# China's new network security law may affect operations inside and outside China: Are you ready?

Network operators in China, especially of critical information infrastructure, face increasing protection requirements that could burden service contracts and affect data beyond China.

By *Hui Xu and Lex Kuo,* **Latham & Watkins**

**Key points:**

- China's new Network Security Law is prioritising protection of cybersecurity and individuals' privacy.
- Network operators in China, who collect personal information in China, are required to establish systems to protect their users' information.
- In-house lawyers should help their enterprises prepare for evolving and expanding cybersecurity laws.

Data protection in China is becoming increasingly challenging for network operators to navigate in the past few months. The promulgation of China's much-anticipated Network Security Law (the Network Security Law) and its accompanying regulations will likely have the most far-reaching impact of any legal measures yet.

Effective since June 1, 2017, the Network Security Law, together with its accompanying regulations, not only provides important rules for China's network data protection and security, but also poses continuing challenges for national and international enterprises. Recent news articles indicate that the Cyberspace Administration of China (the CAC) has conducted several enforcement actions relating to data protection, such as reviewing privacy policies and their implementation in practice by Chinese network operators. These are clear indicators that data protection and cyber security in China are real risks to be taken seriously. This article provides an overview of how in-house counsel can work toward compliance with these rules and the accompanying challenges.

## Lay the groundwork with a cybersecurity management system

The provisions of the Network Security Law apply to network operators (ie, owners and administrators of networks and network service providers) in China, who must establish policies ensuring Chinese cybersecurity protection. Nonperformance of network security management duties under the Network Security Law will not only incur administrative penalties under the Network Security Law, such as suspension of business operation, closure of websites, revocation of permits/licences, and administrative fines applicable to enterprises and relevant individuals. The nonperformance may also trigger criminal liabilities, such as imprisonment, criminal detention, and/or criminal penalties, if nonperformance incurs certain serious consequences as defined under the PRC Criminal Law (eg, leak of user information that causes serious consequences).

In-house lawyers should ensure their enterprises comply with the relevant

requirements of the Network Security Law, including incorporating network security measures into their cybersecurity systems. For instance, network operators in China must address all of the following:

- **Cybersecurity measures.** Implement technical measures to prevent computer intrusions and to monitor network operation; appoint in-charge personnel for cybersecurity matters; keep the relevant logs no less than six months; back up and encrypt important data; and develop and rehearse emergency plans for cybersecurity hazards (eg, virus, cyber-attack, and network intrusions).
- **User Information protection.** Obtain informed consent from users before collecting their information; set up a user information protection system to keep the user information strictly confidential; establish mechanisms to accommodate users' requests to delete or to correct user information under certain circumstances; take immediate remedial measures and promptly notify users and relevant administrative authorities if personal information is or might be leaked, damaged, or lost.
- **Online content management.** Verify users' real identity and information before network operators will provide certain services related to publication or dissemination of online content, such as services regarding network access, domain name registration, access formalities for fixed-line telephone or mobile phone, information release, or instant communication; strengthen the management of user-provided information and prevent the dissemination of illegal information.
- **Network products and services requirements.** Network products and services suppliers must ensure the network products and services comply with relevant mandatory requirements under Chinese national standards; provide security support during the period required under regulations or agreed to by the parties; take immediate remedial measures and promptly inform users and relevant government authorities in case of cybersecurity hazards.

## Expect increased oversight for critical information infrastructure to impact business and data inside and outside China

In addition to the aforesaid requirements applicable to network operators, enterprises that are considered critical information infrastructure (CII) are subject to enhanced cybersecurity requirements, such as heightened cybersecurity measures, data localisation requirements, and national security review on procurements of network products and services.

### *Evolving scope of CII*

While the Network Security Law and its related regulations and standards (currently in draft form for public comments) set out high-level descriptions of industries that the Network Security Law will consider as CII, the specific scope of CII is still pending further clarifications by relevant authorities.

*Hui Xu*

> The Network Security Law not only provides important rules for China's network data protection and security, but also poses continuing challenges for national and international enterprises.

*Lex Kuo*

By way of background, the scope of CII is set out below in a chart summarising the relevant provisions in the Network Security Law and a draft of the Regulations on Security Protection of Critical Information Infrastructure (the Draft CII Regulations) issued by CAC on July 10, 2017:

| | Network Security Law | Draft CII Regulations |
|---|---|---|
| Scope of CII | 1. Important industries and sectors such as public communications and information services, energy, transport, water conservancy, finance, public utilities and e-government affairs | 1. Government agencies and entities in the energy, finance, transportation, water conservancy, health care, education, social insurance, environmental protection and public utilities sector |
| | | 2. Information networks, such as telecommunication networks, broadcast television networks, the internet, and entities providing cloud computing, big data and other large-scale public information network services |
| | | 3. Research and manufacturing entities in sectors such as science and technology for national defence, large equipment manufacturing, chemical industry and food and drug sectors |
| | | 4. Press units such as broadcasting stations, television stations and news agencies |
| | 2. Other industries and sectors that, once damaged, disabled, or data breached, may severely threaten the national security, national economy, peoples' livelihood and public interests | 5. Other key entities, whose network facilities and information systems, if damaged, disabled, or breached, may severely jeopardise national security, people's livelihood and public interest |

