SQUIRE PATTON BOGGS

New Comprehensive Chinese Cybersecurity Law Approved

On November 7, 2016, the Standing Committee of the National People's Congress approved the new *Cybersecurity Law*. The law, which contains 79 articles under eight chapters, is set to take effect in June 2017 and has wide-ranging implications for how companies in China handle personal data and cybersecurity issues. The law applies broadly to entities or individuals that construct, operate, maintain, and use networks within China, as well as those who are responsible for supervising and managing network security. An unofficial English translation can be found online.

Background

Following the Snowden revelations and various international cyber-hacking disputes, in July 2015, China released a draft of the proposed law and provided a period for public comment. A number of foreign companies and associations raised concerns about provisions in the bill, which gives far-reaching regulatory oversight and enforcement authority over cybersecurity and information infrastructure to the Chinese government, based on "cyberspace sovereignty" (Article 1), and broadly-defined national security interests (Article 28).

The new law, which includes many of the controversial aspects of the draft law, sets out a comprehensive framework that essentially legalizes and expands upon current practices, policies and laws that regulate and control all information flows online and offline. Further guidance is expected to clarify the scope and application of the law. The law provides that industry organizations will further establish "mechanisms for regulation and coordination of network security" (Article 29). The law further indicates that the state council will outline a "tiered protection system" for "critical information infrastructure" (Article 31), setting forth some basic requirements, including mandating background checks for responsible personnel and network training for employees (Article 34).

Oversight, Regulation and Enforcement

Government oversight and enforcement is broadly worded but the law requires companies to "accept supervision from the government and public" (Article 9). The law gives authority to the government over "monitoring, preventing, and handling network security risks and threats" in an effort to protect "critical information infrastructure against attacks, intrusions, interference and destruction" (Article 5). In addition, it calls for network operators to "obey social morals and commercial ethics" but does not define those terms (Article 9).

The law sets forth the protocols for China's network information departments, for example, that they have systems in place to identify early warning signs of network security incidents (Chapter 5). And in relation to major security incidents, information departments "may take temporary measures regarding network communications in certain regions, such as restricting it" (Article 58).

Responsibilities on networks service providers and operators:

- **Data Localization** – The law requires critical information infrastructure operators to store personal and business data gathered or produced during operations in China on servers **within mainland China** (Article 37). "Where due to business requirements it is truly necessary to provide it outside the mainland, they shall follow the measures jointly formulated by the state network information departments and the relevant departments of the state council to conduct a security assessment; but where laws and administrative regulations provide otherwise, follow those provisions."

  "Critical information infrastructure" is defined to mean "public communication and information services, power, traffic, water, finance, public service, electronic governance and other critical information infrastructure that, if destroyed, or if it lost function or leaked data, might seriously endanger national security, national welfare and the people's livelihood, or the public interest, on the basis of their tiered protection system." The specific scope and protection mechanism will be published in the future by the state council (Article 31). "Personal data" is defined as information that can be used to identify a person's identity, including but not limited to a person's full name, date of birth, government identification number, personal biometric information, addresses and telephone number (Article 76).

- **Responsibilities on processing and retention of personal data** – The new law sets out various data privacy requirements including personal data confidentiality (Article 40, 41). The law requires a data subject's direct consent for the use of personal data (Article 42), and recognizes a data subject's "right to be forgotten," i.e., a right of users to request the network operators delete their personal information (Article 43).

- **Security reviews and certification** – Companies operating in China will now be required to undergo security reviews, cooperate with investigations by security agencies in the country, and provide investigators full access to data in criminal cases. Although such requirements are scattered across various regulations and have been enforced for years, this is the first time that this position has been affirmed in the highest level of legislation. The law also imposes certification requirements to sell computer equipment and will only allow technology deemed to be secure (Article 23). Foreign companies have argued this provision will give a competitive advantage to domestic companies, and could require companies to disclose intellectual property, such as source coding.
- **Protection of cybersecurity** – The law identifies steps that network operators must take to ensure network security and data protection. That includes a provision requiring companies to implement international security systems and protocols, appoint a person responsible for network security, adopt technical measures to prevent attacks and viruses and establish emergency response plans, among others (Articles 10, 21 and 25).
- **Data breach** – The law requires that companies and network operators develop network security incident emergency response plans, periodically organize drills in relation to such plans, and report "security incidents" to the government and inform consumers of data breaches (Articles 51-58).

Responsibilities of Network Users

- The law requires that network users "must not endanger network security, and must not use the network to engage in activities endangering national security, national honor and interests, inciting subversion of national sovereignty, the overturn of the socialist system, inciting separatism, undermining national unity, advocating terrorism or extremism, inciting ethnic hatred and ethnic discrimination, disseminating violent, obscene or sexual information, creating or disseminating false information to disrupt the economic or social order, as well as infringing on the reputation, privacy, intellectual property or other lawful rights and interests of others, and other such acts" (Articles 12, 14).

Noncompliance Penalties

Chapter VI of the law sets out various fines for non-compliance. For example, it lists separate fines associated with failing to require users to provide truthful identity information, failing to undertake network security certifications and failing to implement data localization. Fines generally range from RMB 10,000 to RMB 1 million, but where circumstances are serious, the government can detain the responsible parties for between five and 15 days. Where there are unlawful gains, officials can confiscate them and give a fine of between one and 10 times the amount of the unlawful gains. Additionally, the government may revoke business licenses in more serious cases, and in certain circumstances civil claims may be asserted.

It is expected that the government will further clarify how the new Cybersecurity Law will be enforced, including how approval will be obtained for the cybersecurity of devices sold in China. What is clear is that there will be far-reaching effects for any company that has operations or customers in China, not the least of which will involve having local servers in China for critical information infrastructure and data policies in place in compliance with the new law.

Contacts

Gretchen A. Ramos
Partner, San Francisco
T +1 415 743 2576
E gretchen.ramos@squirepb.com

Scott Warren
Partner, Tokyo
T +81 3 5774 1800
E scott.warren@squirepb.com

Ju (Lindsay) Zhu
T +86 21 6103 6303
E lindsay.zhu@squirepb.com

The contents of this update are not intended to serve as legal advice related to individual situations or as legal opinions concerning such situations nor should they be considered a substitute for taking legal advice.

© Squire Patton Boggs.

All Rights Reserved 2016