HAN KUN LAW OFFICES

Legal Commentary

CHINA PRACTICE • GLOBAL VISION

November 18, 2016

Comments on the Network Security Law

David TANG | Robin ZHANG | Effy SUN

On November 7, 2016, the *Network Security Law of the People's Republic of China* (the "**Network Security Law**") was adopted at the twenty-fourth meeting of the 12th National People's Congress after the third draft. The Network Security Law is composed of 7 chapters and 79 articles and will come into effect on June 1, 2017.

The Network Security Law will apply to the construction, operation, maintenance and use of networks as well as the supervision and administration of network security within the territory of the People's Republic of China (hereinafter, "**China**"). Below, we review and summarize some important systems and highlights of the Network Security Law.

Emphasizing national sovereignty and security in cyberspace

With the development of Internet and information technology, national sovereignty in cyberspace is facing significant challenges. The worldwide network environment may appear calm on the surface, but significant risks are present underneath. Network security is becoming a major issue of national sovereignty, security and interest. In response, many countries around the world have been formulating legal measures and building monitoring systems to maintain network security.

Take the European Union, for example. The European Court of Justice, the highest judicial body of the European Union, entered a judgment in October, 2015 that invalidated the safe harbor agreement regarding automatic data exchange, which was signed between the European Union and the United States in 2000. In April, 2016, the *General Data Protection Regulation* was adopted by the European Parliament after four years of discussion and has been regarded as the most stringent regulation for personal data protection. In July, 2016, the European Parliament adopted the *Instructions of Network and Information Security,* which marked the first network security act formally issued by the European Union.

Against this backdrop, China has passed the new *National Security Law* in July, 2015 and has defined the concept of "national cyberspace sovereignty". The *Outline of National Informatization Development Strategy*, promulgated in July, 2016, underscores the safeguarding of national sovereignty, security and development interests in advancing the promotion of national informatization construction, as well as accelerating network security legislation.

The Network Security Law follows the State's holistic development approach, and applies equal weight to network security and informatization. The Network Security Law also puts into practice relevant rules and measures for the protection of key information infrastructure, network information security, monitoring, early-warning and emergency responses, and legal liability. In particular, the final draft of the Network Security Law adds accountability measures for non-PRC persons.[1] These measures enhance defense and deterrence with respect to network sovereignty.

Implementing a hierarchical network security protection system

The Network Security Law requires a hierarchical network security protection system,[2] but this system was not first proposed by the Network Security Law.

In 2007, *Administrative Measures for Hierarchical Protection of Information Security* was promulgated by Ministry of Public Security, State Secrecy Bureau, State Encryption Administration and the Information Office of the State Council. Article 7 of the Administrative Measures divides the information security protection system hierarchy into 5 grades, and entities operating or using information systems are required to take concrete measures to carry out protection pursuant to *the Guidelines for Implementing the Hierarchical Information Security Protection System*. After the construction of an information system is completed, the entity operating or using the information system, or the competent department, will select a testing and evaluation agency that satisfies the conditions according to the Administrative Measures to regularly test and evaluate the security of the information system pursuant to the *Requirements for Testing and Evaluating the Hierarchical Information Protection Security System* and other relevant technical standards, and go through record-filing procedures.

Based on the *Administrative Measures for Hierarchical Protection of Information Security* in 2007, the relevant competent authorities have further promulgated guidelines and standards to enhance information security in their respective fields. For example, the November, 2009, *Notice of the General Office of Ministry of Education on Carrying out Hierarchical Protection for*

[1] Network Security Law, Art. 75. Non-PRC persons are subject to legal liability for activities that endanger key information infrastructure within the territory of the People's Republic of China, including attacks, intrusions, interference and damage that cause grave consequences. The Ministry of Public Security and relevant departments of the State Council have the right to freeze assets or impose other necessary punishment measures upon such non-PRC institutions, organizations and individuals.

[2] Network Security Law, Art. 21.

Information System Security requires college, university, and certain education department information systems of Grade III or above to undergo record-filing with the Education Management Information Centre of the Ministry of Education and local public security departments. The November, 2011, *Guiding Opinions of the Ministry of Health on Hierarchical Protection of Information System Security in the Healthcare Industry* requires information systems of Grade II or above to undergo record-filing with public security departments and health administration departments. Consequently, once the information systems of entities in certain industries reach a specified security grade, these entities will be supervised by both the public security departments and the competent departments in charge of that industry.

Furthermore, the *Administrative Measures for the Security Protection of Communication Networks*, promulgated by the Ministry of Industry and Information Technology in January, 2010, requires telecommunications operators and internet domain name service providers within China to partition their officially operating communications networks and to classify their networks into five grades based upon the degree of potential damage to national security, economic function, social order and public interest. Such persons are also required to perform the relevant filing procedures with the telecommunications administration authorities, implement security protection measures and conduct compliance tests.

