Legal Update – China Desk **November 2016**

*

China Adopts Cybersecurity Law

Please visit us:

www.fbclawyers.com

Dear Clients and Colleagues,

On November 7, 2016, the Standing Committee of the National People's Congress (NPC) of China passed the Cybersecurity Law (the "Law"), which will become effective as of June 1, 2017. As the basic law on cybersecurity regulation, the Law touches on the national policy of cyber industry, obligations of network operators, protection of data and personal information, and penalties for noncompliance. The first and second drafts of the Law were released respectively on June 2015 and June 2016, and the third on October 31, 2016, during which the *Law* had elicited extensive discussion among businesses. Below are certain key elements of the Law. An unofficial English translation of the Law can be found here.

A. Highlights of the Law

a. Regulatory bodies

The Law will be jointly administered by the Cyberspace Administration of China, the telecommunication authority, and the public security bureau.

b. When will the Law apply?

The Law applies to **"creation, operation, maintaining and use of networks within territory of China,** as well as supervision and administration of cybersecurity**"** (Article 2)**.** "Network" is defined as "system comprised of computers or other information terminals and related equipment, which collects, stores, transmits, exchanges and processes information following certain rules and programs" (Article 76).

- Based on the above two articles, the "creation, operation, maintaining and use of networks" regulated here shall take place within territory of China by virtue of some physically existing equipment, and in this regard the Law does not regulate **entities or individuals providing online services outside China** using facilities situated also outside China, even

though the service can be accessed in China—in this scenario, if the information from outside China is prohibited to be published or communicated within China, the transmission of this information into China would be blocked by relevant authorities (Article 50).

- **Network operator** refers to "owner and manager of network and **provider of service through network"** (Article 76), which could cover a vast variety of service providers.
- The application of the Law does not differentiate between Chinese and foreign individuals or companies, as long as they meet the relevant criteria mentioned in Article 2.

c. General obligations applying to all network operators

- Safeguarding network—"Multi-Level Protection Scheme for Cybersecurity"

  Network operators in general are obliged to safeguard their networks, and they shall follow the requirements of the "Multi-Level Protection Scheme for Cybersecurity". Specifically, they shall formulate internal security management rules, appoint a person in charge, take technology measures to prevent viruses and cyber-attacks, keep weblog for at least six months, classify, backup and encrypt data, etc. (Article 21).

  Prior to the Law, there exist other "multi-level" protection schemes implemented, for instance the "Multi-Level Protection Scheme for Information System", which uses different levels to classify IT systems and applies different requirements accordingly (e.g. some level asks companies to take assessment each year, some each half year, while some only asks filing for record). Whether the new "Scheme" in the Law will be in line with others in place is up to further clarification.

- Compliance with "**national standards**"

  Network products and services shall comply with mandatory requirements in "national standards"; in addition, "**critical network devices and products exclusively used for network security"** shall be tested by certified institutions proving their compliance with these requirements before made available to market (Articles 22, 23). (Catalogue of "critical network devices and products exclusively used for network security" will be later drafted by administrative authorities.) We will see how the new certification process coexists with the current permit-granting

system for sale of "products exclusively used for security of computer information system".

- Real name registration

  Network operators providing certain services, including instant messaging service, when entering into agreement or confirming provision of services with any user, shall ask for real identity information of such user.

- Network operators shall provide technology support and assistance for national security and criminal investigations.

d. Special obligations applying to operators of **Critical Information Infrastructure ("CII")**

- Definition of CII

  Certain information infrastructures which, once damaged, malfunction or infiltrated, might endanger national security, economy at large or public interest, shall be deemed CII, industries of which include and are not limited to public communication and information services, energy, transportation, water, finance, public services, e-government, etc. Further definition and protective measures are to be provided by the State Council (Article 31).

- Special obligations applying to operators of CII

  In addition to general obligations mentioned above, operators of CII shall meet extra requirements regarding employment, purchase of network products and services, data backup, etc. (Article 34), including data localization.

  - **Data localization (Article 37)**

    Personal information and important data collected and generated while operating CII within the territory of China shall be stored therein, and transfer of such information or data abroad shall be subject to security assessment. This is the first time data localization is required by a NPC passed law. "Personal information" refers to information that allows to be used, alone or in combination with other information, to identify a **natural person**, including and not limited to name, birth date, ID number, personal biometric information, address, phone number, etc. (Article 76).

e. Data and personal information protection

Provisions on data and personal information protection in the Law

follow rules already in force, including principles and rules on collection, storage, use and disposal of personal information.

- Consent of the user is required if network products or services could be used to collect information of users (Article 22). Network operators shall keep confidential the user information collected (Article 40). In these two articles, information of user is not necessarily personal information.
- Consent of the person to whom the information relates is required for collecting and using such personal information (Article 41).
- Leaking, altering, destroying and disclosing collected personal information without prior consent of the individual to whom the information relates, are prohibited, except that such information has already been processed and could not be used to identify individuals or be recovered to do so; network operators shall take measures to protect personal information, stop relevant violations through their networks, report to authorities such violations, etc. (Article 42).
- For individuals against network operators, **right to be deleted** when collection or use of personal information is illegal or falls outside their agreed scope, and **right to correct** when collected or stored personal information is not accurate (Article 43).

f. Penalties

Violations of the Law could lead to punishments from fines between 5,000 RMB (approx. 2,800 NIS) and 1 million RMB (approx. 0.56 million NIS) on companies, individuals or the person directly in charge or responsible for a violation in a company, to business being suspended or closed, detention of individual violators or person directly in charge or responsible for a violation in a company for up to fifteen days, etc. Company violators could also be fined for up to 10 times of illegal gains/amount of purchase price for certain violations. Assets freezing or other sanctions might be imposed on **entities or individuals outside China** which attack, break into, obstruct, or destroy CII of China and cause serious consequences.

B. Implications

As is common in Chinese legislation, the Law only provides general principles and rules, leaving details of implementation and enforcement to be supplemented in further explanatory regulations, such as regarding "Multi-Level Protection Scheme for Cybersecurity", criteria for CII,

preparation of national standards and relevant catalogue, security assessment of cross boarder data transfer, etc., which are expected to be gradually in place before the Law enters into effect in June 2017; some of the provisions are codification of previous regulations which do not create new obligations; in addition, the Law provides no obligation that only applies to foreign entities without applying to their Chinese peers. With that being said, it is clear that China is catching up on legislation and enforcement of cybersecurity and data protection.

IT firms thinking of expanding to the Chinese market or already have operations within China should pay close attention to follow-up regulations so as to fully understand the Law and keep business in compliance.

Sincerely,

Fischer Behar Chen Well Orion & Co.

For further information please feel free to contact:

Ms. Yue Gao ygao@fbclawyers.com +972.3.6944194