China's Cybersecurity Law: More Questions Asked than Answered

by Chris CAO

On November 7, 2016, the Standing Committee of the PRC's National People's Congress (NPC) adopted a new Cybersecurity Law (the "Law"), which shall come into effect on June 1, 2017. Although China has separate laws and regulations that touch on various cybersecurity issues, this is the very first comprehensive law on cybersecurity.

The Law is aimed at promoting network infrastructure construction and security, cyber-technology innovation, and so on[1]. It sets out requirements that impose a duty on "network operators" to develop firm-level security mechanisms.

Innovative requirements for network operators include:

- Multi-layered cybersecurity mechanisms[2];
- Confirmed user-name policies for several business sectors[3];
- Emergency response plans[4];
- Data localization[5];
- Feedback and reaction systems regarding personal data[6].

The Law also reiterates personal information protection and anti-abuse principles:

Image Courtesy of Nico Villanueva

> "When collecting or using personal information, network operators shall comply with the principles of legality, justification and necessity, publicize the rules for collection and use, clearly indicate the purposes, methods and scope of the information collection and use, and obtain the consent of those from whom the information is collected.
>
> A network operator shall not collect personal information irrelevant to the services it provides or collect or use the personal information in violation of the provisions of laws and administrative regulations and the agreements between both parties and shall process the personal information of citizens it has stored in accordance with the provisions of laws and administrative regulations and the agreements with the user."[7]

[1] Article 3, 4, 5 and 7 of the Law.
[2] Article 21 of the Law.
[3] Businesses include internet and telephone services, mobile phone services, blogs and blog-related businesses, and instant messaging services. See Article 24 of the Law.
[4] Article 25 of the Law.
[5] Article 37 of the Law.
[6] Article 43 and 49 of the Law.
[7] Article 41 of the Law.

Personal information leaks have plagued PRC citizens for several years. Consumer protection and reasonable use resonates with similar rules stated by the recently announced Draft of the Implementing Regulations for the Law on Consumer Rights and Interests Protection (the Draft)[8]. Though the use of someone's personal information should be done only with a person's consent, untraceable, anonymous personal information can be exploited without consent. This creates a safe harbor beneficial for the big data industry, which does not rely on identifying specific users, but instead studies consumption trends through metadata.

Data Localization

A coin has two sides. For all the innovations that are good news for end users, the other side of the coin raises serious concerns for businesses, especially multinational firms and FDIs. "Ostensibly designed to strengthen local networks against malicious hackers, in fact the bill looks very much like a techno-nationalist Trojan horse[,]" so stated an article in *The Economist*[9]. The problem is probably rooted in China's overvalued principle of "cyberspace sovereignty"[10]. Under this core value, the Law includes rules that practically hinder the free flow of bytes into and out of China, among which the most noteworthy is data localization. This obligation is on the shoulder of "critical information infrastructure operators" (CIIOs), as distinguished from "network operators" (NOs).

NOs are defined as "the owners and managers of networks and network service providers"[11]. Given that the scope of "network service" has not been expounded, NOs could cover several sectors. CIIOs are not explicitly defined, but it can be inferred from context that CIIOs are a subset of NOs that operate critical information infrastructures. "Personal information and important business data collected and generated in the operation of critical information infrastructure operators within the territory of the People's Republic of China shall be stored within the territory."[12] This means, if a business is categorized as having a "critical information infrastructure", then the firm running such a business would be regulated by the Law as to the inflow and outflow of its data collected from or generated in China. But the question of which business data is "important" is not specified. Besides, "critical information infrastructures" have too broad and vague of a spectrum, and are up to specification by the State Council[13]. As far as it can be reasonably inferred from the Law's text, public communication, information service, energy, communications and traffic, water conservation, finance, public services, and e-government affairs are all covered.

Before the Law, several regulations and ordinances were already in place for data localization. Credit rating[14], personal financial information[15], mapping[16], and online taxi booking service[17] data collected in China must be stored in China. Under the Law, China is

[8] This draft was announced by the State Administration for Industry and Commerce (SAIC), on behalf of the State Council to complete implementation of the Protection of Consumer Rights and Interests Law.

[9] The Noose Tightens, The Economist, November 12th, 2016.

[10] "This Law is formulated with a view to maintaining the network security, safeguarding the cyberspace sovereignty…" Article 1 of the Law.

[11] Article 76(3) of the Law.

[12] Article 37 of the Law.

[13] "The State shall carry out important protection of important industries and fields, such as public communication and information services, energy, communications, water conservation, finance, public services and e-government affairs, and the key information infrastructures that may endanger national security, people's livelihood and public interest in case of damage, function loss or data leakage on the basis of graded protection system for network security. The detailed scope of and security protection measures for the key information infrastructures shall be formulated by the State Council." Article 31 of the Law.