As China's first specialized cybersecurity law, the Network Security Law legally requires national implementation of the hierarchical network security protection system for the first time,[3] although specific mechanisms and standards have not been formulated. It is therefore presently unclear whether operators must follow the dual-track supervision mode under the authority of the public security departments and assisted by the competent departments in charge of industry, or whether a unified network security classification scheme will be formulated in the future. This issue will require further monitoring.

Carrying out important protection of key information infrastructure

The Network Security Law introduces the concept of "key information infrastructure" and carries out important protections on the basis of a hierarchical network security protection system as described above. As a strategic resource to national security and interests, the importance of key information infrastructure cannot be overstated. The importance of protecting key information infrastructure in law and policy has become a legislative trend for many countries around the world.

The definition of key information infrastructure was subject to significant revisions from the first draft to the third draft of the Network Security Law. The final draft provides an open-ended definition, which contains many important industries and fields, including public communications and information services, energy, transportation, water conservation, finance,

[3] Network Security Law, Art. 21.

public services and e-government, and relevant key information infrastructure that could endanger national security, people's livelihoods and the public interest in the case of damage, loss of function or data leakage. The detailed scope of and security protection measures for key information infrastructure is to be formulated by the State Council. The definition roughly describes the attributes associated with key information infrastructure through listing these sectors. On the other hand, the definition leaves flexibility for the State Council to further determine the specific scope and to formulate security protection measures.

The Network Security Law mainly undertakes important key information infrastructure protection measures as follows:

a. Article 35 stipulates that operators of key information infrastructure that purchase network products and services which could affect national security must pass a security review organized by the national Internet information department in conjunction with the relevant departments of the State Council. At the same time, the Network Security Law provides for corresponding punishment in the legal liability chapter.[4]

   It is worth noting that the national security review of key information infrastructure was not first proposed by the Network Security Law. The *Foreign Investment Law of the People's Republic of China (Draft for Comment),*[5] promulgated in early 2015, lists the impact on key infrastructure and technologies as a factor to be considered during the national security review for proposed foreign investments. Thus, we can perceive and appreciate the strategic significance of key (information) infrastructure to the national security.

b. Article 37 establishes the relevant principles for cross-border information transmission for key information infrastructure, namely that personal information and important data collected and generated in the operation of key information infrastructure operators within China must be stored domestically. Where it is necessary to provide such information and data overseas due to business needs, a security assessment is required to be carried out according to measures formulated by the national Internet Information Department in conjunction with the relevant departments of the State Council, absent any contrary legal or regulatory provisions.

   So far, the Network Security Law is the first law to restrict the transfer of data overseas. However, this restriction only refers to personal information and important data collected and generated by the operation of key information infrastructure operators within China. Notably, the information scope of restricting the transfer of data was "personal information" and "important business data" in the second draft, but has been broadened to "important data" in the final draft, thus widening the scope of the transfer restriction.

4 Network Security Law, Art. 66.

5 Foreign Investment Law of the People's Republic of China (Draft for Comment), Ch. 4.

Improving Personal Information Protection

a. Expanding the Scope of Protected Subjects: Compared to the previously issued second draft, the Network Security Law removes the restriction on "personal information" to be of "citizens", which broadens the scope of protected subjects to include all individuals using PRC network services, whether domestic or overseas. The aim is to avoid a legislative vacuum with respect to protecting the personal information of non-citizens.

b. Definition of Personal Information: Article 76 of the Network Security Law provides that personal information refers to all kinds of information, recorded electronically or otherwise, that can identify, independently or in combination with other information, a natural person's personal identity information, including but not limited to the natural person's name, date of birth, identification number, personal biometric information, address, telephone number, etc. This definition, although relatively broad, does not include information that can identify, independently or in combination with other information, when and where the user used the service,[6] which contrasts with the *Provisions on the Protection of Personal Information of Telecommunications and Internet Users* enacted in 2013.

c. Development and Application of Big Data: Article 42 of the Network Security Law prohibits network operators from divulging, distorting or damaging personal information that is collected, and from providing personal information to others without the consent of the person whose data has been collected, except where the information has been irreversibly anonymized. This exception would appear to free network operators from personal information protection rules when using such legally collected data if it has been processed so that specific individuals are unidentifiable and their identities are unrecoverable. This reflects legislators' intent to create feasibility for big data applications at the legislative level, so as to strike a balance between protection of personal information and the public interest.

d. Imposing Information Security Obligations on Network Operators: The Network Security Law consolidates the current provisions applicable to the protection of network information, such as 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 on the Protection of Consumer Rights and Interests*, the *Several Provisions on Regulation of the Order of the Internet Information Service Market*. Such provisions require network operators to, among others: disclose their rules for data collection and use, collect and use information as agreed, provide for certain safeguards to ensure information security and prevent information from being compromised or lost, and promptly undertake remedial measures when any information is or may have been compromised or lost. Any individual that discovers the illegal collection or use of personal

