HAN KUN LAW OFFICES

Legal Commentary

CHINA PRACTICE • GLOBAL VISION

July 26, 2016

Analysis of the Second Review Draft of the Network Security Law

David TANG | Effy SUN

In the Internet age, cybersecurity concerns have become an increasing focus of legislative and regulatory efforts globally. In consideration of the practice of the construction, operation, maintenance and use of networks as well as the supervision and management of cybersecurity, the Standing Committee of the National People's Congress further amended and issued the second review draft of the *Network Security Law of the People's Republic of China* (the "**Second Draft**") on July 5 of this year to solicit public comment, after the issuance of the first review draft of the *Network Security Law* of the *People's Republic of China* (the "**First Draft**") on July 6, 2015, with a view to formally issue a specialized cybersecurity law as soon as possible to regulate network information protection and address cybersecurity concerns.

Legislative Status of Cybersecurity in China

While no specialized cybersecurity law is currently in force in the People's Republic of China ("**China**"), and the cybersecurity related provisions are mainly about personal information protection provided in a number of interrelated laws and regulations, including: the *Provisions on Protection of Personal Information of Telecommunications and Internet Users*, the *Decision of the Standing Committee of the National People's Congress on Strengthening Network Information Protection,* the *Administrative Measures for Online Trading,* the *Law of the People's Republic of China on the Protection of Consumer Rights and Interests*, *Several Provisions on Regulating the Market Order of Internet Information Services* and so on. Collectively, these laws and regulations require companies that collect or use personal information, particularly with an online component, to protect such information and provide for certain safeguards to ensure information security and prevent information from being compromised or lost. When any information is or may have been compromised or lost, the parties responsible must promptly undertake remedial measures.

In order to adapt to the development of the internet economy and global cybersecurity trends, the Standing Committee of the National People's Congress issued the First Draft on July 6, 2015,

and then issued the Second Draft on July 5, 2016, which is expected to be formally issued at the end of this year or at the beginning of the next year, after soliciting public comment.

Main Content and Amendments of the Second Draft

The Second Draft applies to the construction, operation, maintenance and use of networks, and cybersecurity supervision and administration within the territory of China, which basically extends the framework and content of the First Draft, and mainly includes: safeguarding national network sovereignty and strategic planning, protecting the security of network products and services, guaranteeing network operation security, guaranteeing network data security, protecting network information security, monitoring, early warning and emergency measures, and cybersecurity supervision, management and legal liability.

Based on the First Draft, the Second Draft is amended as the following:

a. Raising the Protection and Support of Cybersecurity to the National Level

Cybersecurity protection has been raised to the national level in the Second Draft. For example, the newly added Article 5 requires the State to take measures to monitor, defend, handle cybersecurity risks and threats inside or outside the territory of China, protect key information infrastructure from attack, intrusion, interference and damage, punish network related crimes in accordance with the law and protect the security and order of cyberspace.

Meanwhile, Articles 15, 16 and 17 of the Second Draft further stipulate that the State shall support and promote the development of cybersecurity, and that governments at all levels shall promote safe and reliable network products and services. The State shall promote the creation of a social service system for cybersecurity, and encourage enterprises and institutions to carry out network security certification, inspection and risk assessment and other security services. Additionally, the State shall encourage the development of network data security protection and usage technology, promote the opening of public resources, accelerate technological innovation as well as economic and social development, and support cybersecurity management innovation, and take advantage of advanced network technology to enhance the level of cybersecurity protection.

The State will encourage and support both cybersecurity protection and the development of network products, services and technologies, and will pay equal attention to security and the development of informatization.

b. Further Regulating the Activities of Network Operators

Network operators, which are seen as the source of network security, have been burdened with additional responsibilities under the Second Draft. According to additional rules in general provision of the Second Draft, aside from complying with the laws and regulations, network

operators shall also comply with social and business morals, be honest and trustworthy, perform cybersecurity protection obligations, accept supervision from the government and the public, and undertake social responsibility when conducting business and service activities.

Network operators are notably required to preserve web logs for no less than six months according to Article 20 of the Second Draft. In order to protect network order and regulate network operators' activities, Article 25 of the Second Draft provides that network operators or other institutions and individuals shall abide by national provisions when carrying out network security certification, inspection, risk assessment activities, and releasing information regarding system bugs, computer viruses, network intrusions, network attacks and other security risks.

Network operators are suppliers of network products and services, and the persons directly responsible for network security operations, network data security and network information security. The Second draft provides heightened requirements for network operators by introducing moral and social responsibility, and further regulates the operation and service of network operators, which will protect the order of networks and promote the network security protection and technology development. Moreover, the provisions regarding network security certification and risk assessment activities will strengthen the network users' trust of the network security system and promote the healthy development of the network security system. However, the detailed provisions about releasing system bugs, computer viruses, network intrusions, network attacks and other security risk information are awaiting further details and confirmation.

c. **Strengthening the Protection of Key Information Infrastructure and Data**

According to cybersecurity-related laws and regulations, the protection of "key information infrastructure" includes protecting key information infrastructure security operations and related data and information security, which are essential to national security, the security of economic sector operations and the security of citizens' personal information.

