivity of the Personal Information and/or the Important Data to be transferred
3. the security measures taken by and the capabilities of the data recipient to protect the transferred data, as well as the cybersecurity environment of the nation where the data recipient is resident
4. the risk of leakage, damage or abuse of the data after the outbound transfer
5. possible risks to the national security, the public interest and individuals’ legal rights involved in the outbound data transfer and data aggregation.

Who must conduct the security assessment?

A security assessment must be conducted by Network Operators except in the following circumstances, where Network Operators are required to apply to the State Cyberspace Administration or its local counterparts to conduct the security assessment; in the latter case the authorities are required to respond within 60 business days:

1. outbound data transfers involving Personal Information of over 500,000 individuals
2. data size is over 1,000 GB
3. transfers involving data relating to nuclear facilities, chemistry and biology, national defense and the military, population health, megaprojects, the marine environment or sensitive geographic information
4. transfers involving data relating to information about the cybersecurity of Critical Information Infrastructure, such as system vulnerabilities and security protection
5. outbound transfers of Personal Information and Important Data conducted by an operator of Critical Information Infrastructure
6. outbound data transfers that may affect the national security or the public interest.

If, after performing a security assessment, either the Network Operators or the State Cyberspace Administration decides that the outbound transmission (a) was not approved by the owner of Personal Information, or may jeopardize personal interests, (b) might cause security risks to the nation’s politics, economy, technology and defense, or result in damage to national security and public interests, the Personal Information and/or Important Data may not be transmitted outside of China.

Our Observations

The Draft Measures are not clear as to whether “Network Operators” includes foreign invested Network Operators as well as domestic Network Operators in China. Our understanding, which has been informally confirmed with competent government authorities, is that “Network Operators” as defined under the Draft Measures does include foreign invested companies in China. This status will create a significant legal issue for most of the foreign invested companies in China that are providing Internet services via their offshore entities (e.g., their Hong Kong entities) and collecting Personal Information and/or Important Data via servers established outside of China. Because the Draft Measures expressly require that “Personal Information and Important Data generated or collected by a Network Operator during its operation within the territory of the People’s Republic of China shall be stored domestically,” foreign invested Network Operators (such as foreign invested e-commerce or online advertising companies) in China will have to make a hard decision as to whether to move their servers into China and hence be subject to more PRC laws and regulations that are applicable to situations where the servers are located in China (for example, whether a foreign invested company needs to apply for an ICP license is decided based on, among other things, whether the server used to provide Internet content services is located in China), or to uproot their operation in China and only provide Internet-related services from abroad.

Even if servers are located in China, and therefore all Personal Information and/or Important Data collected is stored within China, the data flow from foreign invested Network Operators or from the VIE entity of a foreign company to its offshore parent company could also be challenged, especially if the data involves Personal Information of more than 500,000 users in the aggregate, or exceeds 1,000 GB. The statutory language of “security assessment” is, not surprisingly, vague and therefore gives government authorities the discretion to reject any transfer of Personal Information and/or Important Data abroad on the basis of national security or the public interest.

The Draft Measures will also affect foreign invested companies in sectors other than the Internet industry, where collection of Personal Information and/or Important Data is an essential part of the business. For example, foreign invested companies in the education or early education industries normally require collection of Personal Information and transmission of that information to offshore parent companies for assessment and market promotion. Foreign invested companies in health care, wearable equipment,
insurance, to mention but a few, will also face the same or similar challenges.

The Draft Measures have not yet been formally promulgated, but we recommend our clients evaluate the Draft Measures and prepare for the impact they might bring. We will closely monitor developments and keep our clients updated.

For additional information on this topic and any other topics relating to investment in China, please contact any member of our China Practice Group.