Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

3 Ways Cybersecurity Law In China Is About To Change

Law360, New York (May 2, 2016, 4:22 PM ET) --


Timothy Stratford


Yan Luo

On July 6, 2015, the same week that China passed a sweeping new National Security Law, the Chinese government published a draft Cybersecurity Law for public comment.[1] The draft law articulated the government's priorities related to cyberspace and information networks, consolidated existing cybersecurity-related requirements, and granted government agencies more powers in regulating cyberactivities.

Nine months later, in March 2016, the head of the National People's Congress ("NPC") Standing Committee, China's highest legislative body, announced that the government is aiming to enact the draft law in 2016. The NPC's legislative plan, which was issued recently, confirmed that the second reading of the draft law will be conducted in June.

Designed to "safeguard cyberspace sovereignty and national security," the draft law was expected to have significant impact on multinationals operating in China or seeking to access China's vast market, if and when it comes into effect. It sought both to introduce new, high-priority mandates such as protection of critical information infrastructure, and to sort out and develop, in a more systematic way, existing but scattered legal requirements in areas such as data localization, cross-border data transfer and security reviews. Many previously under-regulated or unregulated activities that take place over "computer networks," defined broadly to encompass essentially any "network or system, composed of computers or other terminals together with relevant devices, that serves to collect, store, transmit, exchange, or process information following predefined rules and procedures," [2] will be subject to government scrutiny once the law is implemented.

This article discusses three areas where the draft law will bring the most significant changes to the existing regulatory regime, changes that could have long-lasting impacts on multinationals.

Data Localization

In recent years, Chinese laws and regulations increasingly contain data localization requirements as the government seeks to reduce potential barriers to its jurisdiction over data. But these requirements are scattered in many industry-specific regulations.

The table below shows currently effective or proposed data localization requirements.

Law & Regulation	*Industry*	*Restriction*
Notice of the People's Bank of China on Improving Work Related to the Protection of Personal Financial Information by Banking Financial Institutions (PBOC, *effective* Jan. 21, 2011)	**Financial Services** (Banking)	*Banking financial institutions* may not analyze, process, store, or transfer offshore personal financial information collected within China.[i]
Administrative Measures for Credit Reference Agencies(State Council, *effective* Mar. 15, 2013)	**Financial Services** (Credit Reporting)	Any credit information collected within China must be organized, stored, and processed within China.[ii]
Measures for the Administration of Electronic Banking Business (CBRC, *effective* Mar. 1, 2006)	**Financial Services** (E-Banking)	*Chinese-invested banking institutions with e-banking businesses* must keep their relevant business operations systems and servers located within the PRC.[iii]
Administrative Measures for the Online Payment Business of Non-Banking Payment Institutions (PBOC, *effective* Jul. 1, 2016)	**Financial Services** (Online Payment)	*Non-Banking Payment Institutions* must have secure and standardized online payment business processing systems and backup systems located within China. Institutions providing domestic transaction services must process transactions via domestic business processing systems and complete fund settlement within China.[iv]
Opinions of the Office of the Central Leading Group for Cyberspace Affairs on Strengthening Cybersecurity Administration of Cloud Computing Services for Communist Party and Government Agencies (Office of the Central Leading Group for Cyberspace Affairs, *effective* Dec. 30, 2014)	**ICT** (Cloud Computing)	*Cloud computing platforms and data centers* that provide services to Party or government departments must be located onshore. Sensitive information may not be transmitted, processed, or stored offshore without approval.[v]
Measures for Administration of Population Health Information (Trial) (NHFPC, *effective* May 5, 2014)	**Healthcare**	*Institutions that provide medical, healthcare, and family planning services* may not store population health information on servers overseas or otherwise host or rent overseas servers.[vi]
Provisions on Administration of Online Publishing Services (SAPPRFT, MIIT, *effective* Mar. 10, 2016)	**Online Publishing**	*Entities engaging in online publishing* must keep servers and storage equipment within the territory of the PRC.[vii]

Letter on Soliciting Opinions on the Draft Guidelines for Financial Accounting Work of Insurance Enterprises (Draft for Comments) (CIRC, *released* for public comment on Jul. 13, 2011; comments due by Jul. 29, 2011)	**[NON-BINDING DRAFT GUIDELINES] Financial Services** (Insurance)	Business and financial data on financial information systems of *insurance companies* should be stored within China.[viii]
Regulation on Supervision and Administration of Informatization of Insurance Organization (Draft for Comments) (CIRC, *released* for public comment on Oct. 9, 2015; comments due by Oct. 31, 2015)	**[DRAFT REGULATION]** **Financial Services** (Insurance)	*Insurance institutions* shall establish data centers, and the physical location of the data centers must be within China if the source of data comes from within the territory of China.[ix]
Notice of the People's Bank of China on Issuing the Industrial Standards on the Information Security Standards for Credit Reporting Institutions (PBOC, *effective* Nov. 17, 2014)	**[NON-BINDING GUIDELINES]** **Financial Services** (Credit Reporting)	*Credit reporting institutions* engaged in credit reporting activities in China must locate the databases and backup databases they create with in China. The organization, storage, and processing of information collected by credit reporting institutions must be conducted within China. [x]

