LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Data Privacy, Security & Cybercrime Practice 23 November 2016 | Number 2041

China Issues Its First Network Security Law

The law will have far-reaching implications for parties that utilize the Internet and handle network data and personal information in the PRC.

On November 7, 2016, the Standing Committee of the National People's Congress of the People's Republic of China issued China's first and comprehensive Network Security Law (also referred to as "Cybersecurity Law"), which will come into effect on **June 1, 2017**. The Network Security Law establishes an overarching regulatory framework to ensure network security and the law covers the construction, operation, maintenance and use of networks in the PRC by international and domestic individuals and entities, as well as regulators' administration and supervision of network security.[1]

The Network Security Law introduces rules and requirements that will significantly impact individuals and entities utilizing the internet in the PRC. For instance, network operators (*i.e.*, owners and administrators of networks and network service providers) will be subject to "class-based" network security requirements, with different levels of security standards for network operators in different classes. Critical network equipment and network security products will need to comply with mandatory national standards, and will be subject to security certification or inspection.

Further, enhanced security requirements will apply to the "critical information infrastructure" (CII) in the PRC. CII is broadly described to cover infrastructure used by the public communications and information services, energy, transportation, water conservancy, finance, public utilities and e-government affairs sectors, and any other infrastructure that, if damaged or malfunctioning, could significantly jeopardize the PRC's national security or public interests. CII's detailed scope and compliance requirements will be further supplemented at a later stage.

In Brief: Network Security Law

- The new law applies to all "operators" (*i.e.*, owners, administrators and service providers) of networks in China
- Introduces more onerous rules for CII (Critical Information Infrastructure) and CIIOs (Operators of CII)
- Personal information and critical data of CIIOs must be kept in China, absent governmental approval
- Detailed security standards expected for different classes of operators
- Introduces new breach notification requirements
- Requires identify verification
- Further clarifications anticipated

If certain infrastructure qualifies as CII, personal information and critical data generated by operators of CII (CIIOs) within the PRC will need to be stored in the PRC, and cross-border transmission of such information and data will need to be supported by business necessity and will require a security

assessment by government authorities. Further, certain network products and services that CIIOs purchase will be subject to national security review by Cyberspace Administration Office and other relevant authorities.

Relevant entities and individuals need to fully understand the Network Security Law, closely follow related legislative developments, and prepare in advance before the new law comes into effect on 1 June 2017, in order to avoid the legal repercussions of non-compliance.

Jurisdictional Scope

It appears that the Network Security Law would primarily govern activities occurring on networks that are physically within the territory of the PRC. Article 2 of the Network Security Law provides that the law applies to the construction, operation, maintenance and use of any network in the PRC. The term "network" is defined under Article 76 as a system consisting of computer hardware that collects, stores, transfers, exchanges and processes data. Given that Article 2 specifies that the law applies to activities on networks in the PRC, activities foreign network operators engage in solely on network components existing outside of the PRC are less likely to be subject to the compliance requirements, even if such activities can be accessed via the Internet from the PRC.

That being said, the Network Security Law, under Article 5, notably authorizes PRC authorities to monitor and take preventive/defensive actions to defend against certain network activities that occur outside of the PRC but create negative consequences in the PRC (such as security risks and threats, Internet crimes and telecommunication fraud). For instance, under Article 50, government authorities can require entities to screen and block information that originates from outside of the PRC but is prohibited under PRC laws. Article 75 allows authorities to take certain enforcement measures (*e.g.*, freeze property) against foreign entities or individuals that attack, infringe, interfere with or damage CII in the PRC.

Enforcement Agencies

The Network Security Law lists multiple government authorities that will oversee network security matters. Under the current arrangement, the Cyberspace Administration Office is responsible for coordinating with other government authorities to oversee and manage network security matters. The Ministry of Industry and Information Technology, the Ministry of Public Security and other relevant departments (and their respective local counterparts) will each participate in supervising and administering network security matters within their respective areas of authority. The Standardization Administration of the PRC will establish national standards and industrial standards regarding network security. We expect that subsequent regulations will likely clarify more detailed division of authority among the enforcement agencies.

Secured Operations of Networks and CII

The Network Security Law introduces a set of general requirements to ensure secure network operations and an additional set of enhanced rules applicable to CII.

