Client Update
China Passes Network Security Law

NEW YORK
Jeremy Feigelson
jfeigelson@debevoise.com

Jim Pastore
jjpastore@debevoise.com

HONG KONG
Mark D. Johnson
mdjohnson@debevoise.com

SHANGHAI
Philip Rohlik
prohlik@debevoise.com

On November 7, 2016, the Standing Committee of the National People's Congress of China adopted the Network Security Law, which will come into force on June 1, 2017.[1] The country's first-ever law devoted solely to cyber-security:

- codifies a variety of cyber-crimes such as illegally obtaining or selling personal information,[2] disseminating malicious software or "prohibited information,"[3] and online fraud;[4]
- imposes obligations on "Network Operators" with regard to the protection of personal information, content monitoring for "prohibited information," and cooperation with the authorities;
- imposes additional data localization, data transfer restrictions, and cyber-security obligations on "Critical Information Infrastructure Operators"; and
- envisions pre-approval of "critical network equipment" and "specialized cyber-security products" and security screening for "network products or services."

Violations of the obligations and restrictions in the law can result in administrative penalties and fines, including suspension or revocation of a business license, as well as fines and other penalties for responsible persons.

---

1 National People's Congress of China, "Network Security Law of the People's Republic of China" [in Chinese: Wang Luo An Quan Fa], XinhuaNet (Nov.11, 2015), http://news.xinhuanet.com/legal/2016-11/07/c_1119867015.htm.

2 Network Security Law, Art. 44.

3 Network Security Law, Art. 48.

4 Network Security Law, Art. 46.

The scope and impact of the Network Security Law on multinational corporations will depend on additional implementing regulations further clarifying the vague terms in the law. As passed, however, the Network Security Law has the potential to severely restrict businesses' ability to transfer and store data abroad as well as restricting the availability of "critical network equipment" and "specialized cyber-security products" in China. These restrictions could require significant alterations or upgrades to existing or future IT infrastructure in China.

NETWORK OPERATORS

"Network Operators" are defined as "owners and managers of networks and network service providers."[5] Based on similar terms in other laws,[6] a "Network Operator" could include not only telecommunication operators and internet service providers, but also any provider of online information and services, including search engines, video websites, email service providers, e-commerce platforms, mobile messaging tools, social community operators, and websites of corporations and non-profit organizations.

Data Collection and Processing

The Network Security Law integrates scattered provisions of previous regulations[7] into a set of rules governing the collection of personal information[8] by Network Operators.

---

5 Network Security Law, Art. 76 (3).

6 For example, "Provisions on Technical Measures for the Internet Security Protection" (effective on Mar. 1, 2006), Art. 18, which states, "for the purposes of these Provisions, Internet service providers shall mean the organizations that provide users with Internet access services, Internet data center services, Internet information services, and Internet Web services." For another example, "Administrative Measures on Internet Information Services" (effective on Sep. 25, 2000), Arts. 2 & 3, which defines "Internet information service" to be "service activities of providing information to online users via the Internet," including both "profit-making" and "non-profit-making" Internet information services.

7 For example, Decision of the Standing Committee of the National People's Congress on Strengthening Network Information Protection (effective on Dec. 28, 2012), Art.7; Provisions on Protecting the Personal Information of Telecommunications and Internet Users (effective on Sep. 1, 2013), Art. 9.

8 Personal information refers to "information that can be used to identify an individual when used either independently or in combination with other information, including but not limited to an individual's name, date of birth, identification number, biometric information, address, and phone numbers." *See* Network Security Law, Art. 76 (5).

Network Operators must establish and improve their user information protection system and keep their user information strictly confidential.[9] At the time of collection, Network Operators must expressly state the purposes, methods, and scope of data collection and obtain the individual's consent. Only relevant personal information may be collected or used.[10] The Network Security Law does not specify what form of consent is acceptable. Without the consent of the user, Network Operators are prohibited from providing the user's personal information to any third party, unless redacted to remove personally identifiable information.[11] In the event of a breach or other improper transfer, Network Operators must immediately take remedial measures, and notify the affected users and report to the competent authorities in a "timely" manner.[12] "Timely" is not defined in the law.

Content Monitoring

Under Article 47, Network Operators have a duty to monitor the information published by their users. Upon becoming aware of the publication or transmission of "prohibited information," Network Operators must promptly stop transmitting the information and prevent its spread. Network Operators are also required to maintain records and report incidents to the competent authorities.[13] Based on earlier laws and regulations,[14] "prohibited information" includes a wide variety of political and religious speech, other speech that disturbs social stability, pornography and speech that encourages other illegal behavior, slander and other information that damages the lawful rights of third parties, as well as any information that is otherwise prohibited by law or administrative regulation.