While the open-ended descriptions of CII under the Network Security Law and the Draft CII Regulations cannot completely eliminate uncertainties for determining whether an entity will be considered as CII, the Draft CII Regulations provide further clarity on the scope of CII. The Draft CII Regulations also indicate that CAC will collaborate with relevant government authorities to promulgate CII Identification Guidelines, which are expected to further clarify the scope of CII. Reports indicate that the relevant government authorities have identified a few hundred of enterprises, mostly state-owned enterprises in China, as CII operators (CIIOs). The relevant government authorities have informed these state-owned enterprises that they have been identified as CIIOs and of the relevant compliance requirements. Once the relevant government authorities reveal the initial list of CIIOs, and following the upcoming promulgation of the CII Identification Guidelines, enterprises hopefully will have more clarity on CII determination standards in the near future.

***Enhanced data related requirements for CII***

Pursuant to the Network Security Law, CIIOs are subject to enhanced cybersecurity requirements, such as setting up specialised agencies for cybersecurity management, providing CII cybersecurity practitioners with regular cybersecurity education and training, and implementing data categorisation, back-up, and encryption. Some of the most notable and controversial enhanced cybersecurity requirements applicable to CIIO under the Network Security Law are the data localisation requirements.

Specifically, the Network Security Law requires that a CIIO must locally store in the PRC the personal information and "critical data" collected and generated by CIIOs through their operations in 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. In addition to the data localisation

requirements, the Draft CII Regulations further require that any operational maintenance of CII should be conducted within the territory of the PRC, and any remote maintenance to be conducted outside of the PRC should be reported to the industry specific governing or supervising authorities and public security departments.

As many domestic and multinational enterprises could potentially fall within the scope of CII (which is still evolving at the current stage), these enterprises will likely encounter restrictions and impediments resulting from the new local data storage/transmission requirements, and, potentially, restrictions on remote operation maintenance from abroad (as required under the Draft CII Regulations). As such, enterprises must closely follow related legislative developments, and prepare in advance in order to avoid the legal repercussions of non-compliance.

## Maintain protections for an expanding universe of personal information

Another notable development under the Network Security Law and its related regulations is the emphasis on protection of personal information. While similar requirements exist under various previous regulations, the Network Security law reiterates such requirements under a comprehensive and cohesive structure, requiring network operators to establish a user information protection system and to strengthen protection of user information. Crucially, in-house counsel must also review whether an enterprise conforms in all respects with the requirements to protect user information.

Particularly noteworthy under the new law is the emphasis on network operators to set up a comprehensive user information protection system, to explicitly communicate with data subjects about collection, storage, process, and transfer of personal information, and to obtain informed consents from data subjects about the aforesaid operations. Specifically, according to the Network Security Law, network operators must explicitly state the purpose, method, and scope of collecting and using users' personal information, and must ensure they have received consent from the individual for the collection, use, transfer, and sharing of personal data, which must conform with the agreement by and between such network operators and the users. Further, under the Network Security Law, network operators should not disclose user information to third parties without securing consent from data subjects with an exception for disclosure of anonymised user information that cannot be used to identify specific individual.

In practice, the emphasis on network operators has been reflected in recent enforcement actions regarding privacy policies of network operator. Recent news articles indicate that Chinese authorities have reviewed and commented on the privacy policies of at least ten leading online service providers. One of the operators of mobile map applications in China reportedly will adopt its new privacy policy based on the draft regulations entitled "Personal Information Security Regulations" (the regulations are expected to be released for public comments in the near future). Further, the Ministry of Industry and Information Technology also promulgated the Guidelines on the Standardised System Construction for Mobile Network, which contemplate including a set of Guidelines on Protection of Users' Personal Information that in-house counsel should refer to when preparing privacy policies of network operators.

Given the Network Security Law's potential criminal liabilities on enterprises and individuals for non-compliance at a minimum, in-house lawyers should review and conduct self-assessment on their enterprises' existing privacy policies and infrastructure on protection of personal information, in order to identify potential weaknesses and to rectify any non-compliance.

## Are you ready?

In conclusion, China is not only strengthening the supervision of internet activities and data protection, but also imposing more obligations on network operators and users. Wise enterprises will take steps to prepare not only for the changes that have come, but those that are yet to come.

*This article was prepared with the valuable assistance of Jennifer C Archie, partner in the Washington, DC office of Latham & Watkins.*

LATHAM & WATKINS LLP
***hui.xu@lw.com***
***lex.kuo@lw.com***
***http://www.lw.com***