6 Provisions on Protecting Personal Information of Telecommunications and Internet Users, Art. 4.

information by a network operator can require the network operator to take remedial measures, and the network operator is explicitly required to take such measures.[7]

Article 49 of the Network Security Law stipulates that network operators should cooperate with the lawful monitoring and inspections by the Cyberspace Administration and relevant authorities. This provision, however, does not articulate the extent of such cooperation and due process of the authorities, which may result in controversies or even the abuse of power during monitoring or inspections.

e. Punishment for Illegal Acts such as Online Fraud: Article 46 of the Network Security Law provides that individuals and organizations will be held responsible for their use of networks, and cannot set up websites or communication groups for the purpose of committing fraud, imparting criminal methods, manufacturing or selling prohibited goods, nor publish information online regarding such illegal activities. The regulatory authorities may impose punishment on such violators in accordance with Article 67. This article was not contained in the second draft, but appears in the officially promulgated Network Security Law, and reflects legislative and regulatory bodies' determination to regulate the currently flourishing telecommunications fraud and e-commerce disorder.

Liabilities

The Network Security Law amends some of the punishment standards compared to the second draft, such as doubling the monetary penalties for certain illegal acts. Different industry access bans apply to acts that prejudice network security, which include unlawful intrusion into the networks of others, interference with the functioning of the networks of others, theft of network data, or the provision of services for such activities. Persons subject to public security administration punishment cannot take key positions in network security administration and network operations for five years, and criminal violators are subject to a lifetime ban on taking such positions.[8]

Summary of Other Highlights

a. Attention to Juvenile Protection: Article 13 of the Network Security Law calls for research and development of network products and services beneficial to the health of minors, and punishes activities harming physical and mental health of minors through networks with specific punishments. The aim is to provide for a secure and healthy network environment for minors.

b. Definition of "Network Operator": Article 76 of the Network Security Law defines "network operators" broadly to include network owners, administrators and service providers, which

7 Network Security Law, Arts. 40 to 45.

8 Network Security Law, Art. 63.

basically includes all types of persons that carry out activities through networks. The Network Security Law may therefore apply to any for-profit or non-profit entity that provides network services or provides products and services in China via communications networks, the Internet, etc.

c. Real-Name Verification: Article 24 of the Network Security Law requires real-name verification. Network operators must require users to provide genuine identity information when entering into agreements or confirming the provision of services regarding network access, domain registration, landline or mobile telephone network access, information publication or instant communication services. Relevant network service providers and network operators are required to strictly abide by these regulations and standards.

d. Regulatory Authority Confidentiality and Compliance Obligations: Given that regulatory authorities will receive large amounts of information during routine regulatory activities as well as during the investigation and punishment of illegal acts, Article 30 of the Network Security Law provides that the relevant authorities may only use information obtained when executing network security protection duties as is necessary for maintaining network security.

   In addition, Article 14 of the Network Security Law, concerning the reporting of illegal acts, requires the relevant authorities to keep confidential the informant's information and to protect his or her lawful rights and interests. This also encourages positive reporting and facilitates public supervision.

e. Monitoring, Precautions and Emergency Management: Network security is to be maintained through advance precautions, prevention during the course and post-event management. The Network Security Law requires network operators to establish contingency plans in case of network security events.[9] In addition, Chapter 5 of the Network Security Law specifically provides for the establishment of network security monitoring, precautions and emergency treatment, requires the setting up of network security monitoring, precautions and information reporting systems at the national level. These requirements are intended to enhance network security event risk prevention mechanisms and to promote network security event treatment mechanisms, while also introducing relevant laws and regulations including the *Emergency Response Law of the People's Republic of China* and the *Work Safety Law of the People's Republic of China*.[10]

Recap and Commentary

The Network Security Law, the first specialized cybersecurity law in China, concisely consolidates into a single law the provisions on network security and information protection

9 Network Security Law, Art. 25.

10 Network Security Law, Ch. 5.

contained in various lower-level laws. The law also marks a milestone by addressing the evolution of big data and informatization. A major reason for network security events and information leaks that have occurred in China in the past has been the absence of legislation and slack enforcement. Insignificant costs associated with violations and light punishment cannot act to draw enough attention to online information protection, nor encourage network operators to take sufficient protection measures.

In recent years, the PRC government has paid increasing attention to regulating network security and protecting personal information. Therefore, all domestic enterprises, whether network owners, administrators, or the vast number of network product and service providers, should strictly comply with requirements of the Network Security Law and carefully implement network security and personal information protection measures. At the same time, the Network Security Law will still need to be improved through experience from practice, as well as through promulgating supporting laws, regulations, administrative measures and standards. We will continue to monitor subsequent developments related to the Network Security Law.

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）.**