The New Cybersecurity Law—New Compliance Focus for Enterprises in China

By David A. Livdahl, Jenny (Jia) Sheng, Amy Y. Liu and Wenjun Cai

*On November 7, 2016, the Standing Committee of the National People's Congress (**NPC**) of the People's Republic of China (**PRC**) passed the final Cybersecurity Law (**CSL**) after three rounds of review by the NPC since June 2015. China's first law addressing the cybersecurity issue, the CSL's promulgation marks China's increasingly stricter administration and supervision of cyber space, and is a milestone for China's cybersecurity legislation. The CSL will come into effect on June 1, 2017. Given the potential impact of the law, we suggest clients review it closely, especially when transmitting affected data out of the PRC.*

With the wide use of information technology in both the private and public sectors, cybersecurity is now considered an important part of the national security by the PRC government. With the highest number of internet users in the world and the booming internet economy, the PRC is also facing increasing cybersecurity challenges and risks. Moreover, data privacy has become a prominent issue, especially for PRC individuals. Reflecting the need for increased cybersecurity in China, the CSL incorporates previous practices of the PRC government in regulating cyber space, and also introduces certain new requirements.

Key Points

All business operators in and outside the PRC should pay attention to the following key points concerning the CSL and its implementation by the authorities for national security and public interest reasons:

- Identify sensitive Information that may trigger application of the CSL (e.g., classified secrets in the PRC National Secrets Protection Law and regulations, information in relation to military-related transactions and/or interests of the PRC or State-owned/controlled industries and infrastructure utilities, personal financial and health data, etc.).

- Pay attention to the sources of the information and use caution in distributing sensitive information, especially when transmitting such information outside of the PRC.

- CSL and the enforcement authorities will crack down on online, abuses including "unhealthy" live programs and online disagreements which could cause disorder of markets and harm the public interest and moral values. The CSL also defines network operators as those who own or manage networks, or provide network services. These two definitions are broad and will include a wide range of targets.

- The CSL will investigate all business operators that own, operate, build and/or maintain network and computer systems. Also, all other business operators that use computer systems and networks for business operations and management should also comply with the requirements under this CSL with regard to data privacy protection in the PRC. (E.g., the CSL applies to a wide range of network operators, including network owners and suppliers of network products/services.) The CSL also has a "catch all" definition for the term networks which is broad enough to target a wide range of businesses.

Application of the Law

The CSL applies to the creation, operation, maintenance and use of networks by network operators within the territory of the PRC. Obligations under the CSL are structured on the basis of its broad definition of "networks" ("systems composed of computers or other terminals together with relevant devices to collect, store, transmit, exchange or process information following predefined rules and procedures") and "network operators" (who own or manage networks, or provide network services).

Governing Authorities

The CSL mainly designates the Cyber Administration of China (**CAC**, an authority which is not widely known to the public) together with the Ministry of Industry and Information Technology (**MIIT**) and the Ministry of Public Security (**MPS**) to be responsible for supervising and administering cybersecurity-related work.

Obligations of Business Operators

Network operators should (i) formulate internal security protocols and working guidelines, (ii) have designated personnel in charge of cybersecurity issues; (iii) adopt technical measures to prevent virus, cyber-attacks and network intrusion, etc., track security events and keep records for at least six months; (iv) implement data classification, provide backup for important data and encryption; (v) prepare cybersecurity accident contingency plans; and (vi) assist governmental authorities in any national security or crime investigations if needed.

In addition to networks operators, the CSL also requires that suppliers of network products and services provide non-malicious programs to users, obtain consent from users for gathering and transferring user information, and inform users and take remedial measures in case of security risks. However, the CSL does not provide a clear definition for "network products and services." According to our communications with the local counterpart of MIIT in Shanghai, the official we consulted explained that the term "network products and services" refers to those products and services related to the maintenance and operation of a network, such as computer consumables, server maintenance services, etc.

When network operators provide services concerning internet access, domain name registration, fixed-line telephone and mobile phone access, if the user does not provide its actual identity, network operators cannot provide services to such users.

Critical Information Infrastructure

The CSL, for the first time, has introduced the Critical Information Infrastructure (**CII**) concept. CII includes public communications and information services, energy, transportation, water resources utilization, finance, public service and e-government affairs, etc., which could seriously jeopardize national security and the public interest should such infrastructures malfunction, or be subject to damage or data leakages. CSL requires stricter data protection measures to be taken by CII operators, namely:

- **Data Storage within PRC.** CII operators should store, within the territory of the PRC, personal information and critical data which they've collected and produced during their operations in the PRC.
- **Security Assessment when Transferring Data outside PRC.** If a CII operator has to transmit any personal information or critical data to outside the PRC, it must pass a security assessment based on detailed measures to be published by the government.
- **National Security Review for Certain Procurement.** When a CII operator procures network products or services which may affect national security, it must pass the national security review organized by the government.
- **Annual Network Safety Assessment.** CII operators must conduct a network safety assessment at least once a year, either by themselves or by network security service agents.

The governmental bodies in charge of the cybersecurity issues (such as CAC, MIIT, etc.) are drafting detailed rules for the future implementation of the CSL after it becomes effective on June 1, 2017. Such rules may include further details on the definition of CII operators.

Personal Data Protection

The CSL specifically addresses personal data protection. Before collecting any personal data, network operators and suppliers of networks products and services must inform the relevant individuals of the purpose, method and scope of the data collection and obtain their consent. A network provider and supplier of network products and services must also obtain the relevant individual's prior consent if it wants to transfer his/her personal data to any other party, unless the personal data is irreversibly depersonalized so that no particular individual could be identified based on such information. Moreover, network operators have the obligation to keep any collected personal data safe and sound and they must take remedial measures in the event of leakage, damage or losses of such collected personal data.

Any individual is entitled to request network operators to delete his/her personal data if such data is collected or used in an illegitimate manner, or to correct any inaccurate personal data.

Our Observations

The CSL outlines high-level principles and the legal framework for cybersecurity, but detailed rules and regulations will be needed to facilitate its implementation. Hopefully such detailed rules will clarify a number of key ambiguities, such as the roles and respective responsibilities of CAC, MIIT and other governmental authorities in the cybersecurity field, the factors and methods to determine whether a network operator is a CII operator, etc.

Network operators and network products/service providers under the CSL cover a wide range of entities. We recommend clients review the CSL and prepare cybersecurity-related measures to comply with the CSL, particularly in terms of personal data collection or transmission. For example, if a foreign invested

enterprise (**FIE)** collects personal data regarding its employees and transfers such information to its offshore headquarters, it has to obtain the employees' prior consent based on the CSL. Moreover, if the FIE is a CII operator, before transmitting any personal information or critical data to outside the PRC, it must pass a security assessment based on detailed measures to be published by the government.

We will follow the status of the CSL implementation and keep you posted of any development.

If you have any questions about the content of this Alert, please contact the Pillsbury attorney with whom you regularly work, or the authors below.

David A. Livdahl (bio)
Beijing
+86.10.8572.1122
david.livdahl@pillsburylaw.com

Jenny (Jia) Sheng (bio)
Beijing
+86.10.8572.1166
jenny.sheng@pillsburylaw.com

Amy Y. Liu (bio)
Beijing
+86.10.8572.1121
amy.liu@pillsburylaw.com

Wenjun Cai (bio)
Beijing
+86.10.8572.1188
wenjun.cai@pillsburylaw.com