JONES DAY | One Firm Worldwide℠

WHITE PAPER

May 2017

China's New Cybersecurity Law and Draft Data Localization Measures Expected to Burden Multinational Companies

China's new Cybersecurity Law ("new Law") is set to come into effect on June 1, 2017, and introduces sweeping provisions that may have a significant impact on companies doing business in and with China. To provide guidance on a controversial data localization requirement introduced in the new Law, the Cyberspace Administration of China released on April 11, 2017, draft Measures for Security Assessment of Outbound Transmission of Personal Information and Important Data ("draft Measures") for public comment. The draft Measures are sparking outcry from the international community but are expected to come into force on June 1, 2017, largely unamended. The deadline for submissions is May 11, 2017, just three weeks before the new Law takes effect.

This *White Paper* provides an overview of the new compliance obligations the new Law imposes and also takes a close look at the draft Measures giving guidance on the data localization requirements.

Companies should take careful note of this new privacy and cybersecurity landscape to ensure their business practices align with legal and regulatory requirements. The new Law and the draft Measures could substantially increase the costs for China-based companies that process China personal information and engage in cross-border transfers.

A BRIEF HISTORY OF CHINA'S CYBERSECURITY LAWS

Before the new Law, Chinese regulations governing cybersecurity were interspersed across a number of separate laws, including, for example, the Internet Information Services of 2011 and the Telecommunications Regulations of the People's Republic of China 2016. The new Law marks the first comprehensive law in China specifically regulating network security. After undergoing three rounds of public consultation before it was finally adopted on November 7, 2016, the new Law is designed to ensure network security and to protect the privacy and security of its citizens. The final version of the new Law has been widely criticized as containing a number of broadly defined terms and vague provisions that potentially—and significantly—affect a wide range of companies.

NEW OBLIGATIONS FOR NETWORK OPERATORS AND CRITICAL INFORMATION INFRASTRUCTURE OPERATORS

The new Law primarily imposes data security requirements on two key types of organizations—network operators and critical information infrastructure operators ("CII operators").

"Network operators" are broadly defined to include owners, managers, and "service providers" of networks—"systems comprised of computers and other information terminals and related equipment" that gather, store, transmit, exchange, and process information.[1] This definition not only covers telecommunication, wireless communication, and internet service providers but could ostensibly cover every organization or business that owns or operates IT networks in China. Chinese legal drafters and regulators favor the definition to have such a sweeping effect.

CII operators are a subset of network operators. While not explicitly defined, CII operators include any business operating in public communication and information services, energy, transportation, water resources, finance, public services, and electronic communications.[2] Other businesses may be considered CII operators as well if they have infrastructure that would lead to a serious threat to national security, social or economic well-being of the nation, or public interest if it were destroyed, lost functionality, or suffered in a data breach. No further guidance has been issued on what infrastructures the Chinese authorities consider would seriously endanger national security or the economy. What businesses fall under this rubric will likely be left to the government's discretion.[3]

Under the new Law, network operators will be required to comply, *inter alia*, with the following cybersecurity obligations:

- Implement internal security management systems and operating rules, including the requirement to adopt technical measures to prevent viruses and other intrusions; store network logs for at least six months; adopt measures such as data classification systems; and implement security measures such as backup systems and encryption. These data security procedures must be implemented according to China's "tiered system of network security protections";[4]
- Develop emergency response plans for network security incidents, and in the event of an incident, promptly implement remediation measures and report such incidents to the relevant authorities; and
- Provide technical support and assistance to public security agencies to preserve national security and investigate crimes.

CII operators have additional data security compliance requirements:

- Undertake additional security measures including conducting security background checks on responsible personnel in critical positions, carry out network security education and technical training, and implement disaster recovery backups;
- Undergo a national security review by the Chinese authorities when purchasing network products or services that might impact national security; and
- Conduct inspections of their network security on at least an annual basis.

Even if a business or organization is not considered a CII operator, the new Law encourages network operators to participate voluntarily in the CII infrastructure protection system.

In addition to these measures, other key provisions of the new Law are expected to have a significant impact on companies. They include the following.

Data Localization

Perhaps the most controversial provision of the new Law is Article 37, which requires CII operators to store within mainland China "citizens' personal information and important data" collected or generated in China. The term "important data" is not defined in the new Law, but Article 76 defines "personal information" broadly to refer to all kinds of information that, recorded electronically or through other means and taken alone or together with other information, is sufficient to identify a natural person's identity, including but not limited to an individual's name, date of birth, identification numbers, personal biometric information, addresses, telephone numbers, etc.