General Requirements

A class-based network security protection system applies to all network operators in the PRC. The Network Security Law does not further clarify standards or thresholds for each class. While the details of the class-based network security protection system require further definition, the Network Security Law sets out general compliance requirements to ensure security of network operations, which are highlighted below:

- Network Security Protection System. Network operators must establish internal network security protection systems and fulfill certain obligations to ensure network security, such as setting up internal network security policies, appointing a responsible person in charge of network security matters, adopting anti-virus technologies, and implementing data backup and encryption measures.

- Network Monitor and Data Retention. Network operators must implement measures to monitor and record network operations and network security incidents, and are required to retain network daily logs for at least six months.

- Identity Verification. Network operators must require verification of a user's real name and identity, upon execution of a service agreement or upon confirmation by network operators to provide users with network access, domain name registration, local/mobile phone networking access, instant messaging and information publication services.

  Although the new law does not elaborate on how a user's identity will be verified, this requirement is not foreign to Chinese users. In practice, cases exist in which network and phone services providers require in-person or online verification of users' personal identity documents (usually ID cards for PRC nationals and passports for foreigners) upon service subscriptions. For subscriptions that predated the requirements, PRC mobile service providers have suspended services until the users' identity verifications were completed. Websites and apps also commonly require users to verify their identity by providing passcodes received in the users' cell phones.

- Information Management. Network operators are required to monitor the information that users post, to promptly remove prohibited information and prevent further dissemination of such information, and to report such information to government authorities. While information monitoring/management is required under the Network Security Law and other PRC regulations, detailed requirements and procedures (such as censored words or topics) remain unavailable to the general public.

- Cooperation with Government Authorities. Network operators are required to provide technical support and assistance for government authorities in national security and crime investigation matters, and to cooperate with government authorities during legitimate government monitoring and inspections.

- Compliance with Mandatory National Standards. Network products and services must comply with mandatory national standards, and providers of these products and services must take immediate remedial measures in case of security breaches or loopholes; in particular, critical network equipment and network security products (the list of such equipment and products is yet to be publicized) must be produced, tested and certified in compliance with such mandatory national standards before they can be sold or provided.

Enhanced Protection Measures for CII

The Network Security Law requires CIIOs to implement additional enhanced protection measures, which are highlighted below:

- National Security Review. CIIOs must submit to government authorities for review and approval all equipment or infrastructure product purchases that could potentially jeopardize national security. Detailed procedures and standards for such process are yet to be publicized.

- Enhanced Network Security Protection System. CIIOs must appoint a responsible person in charge of network security matters, and conduct a background check on such person. CIIOs are also required

to back up important systems and databases, employ a disaster recovery system for critical systems and databases, and establish a network security incident emergency plan and conduct periodic rehearsals.

- Security and Confidentiality Agreement. CIIOs must enter into security and confidentiality agreements with suppliers when purchasing network products or services.

- Annual Testing and Appraisal. CIIOs must conduct annual testing and appraisal of the CII's network operation security.

Network Information Security and Personal Information Protection

General Requirements

The Network Security Law also emphasizes network information security, with a focus on personal information protection. The Network Security Law defines the term "personal information" as information that can be used, independently or jointly with other data, to identify a natural person's identity, such as the person's name, address, telephone number, birthday, ID number and biometric data. The definition of personal data and most rules regarding personal information protection under the new law are generally consistent with the existing PRC regulations. The following are examples of the relevant rules under the Network Security Law:

- Principles. Network operators must abide by the principals of legality, legitimacy and necessity when collecting and using any personal information.

- User Consent. Network operators must explicitly set out the purposes, means and scope of collecting and using personal information, and are required to seek users' prior consent before collecting such information.

- Confidentiality. Network operators as well as departments and personnel that are responsible for network information security must keep user personal information, privacy and trade secrets strictly confidential, and must not disclose this information to third parties without the user's consent.

- Protection System. Network operators are also required to establish and strengthen their systems to protect user information, and are not allowed to leak, alter or damage the personal information collected. Network operators must immediately take remedial measures in case of actual or potential disclosure, damage or loss of personal information, and are required to report these incidents to the relevant users and government authorities.

Data Localization

The Network Security Law introduces new rules restricting storage and cross-border transmission of personal information and "critical data" collected and generated through CIIO's operations in the PRC. Under the new law, such personal information and critical data must be ***stored within the PRC***. If any cross-border transfer of such information and data is necessary for business reasons, CIIOs must submit the proposed transfer to the government authorities for a security assessment, which will be subject to regulations the relevant authorities will issue. As many domestic and multinational corporations could potentially fall within the scope of CII, these corporations will likely encounter restrictions and impediments resulting from the new data storage and transmission requirements.