[14] Article 24 of Administrative Regulations on the Credit Rating Industry.

[15] Article 6 of Notice of the People's Bank of China on Improving Work Related to the Protection of Personal Financial Information by Financial Institutions of the Banking Industry.

[16] Article 34 of Regulations on Map Administration

[17] Article 27 of Interim Administrative Measures for the Business of Online Taxi Booking Services.

tightening its grip on data localization, which is very likely to inconvenience multinationals. Multinationals have a justifiable management need to pool employee data and store it in their head office, usually located outside of China. Security numbers, bank accounts, and credit ratings are typical employee data an HR department might keep. Falling into the coverage of data localization provided by the Law and other regulations and ordinances, such data should be kept only in servers located inside China. This will bring a new set of challenges to multinationals operating in China.

Multi-Layered Cybersecurity Mechanisms

Although multi-layered cybersecurity mechanisms have been seen in previous regulations and ordinances[18], the Law deals with it under a new concept of "graded protection system for cybersecurity"[19]. It is still unclear whether the Law replaces, takes precedence of, or consolidates it with the previous rules. But it is certain that the Law has set up different criteria for different NOs, and so is a questionable innovation. NOs, as set forth above, are in fact comprehensive. Whether enterprises and nonprofit organizations should be treated differently is unknown, and to be interpreted from the Law's text. High-level security measures are justifiably expected from conglomerates and tycoons like Alibaba. Companies should not count on a high level of security, as well as websites that share information on "non-mainstream" hobbies. There are different government registration schemes for for-profit and nonprofit organizations. For example, for-profit companies involved in internet content work should be granted an ICP license prior to incorporation, and non-profits just need to file with the relevant authorities for record[20].

Similar distinguishments are widely accepted in regulative practice[21].

Cooperation with Law Enforcement

NOs must provide technical support and assistance to public security organs and state security organs[22]. On the face of it, this clause conveys no additional requirements than to be a decent person. There is the worry, however, that police could arrive for a "talk". This tactic is especially popular with the TMT sector when regulating authorities want to strongarm large enterprises to do as they wish without bringing about lengthy statutory proceedings or investigative procedures.

Unfavorable Consequences

As a direct impact created by the Law, multinational firms and FDIs are saddled with onerous duties about data protection and use. As an indirect consequence, the Law builds up a barrier against market entrance for foreign companies engaged in information and communications technologies (ICT) because of the skewed duties imposed. Michael Clauss, Germany's ambassador to China, worries that "security rules might be used to pursue other aims" such as an industrial policy favoring Chinese companies, as reported by *The Economist*[23].

Notwithstanding the above-mentioned restrictions, it is still too early for foreign companies and FDIs who have business in China to feel nervous. As a rule of thumb, crackdowns by administration agencies are remote until there comes into effect an implementation regulation for the Law. Agencies are usually scrupulous about a new but ambiguously phrased law, especially if the law exerts a negative impact on foreign companies and FDIs. When it comes to data localization,

[18] See Article 9 of Regulations of the People's Republic of China for Safety Protection of Computer Information Systems, Administrative Measures for Hierarchical Protection of Information Security, and Administrative Measures for the Security Protection of Communication Networks

[19] Article 21 of the Law.

[20] Article 3 and 4 of Administrative Measures on Internet Information Services

[21] Administrative agencies have separate rules as to licensing aspects like culture, live show streaming, e-commerce, and so on.

[22] Article 28 of the Law.

[23] The Noose Tightens, The Economist, November 12th, 2016.

multinationals can fulfill the local storage requirements by making the data stay with their Chinese subsidiaries and branches while keeping access to the data via internet.

In general, enterprises looking forward to a market share in China need to localize in many aspects. An important measure is to hire savvy mainlanders granted with authority to deal with compliance and lobbies.

Authors:

Chris CAO, **Associate**
chris.cao@eigerlaw.com

DISCLAIMER

This publication is not intended to provide accurate information in regard to the subject matter covered. Readers entering into transaction on the basis of such information should seek additional, in-depth services of a competent professional advisor. Eiger, the author, consultant or general editor of this publication expressly disclaim all and any liability and responsibility to any person, whether a future client or mere reader of this publication or not, in respect of anything and of the consequences of anything, done or omitted to be done by any such person in reliance, whether wholly or partially, upon the whole or any part of the contents of this publication. This work is licensed under the Creative Commons Attribution-ShareAlike 3.0 Unported License. To view a copy of this license, please visit http://creativecommons.org/licenses/by-sa/3.0/.