MAYER • BROWN
JSM

Legal Update
Mainland China
10 November 2016

China Passes Cybersecurity Law

On 7 November 2016, the Standing Committee of the National People's Congress of China (NPC) passed the controversial Cybersecurity Law (the "CSL"). The CSL has gone through three readings since the release of the first draft on 6 July 2015 and will take effect in June 2017. As China's first comprehensive privacy and security regulation in the cyberspace, the CSL enhances data protection in many aspects while bringing in compliance challenges for the international community at the same time.

Applicability

The CSL adopts a tiered approach and imposes different obligations and duties to Critical Information Infrastructures (CIIs) and network operators. "Network operators" are defined to include operators of basic telecommunication networks, internet information service providers, and key information systems. The definition of "CII" has adopted an earlier version that makes specific reference to a few key sectors such as finance and transportation while retaining the broad catch-all phrase from the second draft to cover "infrastructure that, in the event of damage, loss of function, or data leak, might seriously endanger national security, the national welfare, the livelihoods of the people or the public interest." Both the second and third drafts stated that the exact scope of CIIs would be determined separately by the State Council, leaving the government with considerable leeway to bring industries not specifically singled out in the definition into the scope of the legislation at a later stage. Some of the heightened requirements, such as data localisation and cross-border transfer restrictions, apply to CIIs only.

Data Localisation and Cross-Border Transfers

Under perhaps one of the most controversial provision of the CSL, operators of a "CII" are required to store within China "citizens' personal information and important data" collected or generated during business operations in China. If, for legitimate business reasons, the data must be provided to a foreign entity outside China, the operators must complete a "security assessment" jointly formulated by the National Cyberspace Administration and State Council. Notably, the initial draft applied the localisation requirement to "citizens' personal information and other important data" while the later draft revised this to "citizens' personal information and important data." The second draft also narrowed the scope of data subject to localisation to only data collected or generated within China. While the first draft seemed to allow operators to "store abroad such data or provide it" to an entity or individual located abroad provided that it passes a security assessment, the later draft removed the overseas storage option. The terms "security assessment" and "important data" remain undefined.

Upon a narrow interpretation of this localisation requirement, all Chinese citizens' personal data and transaction data collected or generated within China may be required to be stored in China. This in essence would mean a segregation of the global information system into one distinct system for China and one for the rest of the world. This could have a significant impact on multinational companies (MNCs) doing business in China which inevitably need to share data internally and across borders on a daily basis. No exemptions seem to be envisaged by the new law except for the security assessment channel which appears even more stringent than what data privacy regimes such as the EU have always had (be they by way of express consents, internal corporate contractual arrangements sanctioned by regulators, model clauses or other such mechanisms). Even Russia's data localisation rules , which have made headlines, are limited to operators

processing personal data concerning Russian citizens that are physically located in Russia or own a website targeting Russia. However, the rules do not prohibit remote access of a database physically located in Russia that processes personal data of Russian citizens. By contrast, under the literal reading of the Chinese law, CIIs must undergo a security assessment with the Chinese authority if cross-border remote access is considered "provision" abroad.

Increased Penalties for Data Breaches and Violations

The CSL provides that Chinese authorities can require network operators to provide necessary assistance and support to accommodate national security and criminal investigation needs without specifying any limit on such power. It also provides penalties for non-compliance with its provisions by business entities or responsible individuals, including warnings, rectification orders, fines, or confiscation of illegal gains, and suspension of business operations or the revocation of the entity's business license. In the case of a network security incident, Chinese authorities may have the power to compel an interview of network operators. The CSL further provides that violations of the CSL should be included in the credit history of violating entities and individuals and can be made public. Additionally, individuals punished for endangering network security could be prohibited for life from taking on jobs related to network security management or other key posts related to network operation in China. Finally, overseas entities or individuals that attack, compromise, interfere with or destroy Chinese CIIs will be subject to legal liability and sanctions including assets-freezing pursuant to a provision added in the third draft.

Enhanced Privacy Protection for Individuals

Although many of the privacy and security obligations imposed upon network operators and CIIs have appeared in other sector-based regulations and guidelines, the CSL makes progress by addressing many specific privacy aspects such as access, data retention, breach notification, mobile privacy, online fraud, and the protection of the privacy of minors. For example, individuals, for the first time, are given the right to request the deletion of their personal data. All network operators are required to preserve network logs for at least six months, and to report upon discovery any security defect, loophole, or other security risks found in their products or services to the relevant authorities and affected individuals. Instant messaging service providers, like any other traditional network service providers, must require users to register using their real identity information. Individuals and organisations are prohibited from establishing "websites or communication groups used to carry out fraud, to pass on criminal methods, to produce or sell contraband or controlled items and to engage in any other illegal criminal activities" or to publish information relating to such activities online. General principles have been added in the third draft for the protection of minors online, serving as a basis for developing further laws and regulations.

While we are expecting additional guidelines to be issued or precedents to develop to clarify some of the key requirements such as the scope of the CIIs, data localisation and cross-border transfers, for now in-house counsel are advised to take a proactive approach by conducting a compliance risk assessment with the aid of qualified privacy professionals, and possibly a comprehensive privacy and security audit of their Chinese operations to determine the best way to stay "within the law". China is now clearly becoming a jurisdiction that will require extra resources to devise the right solutions that do not jeopardise the day to day operations of international business with a presence there.

Contact Us

For enquiries related to this Legal Update, please contact the following persons or your usual contact at our firm.

Gabriela Kennedy
Partner
T: +852 2843 2380
E: gabriela.kennedy@mayerbrownjsm.com

Xiaoyan Zhang
Counsel, (New York, USA)
T: +852 2843 2209
E: xiaoyan.zhang@mayerbrownjsm.com