WILMERHALE

# *China's Cybersecurity Law Imposes New Requirements on Doing Business in China*

November 10, 2016

*T*he Standing Committee of China's National People's Congress (NPC) adopted the country's Cybersecurity Law[1] on November 7—the latest in a spate of national security-related measures targeting the ICT industry. Drafts of the Cybersecurity Law had raised significant concerns in the international business community, due to provisions with the potential to restrict market access such as data localization requirements, national security reviews for ICT products and services, and data retention and sharing requirements. The final draft is largely consistent with previous drafts, although the provisions of the Law are cast broadly, and it will be up to the State Council, Cybersecurity Administration of China, and other government bodies to issue implementing rules in the months and years ahead (in addition to related rules that are already in place). The Cybersecurity Law itself will take effect June 1, 2017.

The Cybersecurity Law critically distinguishes between two categories of companies that are subject to its provisions: "network operators" (NOs) and "critical information infrastructure operators" (CIIOs). The former category appears to encompass every company in China that operates internal corporate networks to store information (although the scope of this term may be narrowed in forthcoming implementing rules). On the other hand, CIIOs are a subset of NOs. While the Law does not define CIIOs, the term appears to refer to companies operating networks which, were they to fail, would seriously jeopardize public security and public welfare (*e.g.*, public communications and information services, power, traffic, water, finance, public service, and electronic governance). The Cybersecurity Law contains provisions that apply to all NOs, as well as special provisions for CIIOs, which tend to be more stringent.

Specific requirements in the Cybersecurity Law include:

- *Data localization:* Personal information and other important data gathered or generated by CIIOs (but not NOs generally) from operations in mainland China must be stored in China. However, if there is a genuine business purpose, the data may in some cases be stored outside mainland China, following the performance of a security assessment in coordination with relevant government bodies.[2]

- *National security reviews for ICT products and services:* CIIOs that purchase network products and services that may impact national security must undergo a government national security review.[3]
- *Security and confidentiality agreements:* CIIOs, when procuring network products and services from vendors, must obtain a security and confidentiality agreement.[4]
- *Personal data protection:* NOs must limit the scope of data collected to ensure that it is related to services that they provide; and disclose to subject persons the fact that they collect personal data, as well as the purposes, means, and scope of data collected, and their policies for its collection and use.[5]
- *Data retention and sharing:* NOs must not disclose, tamper with, or destroy personal information which they gather, unless it has been properly anonymized.[6]
- *Cooperation with law enforcement:* NOs must provide technical support and assistance to public security organs and state security organs.[7]
- *Real name policies:* NOs that handle network access and domain registration for users, landline or mobile phone network access, or which provide users with information publication or instant messaging services, must require users to provide their real identity when they sign up. Any user who fails to provide his or her real identity must be denied service.[8]
- *Whistleblower protections:* The Cybersecurity Law bestows on all individuals and organizations the right to report conduct endangering network security to responsible government entities—in effect, empowering whistleblowers.[9] The Law leaves it unclear whether companies may impose procedures on the performance of this right, for example by requiring internal reporting of security risks within the company prior to notification of the government authorities.

The Cybersecurity Law imposes a range of penalties for violations, ranging from relatively low monetary fines to detention in serious cases. In addition, as a result of revisions to the Cybersecurity Law last week prior to its adoption, “foreign agencies, organizations or individuals” that endanger China's critical information infrastructure are subject to asset seizures and other punitive measures—a provision that is apparently drafted with foreign hackers in mind, though potentially with broader application.[10] The Cybersecurity Law also establishes civil liability for violations (although such a provision already exists under less authoritative law).

Please contact us if you have any questions about how the Cybersecurity Law affects your company.

---

[1] An unofficial English translation of the Cybersecurity Law is available here: chinalawtranslate.com/cybersecuritylaw/?lang=en.

[2] Article 37.

[3] Article 35.

[4] Article 36.

[5] Article 41. Personal data is defined to include all information that taken alone or together with other information, is sufficient to determine a natural person's identity, including, but not limited to, natural persons' full names, birth dates, identification numbers, personal biometric information, addresses,

telephone numbers, and so forth. Article 76(5).

[6] Article 42.

[7] Article 28.

[8] Article 24.

[9] Article 14.

[10] Article 75.

## *Contributors*

### Ambassador Charlene Barshefsky

**PARTNER**

### Lester Ross

**PARTNER**

### Benjamin A. Powell

**PARTNER**