The draft law, as currently written, would introduce a cross-industry requirement for operators of what is deemed to be "critical information infrastructure" to store "important data" (such as users' personal information), which is collected and generated during operations, within China. "Critical information infrastructure" is a new term that is defined broadly to include networks and systems in sensitive areas, such as public communications, radio and television, energy, transportation, water, finance, utilities, health care, social security, military, and government administration, as well as networks and systems that "have a large number of users."[13] The draft law is unclear as to what, beyond personal information, would be considered to be "important data." It also does not explain what would constitute a network or system with "a large number of users," even though one could imagine that, for instance, popular websites run by online service providers are covered.

Given the increasing emphasis on cyberspace sovereignty, these data localization requirements are likely to stay in the final version, or even to be strengthened to cover additional sectors.

It is uncertain which agencies will be responsible for enforcing these requirements. It remains to be seen whether the Cyberspace Administration of China ("CAC," also known as the Office of Central Leading Group for Cyberspace Affairs), the country's chief Internet watchdog established in late 2014, will obtain the rulemaking authority to issue cross-industry implementing regulations. Despite this uncertainty in the enforcement structure, sector regulators that are already active in the field, such as Ministry of Industry and Information Technology ("MIIT," telecom and Internet services regulator), People's Bank of

China ("PBOC," credit reporting and payment regulator) China Banking Regulatory Commission ("CBRC," banking regulator) and China Insurance Regulatory Commission ("CIRC," insurance regulator), are likely to continue playing important roles because of their in-depth industry knowledge and sector regulatory capacity.

Cross-Border Data Transfer

Similarly, the existing Chinese rules do not provide a comprehensive cross-border data transfer regime. Some sector regulators may allow transfer of data to overseas entities or individuals in limited circumstances, and often on a case-by-case basis, but such requirements are uneven and the process to obtain regulators' consent is often opaque. Examples of currently effective data transfer requirements include:

LAW	INDUSTRY	RESTRICTION
Opinions of the Office of the Central Leading Group for Cyberspace Affairs on Strengthening Cybersecurity Administration of Cloud Computing Services for Communist Party and Government Agencies (Office of the Central Leading Group for Cyberspace Affairs, *effective* Dec. 30, 2014) Opinions of the State Council on Promoting Innovation and Development of Cloud Computing to Cultivate New Types of Information Industry (State Council, *effective* Jan. 6, 2015)	**ICT** (Cloud Computing)	... Sensitive information may not be transmitted, processed, or stored offshore without approval.[xi] The importance of regulating cross-border data flows is highlighted in another Opinion from the State Council, which sets out guidelines intended to serve as a framework for future cloud computing laws and regulations. No implementation regulation has been issued thus far.[xii]
Measures for the Administration of Electronic Banking Business (CBRC, *effective* Mar. 1, 2006)	**Financial Services** (E-Banking)	*Foreign-invested banking institutions with e-banking businesses* may keep their relevant business operations systems and servers within the PRC or overseas. If they are kept overseas, they must also maintain facilities and equipment recording and storing business data within the PRC such that they can comply with requirements for field inspections by financial regulators and judicial authorities. [xiii]
Notice of the People's Bank of China on Soliciting Public Opinions on the Administrative Measures for Bank Card Clearing Institutions (Draft for Comments) (PBOC, *released* for public comment on Jul. 2, 2015; comments due by Aug. 3, 2015)	**[DRAFT REGULATION] Financial Services** (Bank Card Clearing)	*Bank card clearing institutions* ("BCCIs") are prohibited from transferring users' financial information overseas without users' authorization.[xiv] Where a BCCI transmits personal financial information collected in China to foreign issuers or acquirers, for the purpose of processing cross-border transactions and with authorization from the parties concerned, the BCCI must ensure that the foreign issuers or acquirers keep the personal financial information they have received confidential.
Regulation on Supervision and Administration of Informatization of Insurance Organization (Draft for Comments) (CIRC, *released* for public comment on Oct. 9, 2015; comments due by Oct. 31, 2015)	**[DRAFT REGULATION]** **Financial Services** (Insurance)	The overseas transfer of data stored in the information systems of *foreign invested insurance institutions* must comply with China's relevant laws and regulations."[xv]

The draft law also seeks to change the existing regulatory regimes relating to cross-border data transfers by introducing a new security assessment process before operators of "critical information infrastructure" can transfer "important data" to overseas for business reasons. No further explanation was provided on how the government intends to conduct such a security assessment (for instance, through a case-by-case assessment or through blanket authorization) and what are the criteria for such an assessment.

