Overview of China Cyber Security Law and Implications on Foreign Companies

Description

China Cyber Security Law ("**CCSL**") has been enacted and took effect (since June 1, 2017) for some time prompting many multinational companies to review and revise their internet policies and take actions to comply with the new law which has profound and far-reaching impact on their business operation in China.

I. Overview of China Cyber Security Law

(1) What and Whom CCSL is Intended to Regulate

Article 2 of China Cyber Security Law gives the answer:

> The construction, operation, maintenance and use of networks within the territories of the People's Republic of China shall be subject to this Law.

Naturally you would like to know what definition is given to the concept of "network". Here it is in Article 76 of CCSL:

> A network refers to any system that is comprised of computers or other information terminals and relevant equipments that collect, store, transmit, exchange and process information in accordance with certain protocols and programs.

The definition of network is very general and vague and potentially can be interpreted to encompass any connecting devices such as telecommunication network, internet, mobile networks and the like. It definitely refers to network accessible by the public and can also include intranet operated by a certain organization within itself.

Throughout the China Cyber Security Law, another frequently used key legal concept is "network operators" which is defined in Article 76 as well:

> A network operator refers to the owners, administrators of networks as well as network service provider.

The Law doesn't further define what a network service provider is, and in Article 10 of this Law, it uses the wording "provide services through network" which is supposed to mean "network service provider", thus rendering the concept of "network providers" able to cover not only technical companies such as anti-virus firms, internet companies such as Yahoo!, or internet platform companies such as Alibaba but also those traditional consumer product companies that have come to utilize internet to sell their products

(2) Major Aspects of Cyber Security

Basically, China Cyber Security Law focuses on three aspects of cyber security practice:

(a) the security for the network operation/running, in other words, ther security of networking itself.

The law mandates a system of multi-level/graded protection of network security whereby multiple layered obligations in terms of onerousness will be set out for different types of network facilities. The grading of protection of network security has yet to be formulated and promulgated later on.

The law further provides that network products and services shall be in compliance with the national compulsory standards and their providers of the same shall not contain any malicious programs. Furthermore, certain critical network equipments and specialized cyber security products shall be certified as qualified up to compulsory standards before they are sold or provided in the market. A List of such critical network equipments and special products has been announced already.

Most importantly, the law requires networks in certain industries and economic sectors to be designated as critical/key information infrastructure that will greater protection in addition to the graded protection discussed above. What makes this most important is that the law requires the personal information and important data collected by the operators of the key information infrastructures in its operation within China to be stored in China. In other words, foreign companies that operate key information infrastructures shall store those personal information and important data in a server located in China. Indeed, big players such as Apple has already moved its data storing server into China.

(b) Security of Network Information

This is aimed to protect the personal information from being misused by network operators.

In Article 41, the law provides that:

> The collection and use by network operators of personal information shall be conducted in the principles of legitimacy, justification and necessity and subject to the consent of the person whose information is being collected, and rules for such collection and use shall be made public, and the purpose, manners and scope for collecting and using the information shall be made aware.
>
> Network operators shall not collect personal information that is not in any way related to the services they provide, and shall not collect and use personal information in violation of laws and administrative regulations and the agreements between the parties, and shall process the personal information they store in accordance with laws and administrative regulations and the agreement between the parties.

This is the fundamental legal framework established by China Cyber Security Law for purpose of protecting personal information. In furtherance of this objective, the law has prescribed other specific measures such as requiring network operators not to divulge, tamper with, or damage personal information, not to provide the same to others (unless de-identification work is done), setting up internal regime for entertaining users' complaint, requests etc.

(c) Monitoring, pre-warning and emergency response

Here the law requires that the state shall establish the network security monitoring and pre-warning system and information sharing system and publish such monitoring and pre-warning information.

Government agencies (generally the police offices) responsible for network security can summon the legal representative or person-in-charge for talk if they find substantial network security risk or in the case of security incidents.

II. Actions to be Taken by Foreign Companies Operating Business in China

In today's world, due to China's position as the world's second largest economy and due to the internet eliminating borders that otherwise limits business operation, big companies in foreign countries may have already been engaged in business operation or activities in China, and it is important for them to understand the legal implications to them or their business operation. In particular, manufactures or sellers of world luxury goods that have been targeting Chinese buyers for long should given particular attention to this cyber security law. Indeed, our team has been retained by one of those big companies in helping them to comply with this law.

If you have already set up your manufacturing facilities or points of sale in this country, then you definitely need to review what and how much you need to do to ensure your compliance with this law.

But for those companies that are not registered or incorporated within China, and may not have their business entity set up in China, but may be doing business with Chinese people or involve China in its business operation one way or another, things can be murky.

The key factor in making a correct determination therefor much depends on whether they will be considered as having domestic operation.

If a foreign company conducts its business within China or provides products or services into China, then it will be considered as conducing domestic operation. According to one of the draft implementing regulation, following factors will be taken into account when determining whether a network operator has domestic operation: use of Chinese language (the website), trade settlement in RMB (Chinese currency), and goods dispatched into China.

If the foreign company collects personal information during its domestic operation, then despite that their network (computers, servers) is outside of China, it will also be caught by China Cyber Security Law.

As indicated above, there will be more implementing regulations to be issued by the government soon, and some of the drafts are already published for comments. We will keep you updated about those developments.

Date Created
March 17, 2018
Author
admin