Notifications

The law also contains unique and interesting notification requirements. In addition to Article 24 covering notifications of incidents, for example, Article 22 states that Internet product and service providers must not install or distribute malicious programs. In the event products or services have been discovered to contain security defects, or that data leakages or other security risks have occurred, providers must promptly inform their users and take remedial action. Network operators must also promptly inform their users and supervisory departments. The article specifies no time frames under which these notifications or reports must be delivered, nor does language clarify responsibility in cases where third parties or other unsanctioned actors install malicious products or services without the knowledge of the original provider, or if third parties install software or services incorrectly.

Penalties for Non-Compliance

Any entity's or individual network operator's non-compliance with the requirements under the Network Security Law may result in demands for rectification, warnings, forfeiture of illegal gains, administrative fines and/or administrative retention. Under serious circumstances, enforcement agencies could also suspend non-compliant business operations, suspend a business' entire operation, shut down websites and/or revoke operational licenses. If the non-compliance rises to the level of a criminal offense, the non-compliance may also be prosecuted criminally under PRC Criminal Law. The Network Security Law also allows a party to recover damages through civil litigation in court.

Article 65 requires that CIIOs only use products and services that have passed the mandatory government cybersecurity review. Agencies can order CIIOs to stop using non-certified products or services, and CII operators can be fined an amount ranging from one to 10 times the original cost of the procured item. A direct fine of anywhere from RMB10,000 to RMB100,000 may also be levied to responsible personnel.

Observations – Significant Implications for Business Operations in the PRC

The Network Security Law introduces sweeping new certification requirements and national standards that further strengthen the PRC's control over network security and related technology, which could present significant challenges to market participants in the relevant sectors and create compliance requirements for business far beyond these sectors.

For instance, to comply with new data storage and transmission requirements under the Network Security Law, domestic and multinational corporations that may qualify as CIIOs will need to reevaluate their internal processes regarding collecting, storing, processing and transmitting user information and critical data, and adjust accordingly. Further, corporations that provide network or phone access, domain name registration, instant messaging or information publication services should be prepared to implement measures to verify their users' personal identification, which may require significant resources and impact users' satisfaction with the services. The law also explicitly requires the network operators to cooperate with government in support of activities relating to national security and law enforcement. This obligation is drafted broadly and will only become clear through further interpretation and application.

Such challenges are heightened by uncertainty. The Network Security Law has yet to clarify the definition and scope of key concepts (*e.g.,* CII, critical data, critical network equipment); required procedures and processes (*e.g.,* the process to be followed to undertake a security assessment for a cross-border transmission of CII's information, or a security review for network products and services CII will purchase); and scope and degree of cooperation government authorities will require.

On the other hand, to the extent Article 16, for example, calls for promoting "secure and trusted" network products and services, the Network Security Law could also bring new investment opportunities for corporations, such as network security certification services, and development and application of network security technologies and convenient digital ID technology.

As the Network Security Law is the fundamental law to all organizations, we expect implementing rules and supplemental regulations and guidance will be issued to fill in some of the detail needed to underpin the principles set out in the new law. Given the new law's significant impact, organizations are advised to pay close attention to further legislative developments relating to the law, and prepare in advance to avoid any non-compliance before the Network Security Law comes into effect on June 1, 2017.

If you have questions about this *Client Alert*, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

China Contacts

Hui Xu
hui.xu@lw.com
+86.21.6101.6006
Shanghai

Lex Kuo
lex.kuo@lw.com
+852.2912.2511
Hong Kong

Data Privacy Specialists

Jennifer C. Archie
jennifer.archie@lw.com
+1.202.637.2205
Washington, D.C.

Gail E. Crawford
gail.crawford@lw.com
+44.20.7710.3001
London

Serrin A. Turner
serrin.turner@lw.com
+1.212.906.1330
New York

You Might Also Be Interested In

Mitigating Cybersecurity Risks

New EU Data Protection Rules Move the M&A Goalposts

Europe Counts Down to the General Data Protection Regulation

7 Tips for Conducting Effective Cybersecurity Due Diligence in M&A Transactions

---

Endnotes

[1] The US-China Business Council published a useful position paper on an earlier draft of the law, available in an English-language version, here.