---

9 Network Security Law, Art. 40.

10 Network Security Law, Art. 41.

11 Network Security Law, Art. 42.

12 Network Security Law, Art. 42.

13 Network Security Law, Art. 47.

14 For example, Administrative Measures for Protection of the Security of International Internetworking of Computer Information Networks (Dec. 30, 1997), Art. 5; Administrative Measures for Internet Information Services (effective on Sep. 25, 2000), Art. 15; Telecommunication Regulations (effective on Sep. 25, 2000), Art. 57; Anti-Terrorism Law (effective on Jan. 1, 2016), Art. 19.

Cooperation with Authorities

Article 28 of the Network Security Law imposes duties (echoing those imposed by the Anti-Terrorism Law) on network operators to provide technical support and assistance to public security and national security agencies in national security and criminal investigations. Although technical support and assistance is not defined in the Network Security Law, under the Anti-Terrorism Law, this support would require providing "technical interfaces, decryption and other technical support and assistance" to security agencies.[15] The Network Security Law does not specify any process that the agencies must go through prior to requesting cooperation.

ADDITIONAL OBLIGATIONS OF CRITICAL INFORMATION INFRASTRUCTURE OPERATORS

"Critical Information Infrastructure Operators" are defined as entities involved in a wide range of sectors including public communication and information services, energy, transportation, water conservancy, finance, utilities and e-commerce.[16] The definition also includes a catch-all category "other important sectors and fields." Moreover, the detailed scope and protective measures relating to critical information infrastructure is explicitly left to future regulation by the State Council.[17] The impact of the Network Security Law on foreign businesses will largely be determined by how narrow or broad these future regulations are.

Data Localization Requirement

The Network Security Law imposes a data localization obligation on Critical Information Infrastructure Operators. Article 37 of the Law states,

> Personal information and important business data collected and generated in the operation of critical information infrastructures operators within the territory of the People's Republic of China shall be stored within the territory. Where it is necessary to provide such information and data abroad due to business needs, security assessment shall be carried out according to the measures formulated by the national Internet information department in conjunction with the

[15] Anti-Terrorism Law, Art. 18.

[16] Network Security Law, Art. 31.

[17] Network Security Law, Art. 31.

> relevant departments of the State Council; if there are other provisions in laws and regulations, those provisions shall prevail.

The broad wording of Article 37 requires the adoption of detailed implementing rules. Most significantly, "important business data" is not defined, making it difficult to determine what must be stored in China. It also remains to be seen: which entity will conduct the security assessment prior to "provision of information abroad"; how onerous that assessment is likely to be; and whether such an assessment will apply only to individual transfers, or whether it could permit routine transfer—equivalent to the storage of data abroad.

Ongoing Cyber-security Obligations

The Network Security Law also introduces a new set of security protection obligations applicable to Critical Information Infrastructure Operators, including: (i) setting up special security management departments and responsible persons (and conducting background checks of such responsible persons),[18] (ii) conducting training on cyber-security on a regular basis,[19] and (iii) carrying out testing and evaluation of the security and potential risks of its network.[20]

Technology Regulation

Article 23 of the law requires certification and approval of "critical network equipment" and "specialized cyber-security products" by a "qualified institution" not defined in the law. While the purpose of certification is to ensure that such technology is "secure and reliable," in practice, it is likely to restrict the availability of such equipment and products to a preapproved list which could result in: (i) currently existing equipment and products (especially foreign equipment and products) becoming unavailable if it is not certified and/or (ii) a delay in the ability of multinationals doing business in China to implement global technology upgrades pending certification. Obviously, Article 23 also raises concerns about the possibility of discrimination against foreign technology companies in the certification process.

In addition to the certification requirement in Article 23, Article 35 of the law restricts how Critical Information Infrastructures Operators may store data.

---

[18] Network Security Law, Art. 34 (1).

[19] Network Security Law, Art. 34 (2).

[20] Network Security Law, Art. 38.

Specifically, when a Critical Information Infrastructures Operator purchases "network products or services" that may affect or involve national security, the product or service will be subject to a security review jointly arranged by the National Internet Information Department and the relevant departments of the State Council.[21]

* * *

Please do not hesitate to contact us with any questions.

[21] Network Security Law, Art. 35.