The First Draft provided that the scope of "key information infrastructure" was to include basic information networks that provide public communications, radio, television broadcasting and other services, important information systems for critical industries, including energy, water conservation, transportation, finance and public services, and military networks, governmental networks, and networks and systems with numerous users. However, Article 29 of the Second Draft removes these examples and instead authorizes the State Council to enact administrative regulations in order to determine the scope and the measures for the security and protection of key information infrastructure.

Regarding "key information infrastructure" data and information protection, the First Draft requires key information infrastructure operators to store personal information and other important data collected and produced during operations within the territory of China, while

Article 35 of the Second Draft adds important business data into the scope of “important data”. Additionally, Article 38 of the Second Draft requires the Cybersecurity Administration and related authorities to collect information when protecting key information infrastructure, which can only be used for cybersecurity protection in order to prevent the authorities from abusing their power and threatening information security.

Clearly, the deletion of the “key information infrastructure” scope language in the Second Draft, and authorizing administrative regulations to define this concept increases the flexibility of “key information infrastructure” as the basis for infrastructure and data protection. This revision will allow for easier adjustments in the future according to changing network technology and the environment to better protect key information infrastructure. There is no doubt that the State Council will formulate supporting documents to define the scope of "key information infrastructure", and we believe that this should occur when or directly after the Network Security Law is officially promulgated as not doing so would lead to operational issues when implementing the new law.

In addition, while the specific mechanisms are as of yet unclear, the Second Draft indicates that network operators are to voluntarily participate in key information infrastructure protection to strengthen cybersecurity information sharing among network operators, professional institutions and relevant government departments and, at the same time, strengthen the protection of such information.

d. Increasing the Scope of Real Identity Authentication

Article 23 of the Second Draft additionally requires users to provide real identity information when network operators provide instant messaging services, besides providing network access and domain name registration services, network access formalities for fixed-line or mobile phones, and information publication services. The Second Draft also requests the State to implement reliable identification strategies, support the research and development of secure and convenient electronic identity authentication technologies, and to promote mutual recognition and common use among different electronic identity authentication technologies. It increases the scope of network information traceability to force network users comply with cybersecurity related laws and regulations, and to promote related technology to facilitate identity authentication, accelerate the popularization of identity authentication, and establish a strategic system for network trusted identification.

e. Connecting with the Internet Age of Big Data

Article 41 of the Second Draft requires network operators not to divulge, distort or damage personal information without consent of the person whose personal information has been collected. Such personal information shall not be provided to others unless the information has been processed so that the identity of specific individuals cannot be determined. Such

provisions provide a legal basis and grounds for big data technology's collection and use of non-sensitive information. Meanwhile, the State will encourage the development of security protection and usage technology, support the openness of public resources and network technology innovation, cybersecurity certification and risk assessment regulations, and other measures mentioned above are also to support the development and practice of cloud computing and big data.

f. Enhanced Penalties for Activities Jeopardizing Cybersecurity

Article 54 of the Second Draft adds an interview requirement with the legal representative or responsible person of network operators that present cybersecurity risks. Article 61 of the Second Draft prevents violators of the law from engaging in related businesses. People who conduct activities jeopardizing cybersecurity on purpose and are imposed with public security administrative punishment or criminal punishment shall not engage in cybersecurity management and key network operation positions for the rest of their lives. In addition, there are punishments such as remediation orders, warnings, suspension of relevant businesses, suspensions pending rectification, website closures, business permission and business license revocations, and administrative fines, Article 68 of the Second Draft requires record disclosures of related violations of the Network Security Law.

The Second Draft makes clear that it is intended to decrease illegal and criminal activities by enhancing the penalties for activities that jeopardize cybersecurity, and to prevent risks and eliminate hidden dangers to the greatest extent.

Conclusion and Advice

In comparison to the First Draft, we consider the Second Draft to have been issued on the basis of practical experience with network information protection and network technology development, which is to mutually support and promote the development of the internet economy advocated by the State. The Network Security Law will help to decrease the current complexity of cybersecurity-related supervision and legislation. Without question, further discussion and debate, and the introduction and implementation of related supporting documents are needed for formal issuance and effective enforcement of the Network Security Law. We will continue to monitor updates of the Network Security Law as they become available.

Before the *Network Security Law* is officially promulgated, the currently effective cybersecurity-related laws and regulations focus on the protection of personal information. We would thus suggest that businesses take reasonable precautions when handling any form of personal information or acting as a manager of personal information for others, including: establishing sufficient technical measures and internal protocols to maintain information security and to prevent hacking or illegal access, either internally or externally; providing clear disclosures to the providers of information and receive consent (written or electronic) with respect to the

collection, use, or transfer of personal user information, and such consents should be drafted with great care so as to allow for flexibility to the extent permissible under the law. Other important legal requirements include restricting the collection, use, and transfer of personal information to that which is within the scope of consent and necessary for business purposes, not transferring without due authorization, or selling, any personal information under any circumstance, and promptly notifying concerned parties and taking proper measures if material information leaks or hacking has or is suspected to have occurred.

Important Announcement

This Legal Commentary has been prepared for clients and professional associates of Han Kun Law Offices. Whilst every effort has been made to ensure accuracy, no responsibility can be accepted for errors and omissions, however caused. The information contained in this publication should not be relied on as legal advice and should not be regarded as a substitute for detailed advice in individual cases.

If you have any questions regarding this publication, please contact **David TANG (+8621-60800905; david.tang@hankunlaw.com）.**