COVINGTON

China Releases Second Draft of Cybersecurity Law

July 12, 2016
Data Privacy and Cybersecurity

On July 5, 2016, China's National People's Congress ("NPC") released a new draft of the *Cybersecurity Law* for public comment (official Chinese version available here; unofficial translation from AmCham China available here). The revised draft contains a number of significant changes from the first draft, which was released in July 2015, but retains many of the provisions from the first draft that raised concerns among multinational companies, especially those in the tech sector, about the potential to serve as a tool for discriminating against foreign technologies in favor of domestic industry.

Public comments on this new draft can be submitted to the National People's Congress by August 4, 2016. Our analysis of the first draft of the *Cybersecurity Law* can be found in our alert on the topic here.

This alert examines some of the changes found in the new draft:

- **Multi-Level Classification System for Network Security Protection.** The new draft of the law maintains language calling for a multi-level classification system with differentiated security requirements for all information networks in China, based on their degree of importance/risk from a cybersecurity perspective. Although the draft does not provide details regarding this new scheme, it is likely to be similar to the "Multi-Level Protection Scheme," a multi-level system set out under the 2007 *Information Security Multi-Level Protection Administrative Measures* that classifies information systems on a five-point scale and imposes different cybersecurity requirements based on the classification. The new draft of the *Cybersecurity Law* adds language linking the protection of "critical information infrastructure" (see discussion below) with the new multi-level system, indicating that "critical information infrastructure," which would cover sectors of strategic importance, would be subject to enhanced protection under that system.

- **Critical Information Infrastructure.** The new draft replaces the definition of the term "critical information infrastructure" -- the first draft made specific reference to a number of sectors such as financial services, transportation, and agriculture, with a catch-all covering "networks and systems owned or managed by network service providers with a large number of users" -- with a broadly worded alternative: "Infrastructure that, in the event of damage, loss of function, or data leak, might seriously endanger national security, national welfare and the people's livelihoods, or the public interest." The scope of coverage would be determined separately by a regulation to be drafted by the State Council. Network operators that are not responsible for critical information infrastructure would be encouraged to voluntarily join in the protection of such infrastructure.

- **Data Localization.** The original draft would have required operators of critical information infrastructure to store within China all "important data" collected or generated during business operations. The new draft changes "citizens' personal information and other important data" to "citizens' personal information and important

business data." As with the previous term "important data," the new term "important business data" remains undefined. Additionally, the new draft narrows the scope of data subject to this localization requirement to only data that is collected or generated within China.

Furthermore, the original draft mitigated its data localization requirement somewhat by stating that, if there were a business need, operators could "store abroad or provide to organizations or individuals located abroad" data subject to the localization requirement on the condition that it passed an unspecified security assessment. That language has since been changed in the new draft to merely "provide abroad." It is unclear whether this represents a substantive change, or simply reflects a view on the part of the drafters that "storage abroad" is a subset of "provision abroad."

- **"Secure and Reliable" Standard**. The new draft adds "promotion of secure and reliable network products and services" to a list of areas in which governments at or above the provincial level should make plans and increase support No further guidance is provided as to what would be considered "secure and reliable," but the phrase resembles the term "secure and controllable," which appears in rules (and draft rules) issued by agencies such as the China Banking Regulatory Commission and China Insurance Regulatory Commission and has raised concerns among non-Chinese technology companies and their customers in China.

- **Data Retention Requirement.** The new draft law would require all network operators to preserve network logs for at least six months, and to report upon discovery any security defect, loophole, or other risk found in their products or services to the relevant authorities (in addition to users).

- **Real-Name Registration.** The new draft law adds instant messaging service providers to the list of types of service providers that must require users to register using real identity information. The other types of service providers (already listed in the original draft) are providers of Internet access, domain registration, landline or mobile phone network access, and information publication.

- **Data Protection & Breach Notifications.** The new draft modifies language about data protection. According to the updated language, network operators may not disclose, tamper with, or damage citizens' personal information they have collected, and they may not provide citizens' personal information to others without consent. Irreversibly de-identified personal information is exempted from these rules.

  The new draft clarifies that the law's breach notification requirements apply only to breaches involving personal information.

- **Investigative Powers**. Chinese authorities would, under new draft language, have the power to compel an interview of the legal representative or other key individuals associated with a network operator in the case of a network security incident or relatively large security risk.

- **Penalties.** The new draft would require that violations of the law be included in the credit history of violating entities and individuals and 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.

- **Social Responsibility & Supervision.** The new draft adds general language regarding the need for network operators to comply with social and business ethics, assume social responsibility, accept government and public supervision, and cooperate with government inspections.

- **Promotion of Network Security Technologies and Services**. According to the new draft, the State would encourage enterprises to provide services related to network security certification, testing, and risk assessment. It would also encourage the development of technologies related to network data security protection and utilization, promote the opening of public data resources, and support innovation in network security management.

In China's legislative process, new laws usually require three "readings" in the National People's Congress before they are formally passed. The period before the second and third readings can be as short as a few months, and the third reading often does not include a public comment period. Therefore, companies that may be affected by this law's implementation are advised to pay close attention to this draft and take advantage of this potentially final opportunity to formally provide comments.

* * *

Those interested in learning more about the new draft *Cybersecurity Law* may contact the following members our Covington China team:

Tim Stratford (Beijing)	+86 10 5910 0508	tstratford@cov.com
Eric Carlson (Shanghai)	+86 21 6036 2503	ecarlson@cov.com
Yan Luo (Beijing)	+86 10 5910 0516	yluo@cov.com
Ashwin Kaja (Beijing)	+86 10 5910 0506	akaja@cov.com