The new Law further provides that if such information must be transferred outside of China for "legitimate business reasons," CII operators must complete "security reviews" (an undefined term) jointly formulated by the State Council and the National Cyberspace Administration. Penalties for noncompliance include confiscation of income, payment of fines (by both the offending organizations as well as the responsible individuals) and suspension of business.

These new data localization requirements represent some of the strictest data localization requirements worldwide. As explained below in "Draft Measures Expand Data Localization and Cross-Border Transfer Requirements," China's Cyberspace Administration's April 11, 2017, draft Measures now have expanded the data localization requirement even more, applying this obligation to other network operators.

Handling of Personal Information

Akin to personal data laws in the European Union, the new Law imposes a host of data protection requirements on network operators, including abiding by the principles of legality, propriety, and necessity in their data handling and also making publicly available privacy notices that explicitly state the purposes, means, and scope for collecting and using information. Data subjects, furthermore, are afforded the right to access, modify, and delete their personal information.

Transfer of Personal Information

The new Law prohibits network operators from transferring personal information absent the consent of the data subject unless such information has been processed so that the specific individual is unidentifiable and cannot be recovered. Businesses have voiced concerns that such a legal requirement can be an insurmountable obstacle to the transferring of personal information as it is, in practice, difficult to obtain consent from all relevant individuals.

Identity Verification of Internet Users and Instant Messaging Service Users

The new Law expands the requirement of using only true identification to various internet users and users of instant messaging services by imposing on service providers the responsibility of verifying users' real identification prior to providing services.

Online Protection of Minors

The new Law aims to strengthen the principles for the protection of minors in cyberspace and to avoid exploitation. The principles set forth in the new Law make way for supplemental regulations on children's online privacy protection to follow.

Investigation and Punishments

Companies can expect increased regulatory oversight as the new Law provides regulatory authorities with more explicit and wider monitoring, investigative, and enforcement powers. As noted above, network operators are required to cooperate with such authorities. However, there is some concern that "cooperation" may require the companies to disclose their systems to the regulators, which may result in further security leakage. Failure to cooperate with the authorities would attract penalties against network operators as well as the responsible individuals. Some companies are considering ring fencing their security systems as far as possible to avoid risks to their security systems outside of China.

Penalties for Noncompliance

Companies also can expect increased penalties for noncompliance with the new Law. Violations of the new Law trigger a wide range of potential penalties for network operators and CII operators alike, including warnings, suspensions of operation, imprisonment, and fines up to RMB 1,000,000 (~US$150,000). Notably, Article 75 of the new Law imposes penalties (such as

the freezing of assets) against foreign organizations or individuals who attack or otherwise endanger China's CII.

DRAFT MEASURES EXPAND DATA LOCALIZATION AND CROSS-BORDER TRANSFER REQUIREMENTS

On April 11, 2017, the Cyberspace Administration of China released draft Measures to assist in the implementation of the new Law. The draft Measures remain open for comment until May 11, 2017, three weeks before the new Law is set to take effect.

The purpose of the draft Measures is to detail the restrictions on cross-border transfers, give guidance on security assessment for data transfers, and further clarify when data may not be exported outside China. If issued as written (which is expected), the draft Measures will not only expand the data localization requirement to an even broader range of companies than originally contemplated under the new Law, but also require all network operators to conduct their own security reviews prior to transferring personal information outside of China.

"Important Data" Defined

The draft Measures now define the term "important data" to mean data closely related to national security, economic development, and social and public interest. The draft Measures lack any further guidance or helpful examples to demonstrate what data would meet this criteria, other than to note that the scope will follow national standards and guidance. This nebulous definition suggests Chinese authorities will use the term at its discretion and on a case-by-case basis, leaving businesses with legal uncertainty as to when it will be applied.

Data Localizations Requirements Expand to Network Operators

As noted above, the new Law contemplated that only CII operators would be subject to China's new data localization requirement, originally giving comfort to some businesses that this obligation would be limited in its application and scope. The draft Measures, however, have taken a new turn, now requiring all network providers to store personal information and "important data" within China unless there is a genuine and legitimate business need to export the data overseas, in which case, network operators must conduct a security assessment. This wide net cast over who must comply with the data localization requirement has significant implications for entities doing business in China. If implemented as written, effectively any business that uses computer systems in China would be subject to the data localization requirement, a potentially costly undertaking.

