PUBLICATION

What In-House Counsel Need to Know About China's New Cybersecurity Law

November 15, 2016

On November 7, 2016, the Chinese government ratified a new cybersecurity law that provides a legal basis for a wide range of matters including personal privacy, electronic communication, requirements on technology companies operating in China, data-localization and sanctions for violations of the law. The new law goes into effect on June 1, 2017. While this leaves relatively little time for the business community to decide how to react and comply, China circulated earlier drafts of the law for public comment during the last year – reportedly a step that China had not taken with any previous law.

What the Cybersecurity Law Provides

The scope of the new law is broad. It "applies with respect to the construction, operation, maintenance and usage of networks, as well as network security supervision and management within the mainland territory of the People's Republic of China."[1] The law thus appears to govern any business that relies on computer networks in China.

Regarding the collection and use of personal information, the new law prohibits "network operators" from providing a data subject's personal information to third parties without the data subject's consent (unless the information is anonymized and does not identify particular individuals). If personal data is released, the network operator must promptly inform affected users and the authorities. A data subject may also request a network operator to delete personal information from a computer system if he or she discovers that collection or use of the information violates the law or a contract between the parties. A data subject may likewise request a network operator to correct any personal information that is inaccurate.

The new law also places additional obligations on network operators. For example, network operators must provide technical support and assistance to the government when it is investigating a crime. They, moreover, are required to adopt technical measures to monitor and record their network operations, and to preserve related web logs for at least six months. Further, they must report "network security incidents" to the government.

The new law singles-out "critical information infrastructure" for special treatment. This term refers to information maintained by certain industry sectors that, if destroyed or damaged, "might seriously endanger national security, national welfare and the people's livelihood, or the public interest." The relevant industry sectors include public communication and information services, energy, transportation, water resources utilization, finance, public service and e-government affairs, and others.

Operators of critical information infrastructures are also subject to a data-localization requirement, under which they must retain, within the territory of China, critical and personal information which they collect and produce during their operations in China. While such information may be transferred outside of China, it must first undergo a security review. Overseas entities or individuals that attack, invade, interfere with or destroy critical information infrastructure in China are subject to fines, and public security agencies in China may adopt sanctions against them, including asset freezing.

Operators of critical information infrastructure are further required to undergo a network safety assessment at least once a year. In addition, when such operators procure network products or services that may affect national security, a national security inspection is required. The broad scope of critical information infrastructure companies, coupled with these inspection requirements, has reportedly raised concerns among non-Chinese businesses that they will be forced to disclose their source code and other corporate secrets to the Chinese government to prove their equipment is secure.

Our View

How the new law ultimately will impact the international business community remains to be seen. Significant aspects of the law, such as the scope and content of mandatory inspections, require the Chinese authorities to promulgate implementing regulations. That being said, any company doing, or considering doing, business in China should consult experienced counsel about the implications of the new law, and developments concerning the law must be watched carefully over the next several months.

---

[1]An unofficial translation of the law is available at http://chinalawtranslate.com/cybersecuritylaw/?lang=en