Client Alert

pillsbury

Global Security Services

Privacy, Data Security & Information Use | Cybersecurity Task Force

China | Corporate & Securities

August 17, 2015

China's Draft Cybersecurity Law – A New Regime for Network Security

By David A. Livdahl, Jenny (Jia) Sheng and Chunbin Xu

China's current leadership has attached significant attention to network security, which is deemed to be a core aspect of national security. In early 2014, China's President, Xi Jinping, who is also the head of the Office for the Central Leading Group for Cyberspace Affairs, stated that "network security and informatization are key strategic issues related to national security and development," and "No cyber safety means no national security." On July 1, 2015, the National Security Law of the People's Republic of China (《中华人民共和国国家安全法》) *came into effect. Immediately after the National Security Law became effective, on July 6, 2015, a draft Network Security Law (Draft Cybersecurity Law) was released by the standing committee of China's National People's Congress (**NPC**) for public comments.*

The last 10 years have seen the rapid spread of the Internet and information technology in China. While it has benefited economic and social development, the PRC leadership also believes the wide use of network and information technology has caused security risks such as cyber-attacks, illegal activities using personal data and intellectual property, and even terrorism, etc. The focus on network security by China's government appears to have increased since Edward Snowden's disclosures in 2013 regarding activities of the U.S. National Security Agency. Since then, the Chinese government has been working actively to protect government networks and financial systems. The Draft Cybersecurity Law is the government's latest effort to consolidate existing security-related requirements and grant government agencies more security-protection and monitoring powers. Apart from the Draft Cybersecurity Law, a number of laws and regulations including the National Security Law and the Anti-Espionage Act have been released by the NPC and others, such as the draft Anti-terrorism Law, have been submitted to the NPC for review.

The Draft Cybersecurity Law is designed to govern activities that take place via "computer networks," defined broadly in Article 65(1) to cover essentially any "network or system, composed of computers or other terminals together with relevant devices, that serves to collect, store, transmit, exchange, or process

information following predefined rules and procedures." The Draft Cybersecurity Law provides more details on, among others, security requirements for network-related products and services; data privacy; and monitoring and emergency response systems. The Draft Cybersecurity Law intends to develop legal requirements (e.g., obligations of network users to provide real identities and obligations of network operators to protect personal information of users), and implement high-priority mandates such as provisions on the protection of critical information infrastructure (CII).

This alert focuses on some major requirements and mechanisms introduced by the Draft Cybersecurity Law.

Network Operators' Obligations

Network operators who own and manage networks and provide network service (Network Operators, or 网络经营者) must ensure continuous network security protection for its network. Measures to be taken by Network Operators to ensure network security include formulation of internal security protocols, adoption of technical measures to defend against cyber-attacks and tracking security events, and implementation of data classification, backup of important data and encryption. Moreover, the Draft Cybersecurity Law requires that suppliers of network products and services provide non-malicious programs to users, obtain consent from users for gathering user information, and inform users and take remedial measures in case of security risks. In case of providing services concerning Internet access, domain name registration, fixed-line telephone and mobile phone, if the user does not provide genuine identity information, the Network Operators cannot provide such services to the user.

Protection of Data Privacy

In addition to the general obligations of the Network Operators provided under Section 1 of Chapter 3, the Draft Cybersecurity Law also imposes obligations on the Network Operators to protect data privacy of network users, including but not limited to the following:

- Obtain consent from the user in collecting and using personal data
- Refrain from leaking, tampering, damaging, stealing or selling personal data
- Establish technical measures and other necessary measures to ensure security of personal data and take remedial measures in case of leakage, damage or loss of personal data
- Keep confidential all personal data and privacy and trade secrets obtained in the course of business
- Establish complaint and reporting platform to handle claims regarding violation of network security regulations

Critical Information Infrastructure (关键信息基础设施)

The Draft Cybersecurity Law, for the first time, introduces the concept of Critical Information Infrastructures (CII), which is defined broadly by the draft to include networks and systems in sensitive areas, i.e., (1) fundamental information systems providing services such as public communication and television transmission; (2) important information systems for key industries (such as energy, transport, water resource and finance) and public service sectors (such as electronic power supply, water supply, natural

gas supply, medical care and social security); (3) military network; (4) government affair networks; and (5) networks and systems owned or managed by the network service providers with large number of users. The draft does not explain what would constitute a "large number," but one could imagine it will be interpreted broadly to cover, for example, popular websites run by online service providers.