When Security Assessments are Required

Network operators must conduct a security self-assessment before transferring personal information outside of China. The security assessment must take into account the following criteria:

- The necessity of the transfer;
- How personal information is involved, and whether consent of the data subject is obtained;
- How important data is involved;
- The protective measures implemented by the data recipient, the security of the data protection of the data recipient, and the environment of data protection in the destination country or region;
- The risks of data being leaked, destroyed, amended, or abused; and
- Risks relating to national security, societal and public interests, and the legitimate interest of an individual.

Where the transfers meet the following criteria, the draft Measures require network operators to entrust a government agency to conduct the security assessment and review:

- Transfers of personal information of over 500,000 citizens;
- Transfers that exceed 1,000 gigabytes;
- Transfers of data concerning fields such as nuclear facilities, chemical biology, national defense or military, public health, large-scale engineering projects, marine environments, and sensitive geographical information;
- Transfers of network security information concerning system vulnerabilities and security safeguards of CII operators;
- Transfers of data involving the provision of personal information or important data to overseas recipients by CII operators; and

- Other transfers that potentially affect national security and public interests, or transfers where the industry regulators or supervisory authorities require review.

These criteria represent a relatively low threshold for triggering government review, have become the immediate sources of complaints, and are expected to stymie daily business operations as the government assessments will take as many as 60 days to complete.[5]

Annual Assessments

In addition to undergoing security assessments, network operators transferring personal information also must conduct security reviews of their cross-border transfers at least annually and report the assessment to the respective industry regulatory or supervisory authority. Reassessments must occur even more frequently when: (i) the data recipient changes; (ii) there is significant change in the purpose, scope, volume, or type of data being transferred cross-border; or (iii) the data recipient or cross-border data transfer suffer a significant "security incident" (an undefined term).

"Prohibited Exports" Defined

Article 9 of the draft Measures sets out three circumstances under which data transfers are prohibited:

- Where the data subject has not consented or when it may infringe upon the interest of the data subject. Even where a data subject has consented, network operators are expected to expressly notify the data subject of the purpose, scope, content, and recipient and country where the recipient resides;
- Where the cross-border transfer poses security risks to the national political system, economy, science and technology, or national defense, or the societal or public interest could be jeopardized; and
- In other circumstances where the Chinese government deems necessary.

These conditions are generally discretionary in nature and leave uncertainty as to whether—and to what extent—they will be applied consistently.

POTENTIAL IMPLICATIONS

Multinational companies across all industries and sectors need to closely review their data security systems and privacy policies for possibly significant changes before the new Law comes into effect on June 1, 2017. Special care must be taken to meet the new data localization requirements that the draft Measures expand. This means, for example, establishing network systems to isolate and store China personal information locally, which could potentially be a costly endeavor. Companies also should begin considering whether it can make a legitimate business case for cross-border data transfers using the draft Measures' criteria.

Still, further guidance from the Chinese government is needed for companies to parse through the new Law's fairly vague language to avoid ambiguity and uncertainty as to how the new Law—and its corresponding draft Measures—will be interpreted. Both the new Law and the draft Measures leave much to be legally resolved.

Companies potentially affected by the draft Measures may consider contacting their respective trade unions or government officials to offer comment prior to the May 11, 2017, deadline.

LAWYER CONTACTS

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com/contactus/.

Chiang Ling Li
Hong Kong
+852.3189.7338
chianglingli@jonesday.com

Haifeng Huang
Hong Kong/Beijing
+852.3189.7253/+86.10.5866.1216
hfhuang@jonesday.com

Todd S. McClelland
Atlanta
+1.404.581.8326
tmcclelland@jonesday.com

Mauricio F. Paez
New York
+1.212.326.7889
mfpaez@jonesday.com

Undine von Diemar
Munich
+49.89.20.60.42.200
uvondiemar@jonesday.com

Jörg Hladjk
Brussels
+32.2.645.15.30
jhladjk@jonesday.com

Jennifer C. Everett
Washington
+1.202.879.5494
jeverett@jonesday.com

ENDNOTES

1 *See* Art. 76(1), (3) of the new Law.
2 *See* Art. 31 of the new Law.
3 Article 48 of the new Law also places an obligation on "electronic information distribution service providers" and "application software download service providers"—both undefined terms—to "perform security management duties." Further guidance from the Chinese authorities is required to understand who is subject to this provision and what specific practical responsibilities must be undertaken to comply.
4 *See* Art. 21(1)-(4) of the new Law.
5 *See* Art. 10 of the draft Measures.