ANDERSON KILL
ATTORNEYS AND COUNSELORS AT LAW

AN OVERVIEW OF CHINA'S NEW CYBERSECURITY LAW

By: Eric W. Huang*

China's new Cybersecurity Law, effective on June 1, 2017, was adopted at the 12th People's Republic of China National People's Congress. Before this statute was formally enacted, China already had some administrative rules and regulations in place to govern data and privacy protection. However, the enactment of the new Cybersecurity Law is a good indication that China is now focusing more attention on these priorities.

Before delving into the details of the new Cybersecurity Law, it is important to have a general picture of the unique data and privacy protection legal system in China. Unlike the U.S. and many developed countries in the world, China did not have a series of uniform data and privacy protection laws before the new Cybersecurity Law became effective.

The new law integrates cybersecurity, data and privacy protection into different industrial regulatory laws -- for example, the Postal Law, the Commercial Banking Law, the Practicing Lawyers Law, the Medical Practitioners Law, and the Provisions on Protecting the Personal Information of Telecommunication and Internet Users. Moreover, the Chinese government does not have a special authority to enforce its data and privacy protections. Companies or individuals can only seek enforcement and remedies in front of tribunals.

Due to the lack of centralized laws and authority protection, it can be complicated and difficult to take action or seek uniform legal guidance on data and privacy infringement in China, especially for those foreign companies not familiar with the Chinese judicial system and business environment. Although the new Cybersecurity Law is not a centralized law that regulates all aspects of data and privacy protection across all businesses, it gives clearer legal guidance on the issues related to cybersecurity and privacy protection in China.

Broad categories of "service providers" affected

Unlike the US, China is a civil law country, which means all the laws are codified statutory laws -- case law has little influence. The new Cybersecurity Law does not apply to all companies, but the key provisions apply to two major types of service providers – the "network operator" and the "operator of critical information infrastructure." The law has very broad definitions for these two categories, and the absence of common law interpretation affords the government and authorities a wide range of discretion in real practice.

The term "network operator" includes owners, administrators and service providers of networks. This term may capture any companies that maintain computer networks to operate businesses or provide services in China. The term "operator of critical information infrastructure" applies generally to those who provide

> public communications and information services, energy, finance, transportation, water conservation, public services and e-governance, as well as other critical information infrastructure that could cause serious damage to national security, the national economy and public interest if destroyed, functionality is lost or data is leaked.[1]

Even companies headquartered outside China that use a network to manage business within the territory of China may fall within these broad definitions. As in the U.S., the Chinese government claims the right of final interpretation on what services, if compromised, may damage national security, economy and public interests,

[1] Article 31

***Eric W. Huang is** an attorney in the New York office of Anderson Kill and a member of the Corporate and Securities Group. Mr. Huang has a particular focus on advising and assisting Chinese businesses in the U.S. market, and U.S. businesses in the Chinese market. His practice encompasses a broad range of matters involving international business, including mergers and acquisitions, corporate financing and compliance. He has relationships with major law firms in China and counsels clients in both the U.S. and China. Mr. Huang can be reached at (212) 278-1255 or ehuang@andersonkill.com.

and this is going to be decided on the basis of case-by-case analysis.

Responsibilities under the new law

The Cybersecurity Law identifies the responsibilities of network operators and operators of critical information to safeguard infrastructure. A network operator is required to follow certain privacy safeguard procedures to protect networks from interference, destruction or unauthorized access, and to prevent network data from being leaked, tampered with or stolen.[2] An operator of critical information infrastructure has to store "personal information" and "important data" within China, unless the business passes the government security assessment. This means that if some companies need to transmit data to their overseas affiliates, they will have to restructure their mechanisms regarding data transfer, in order to avoid violation of the data localization requirements under the new law. This requirement reflects the tendency of the Chinese government to put more emphasis on localizations of business and personal data.

Other requirements in the Cybersecurity Law

In addition to the data localization requirements, the Cybersecurity Law addresses other key aspects of cybersecurity and privacy protection.

Cybersecurity Protection

- Critical information infrastructure operators that purchase network products and services that might affect national security must pass a national security review. Critical network equipment and special cybersecurity products can only be sold or provided after being certified by a qualified establishment and found to be in compliance with national standards.[3]
- Network operators are required to clarify responsibilities within their organizations, and ensure network security by implementing sound internal security protocols, appropriate technological measures and reporting processes.[4]

Privacy Protection

- Network operators are required to give notice and obtain consent before collecting personal information.[5] The personal information can only be collected in a legal and proper manner.[6]
- Network operators must gather and store personal information under the requirements of law, administrative regulations and agreements with users. If the operator violates the provisions of law or regulations, an individual has the right to request that the operator delete the collected personal data.[7]
- Network operators have responsibilities for cybersecurity supervision and shall maintain the confidentiality of all personal information. Operators shall not disclose, tamper or destroy personal data.[8]

Penalties

The Cybersecurity Law establishes different categories and different levels of penalties, including monetary, administrative and criminal penalties. For example, violators of the data localization requirement will face fines of around $7,700 to $77,000. Individuals can also be subject to penalty: personal violations may face fines about $1,500 to $15,000. The maximum fine is around $155,000.[9] The Chinese government is authorized to issue warnings, suspend business licenses or permits, or block websites.

Conclusion

The Cybersecurity Law establishes a range of new responsibilities for broadly defined categories of network service providers and operators. Some of those new responsibilities may reach companies not domiciled in China that do business in China.

The enforcement of the new law may prove arbitrary in some cases due to the wide discretion invested in the authorities by the law's broadly defined terms. Application and interpretation of the law going forward requires close monitoring by all entities that maintain a presence in the country or serve the Chinese people.

[2] Article 21
[3] Article 35 and Article 23
[4] Article 21 and Article 49
[5] Article 22 and Article 41
[6] Article 41 and Article 44
[7] Article 41 and Article 43
[8] Article 45 and Article 42
[9] Article 66

About Anderson Kill

Anderson Kill was founded in 1969 on the principles of integrity, excellence in the practice of law, and straightforward solutions to complex legal issues. The firm's attorneys approach engagements aggressively, and have earned a reputation for combining corporate polish with pugnacity. Based in New York City, the firm also has offices in Philadelphia, PA, Stamford, CT, Washington, DC, Newark, NJ and Los Angeles, CA, but the attorneys travel around the country and around the world to handle all types of matters. Anderson Kill attorneys work together, leveraging creativity and legal and business acumen to deliver cost-effective resolutions to clients' problems. Many of the firm's professionals are recognized experts in their practice areas, leaders and active participants in professional associations, and are frequently invited to speak to business organizations.

Anderson Kill clients include some of the nation's largest public and private entities, including companies in financial services, retail, oil/gas, telecommunications, construction, food supply, technology, pharmaceutical and life sciences, and utilities, municipalities and state governments, religious and not-for-profit organizations, small companies and individuals. Anderson Kill prides itself on attracting and retaining intelligent, personable and well-rounded attorneys. Smart attorneys with sharp skills, excellent client service, and a track record to prove it: that is the Anderson Kill difference.