The Draft Cybersecurity Law requires operators of CII to sign security and confidentiality agreements with any suppliers providing network products and services to such operators. If the network products and services purchased by the CII operators may affect national security, such products and services are required to undergo a security review by the national network security administration authorities. However, the Draft Cybersecurity Law is unclear about how to determine whether a network product and service affects national security and what are the procedures for security review.

Operators of CII must store "important data" such as users' personal information collected and generated during operations within the PRC. If they seek to store or transfer such data overseas for business reasons, it must apply to undergo a new government security assessment process. This will impose additional burdens on operators of CII which may need to transfer data internationally.

Regulatory Authorities

The Draft Cybersecurity Law provides that the State Internet Information Office (SIIO) is responsible for coordinating network security monitoring and administration, with the Ministry of Industry and Information Technology (MIIT), Ministry of Public Security (MPS) and other relevant ministries of the State Council performing their administrative duties within their respective authority. Ministries in charge of telecommunications, radio and television, energy, transportation, water resources, finance and other relevant industries (Relevant Authorities) must work with SIIO to supervise network security in their respective industries by formulating network security planning for key industries and important areas.

Monitoring, Early-Warning and Emergency Response Mechanism

The Draft Cybersecurity Law establishes a multilevel monitoring, early-warning and emergency response mechanism to prevent, respond to and deal with different levels of network security incidents. The SIIO and Relevant Ministries will formulate emergency plans within their respective mandates. Governments above county level (县级以上人民政府) are authorized to adopt necessary measures if any network security incident occurs or is likely to occur, including but not limited to organizing assessment of network security incidents, disclosing information and assessment results that are relevant to the general public, etc.

Legal Liabilities

The Draft Cybersecurity Law provides in Chapter 6 various penalties for non-compliance with their obligations under the Draft Cybersecurity Law by Network Operators, operators of CII, suppliers of network products and services and other entities and individuals. The penalties include warnings, rectification orders, fines, confiscation of illegal income, suspension of business, shut-down of website, revocation of business license and/or permit. The Draft Cybersecurity Law also includes two general provisions stipulating that any violation of the Draft Cybersecurity Law that causes damage to others could bear civil liability, and any violation of the Draft Cybersecurity Law that constitutes a crime could be subject to criminal liability.

* * *

The Draft Cybersecurity Law evidences the Chinese government's ongoing effort to strengthen the supervision of Internet and telecommunication networks. The new requirements on the data privacy and requirements for operators of CII will have significant operational and commercial impact on domestic and foreign network operators, as well as network products and services providers. These requirements may also affect entities engaged in in the energy, broadcasting, financial services, transportation, medical/healthcare and other public services industries.

The Draft Cybersecurity Law is expected to be released and come into effect by the end of this year. Once adopted, the Draft Cybersecurity Law will almost certainly have significant influence on all sectors of business in China. We will follow the legislative process of this law closely.

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

Chunbin Xu (bio)
Beijing
+86.10.8572.1126
chunbin.xu@pillsburylaw.com

About Pillsbury Winthrop Shaw Pittman LLP
Pillsbury is a full-service law firm with an industry focus on energy & natural resources, financial services including financial institutions, real estate & construction, and technology. Based in the world's major financial, technology and energy centers, Pillsbury counsels clients on global business, regulatory and litigation matters. We work in multidisciplinary teams that allow us to understand our clients' objectives, anticipate trends, and bring a 360-degree perspective to complex business and legal issues—helping clients to take greater advantage of new opportunities, meet and exceed their objectives, and better mitigate risk. This collaborative work style helps produce the results our clients seek.