COVINGTON

China Passes New Cybersecurity Law

November 8, 2016

Data Privacy and Cybersecurity

On November 7, the Standing Committee of China's National People's Congress ("NPC") passed China's first Cybersecurity Law (the "Law"), which will take effect starting June 1, 2017.

Described as China's "fundamental law" in the area of cybersecurity, the new Law articulates the government's priorities with respect to "cyberspace sovereignty," consolidates existing network security-related requirements (covering both cyber and physical aspects of networks), and grants government agencies greater power to regulate cyber activities. It is the first Chinese law that systematically lays out the regulatory requirements on cybersecurity, subjecting many previously under-regulated or unregulated activities in cyberspace to government scrutiny. At the same time, it seeks to balance the dual goals of enhancing cybersecurity and developing China's digital economy, which relies heavily on the free flow of data.

With its broad application, the new Law will have significant and long-lasting implications for companies operating in China or seeking to access the Chinese market. This alert highlights key features of the Law and explains these implications.

Legislative Overview

Prior to the Law's formal adoption, the NPC released two previous drafts for public comment—the first in July 2015, and the second in July 2016 (see the Covington alerts on these drafts here and here, respectively).

The final version of the Law contains seven chapters and 79 articles.

- Chapters 1 and 2 discuss general principles and the government's cybersecurity strategy, respectively.
- Chapter 3 sets out (i) the cybersecurity obligations applicable to network operators based on their classification under the Multi-level Network Security Protection Scheme, (ii) requirements with which providers of network products and services must comply, and (iii) the definition of Critical Information Infrastructure ("CII") and specific obligations applicable to CII operators.
- Chapter 4 addresses information security issues, focusing on data privacy, cybercrimes (covering online fraud, installation of malware, and dissemination of unlawful information), and the establishment of a system for reporting bad behavior.
- Chapter 5 covers network monitoring along with emergency response and handling.
- Chapter 6 provides the penalties for violation of network security rules.
- Chapter 7 includes definitions and other supplementary provisions.

Key Highlights

In announcing its passage, NPC officials highlighted the following key aspects of the Law:

Principle of Cyberspace Sovereignty

China has been a vocal proponent of "cyberspace sovereignty," the theory that states have the power to regulate the Internet within their borders. The Law is, in part, motivated by a desire to create a framework for exercising such sovereignty and echoes President Xi Jinping's recent speech on cyberpower strategy, which calls for the development of secure and controllable technologies to enhance cybersecurity.

Security Obligations of Network Operators and Providers of Network Products and Services

The new Law imposes specific cybersecurity obligations on network operators, as well as on providers of network products and services. Network operators are generally obligated to safeguard their networks against disruption, damage or unauthorized access, and to prevent data leakage, theft or tampering, and they will also be subject to specific rules depending on their classification under the Multi-level Network Security Protection Scheme. Providers of network products and services must comply with certain Chinese "national standards" and ensure the security of their products. Those products deemed "Critical Network Equipment and Network Security Products" must be tested by accredited evaluation centers before being marketed in China, and the government is contemplating issuing a comprehensive catalogue of approved products.

Protection of Personal Information

The new Law imposes certain data protection obligations on network operators. For example, network operators may not disclose, tamper with, or damage citizens' personal information that they have collected, and they are obligated to delete unlawfully collected information and to amend incorrect information. Moreover, they may not provide citizens' personal information to others without consent. Exempted from these rules is information irreversibly processed to preclude identification of specific individuals. Also, the new Law imposes breach notification requirements that will apply to breaches involving personal information.

Protection of Critical Information Infrastructure (CII)

The new Law applies the most stringent cybersecurity rules to operators of CII and their suppliers. CII is defined broadly as "infrastructure that, in the event of damage, loss of function, or data leak, might seriously endanger national security, national welfare or the livelihoods of the people, or the public interest," and specific reference is made to "key sectors" such as telecommunications, financial services, transportation, and e-government.

In addition to having to comply with cybersecurity requirements applicable generally to network operators, CII operators are also required to sign security and confidentiality agreements with their suppliers when procuring "network products and services." If products and services that the operators procure "may affect national security," the operators are required to ensure that such products or services have undergone a "national security review."

Cross-Border Transfer of Data

Operators of CII must store within Chinese territory "citizens' personal information and important business data" collected or generated in the course of operations within the country. If transfers of data offshore are necessary for operational reasons, a security assessment must be conducted by designated agencies.

Specific Penalties for Foreign Offenders

In addition to the usual penalties for non-compliance (*e.g.*, warnings, suspension of operations, revocation of licenses, fines set within a fixed range), the new Law provides for specific penalties such as the freezing of assets or other sanctions that would be applicable to foreign organizations and individuals that attack any CII in China.

Network Interoperability and Standardization

The new Law promotes the interoperability of network infrastructures and encourages enterprises, institutions and universities to participate in the formulation of network security standards. While this development could enhance cybersecurity, questions remain about whether the scope of interoperability will be broad enough to encompass and ensure compatibility with international standards. It is uncertain at this stage whether China will adopt domestic standards compatible with international standards, or instead establish its own homegrown standards in an attempt to develop its own cyber ecosystem.

Online Protection of Minors

The new Law also sets forth general principles for the online protection of minors, intended to provide a basis for developing ancillary laws and regulations on the subject. This is in line with efforts by the Cyberspace Administration of China ("CAC"), the key agency tasked with implementing the new Law, which recently issued a draft regulation on the protection of minors in cyberspace. See our note on that draft regulation here.

Key Developments in the Final Version

In comparison with the second draft, which was released for public comment last year, the final version of the Law includes a more specific definition of CII, which restores language referencing a number of key sectors. It also imposes new penalties directed at foreign individuals or organizations attacking Chinese CII and increases punishments for online fraud and other new forms of cybercrime. Finally, it promotes network interoperability and standardization and adds new provisions addressing the online protection of minors.

Potential Implications

Companies operating in China or seeking to access the Chinese market should take steps to evaluate how the new Law might impact their operations through exercises such as cybersecurity compliance audits or gap analyses. Meanwhile, as the CAC is expected to roll out implementing regulations on its own, or in conjunction with other agencies over the next six months, companies are advised to pay close attention to those developments and potentially take advantage of opportunities to proactively provide inputs to regulators.

Those interested in learning more about the Cybersecurity Law may contact the following members of the Covington China team:

Tim Stratford	+86 10 5910 0508	tstratford@cov.com
Eric Carlson	+86 21 6036 2503	ecarlson@cov.com
Grace Chen	+86 10 5910 0517	gchen@cov.com
Yan Luo	+86 10 5910 0516	yluo@cov.com
Ashwin Kaja	+86 10 5910 0506	akaja@cov.com