Again, the data transfer requirement is likely to remain in the final version, and likely to be strengthened to impose additional hurdles on cross-border data transfer. As indicated in the banking and payment data transfer examples, sector regulators such as PBOC, CIRC and CBRC are taking the lead in assessing whether business-related data such as transaction data can be transferred overseas. This is unlikely to change after the draft law is officially enacted. But it remains uncertain which agency will have the broad mandate to enforce the data transfer requirement in relation to personal information (e.g. employee data).

Security Reviews of Network Products and Services

Since 1997, "information system security products," which are defined to include "hardware and software designed to protect information system security," have to pass a security review by the Ministry of Public Security ("MPS") before they can be marketed in China.[19] This security review largely focuses on the technical functionality of these products.[20]

In recent years, the government has started to mandate security reviews on services procured by government agencies (especially central-level agencies). Examples include cloud computing, information technology system design and development, data processing services and so on.[21] These reviews require suppliers to submit information on themselves and their services, as well as information on the testing or evaluation centers which certify the security of such services. In addition, some sector regulators, such as PBOC, MIIT and the National Health and Family Planning Commission, have mentioned in various policy documents that security reviews should be conducted when companies in the regulated industries procure network products or services. None of these documents offer insights on how these reviews would be implemented in practice.

Mirroring this two-pronged approach, the draft law proposes a more comprehensive security review system that covers both product security review and procurement-related security review. Article 19 requires that "Critical Network Equipment and Network Security Products" (not defined) must pass a security review or test by an accredited evaluation center before they can be marketed in China. Existing review requirements should be consolidated and a comprehensive catalogue of approved products should be issued. Moreover, Article 31 requires operators of "critical information infrastructure" that "may affect national security" to procure only network products and services that pass a security review. It is uncertain how the procurement-related security review process under Article 31 would interact with the product security review mentioned in Article 19.

The proposed security review requirements would have important implications: They are likely to broaden the scope of product security reviews and subject more sectors to the procurement-related security reviews. The existing rules impose the review requirements only on a limited number of products and on companies who supply these products or services to government agencies. The new review system will expand to all "Critical Network Equipment and Network Security Products" and to operators of "critical information infrastructure," such as banks, utility companies, transport companies, and potentially major websites.

In addition to the expansion in scope and coverage, the new review system proposed by the draft law could focus more on the potential impact on China's national security, a factor that has not been emphasized in the past. This trend of emphasizing national security concerns associated with information technology products could pose additional market access risks to multinationals.

—By Timothy Stratford and Yan Luo, Covington & Burling LLP

Tim Stratford is managing partner in Covington & Burling LLP's Beijing office, former assistant U.S. trade representative and former general counsel for General Motors' China operations. Yan Luo is an associate in the firm's Beijing office.

[1] 中华人民共和国网络安全法（草案） [Cybersecurity Law of the People's Republic of China (Draft for Comments)] ("Draft Cybersecurity Law") (The Standing Committee of the National People's Congress, released for public comment on Jul. 6, 2015; comments due by Oct. 5, 2015).

[2] Id., Art. 65(2).

"The following terms used herein are defined as follows: … (2) "Network Security" refers to the capability of taking necessary measures to prevent attacks on, intrusion into, interference with, damage to, and illegal use of networks, as well as emergencies, aiming to enable networks to operate stably and reliably, and ensure the integrity, confidentiality and availability of information stored, transmitted and processed over networks."

[3] 人民银行关于银行业金融机构做好个人金融信息保护工作的通知 [Notice of the People's Bank of China on Improving Work Related to the Protection of Personal Financial Information by Banking Financial Institutions], Art. 6 (People's Bank of China, effective Jan. 21, 2011).

"Personal financial information collected within the territory of China shall be stored, handled and analyzed within the territory of China. Unless otherwise stipulated by laws, regulations and provisions of the People's Bank of China, financial institutions of the banking industry shall not provide domestic personal financial information to overseas countries."

[4] 征信业管理条例 [Administrative Measures for Credit Reference Agencies], Art. 24 (State Council, effective Mar. 15, 2013).

"A credit reporting agency shall, within the territory of China, organize, store and process the information collected within the territory of China.

A credit reporting agency shall provide information for an overseas organization or individual in compliance with laws, administrative regulations and relevant provisions of the Credit Reporting Industry Regulatory Department under the State Council."

[5] 电子银行业务管理办法 [Measures for the Administration of Electronic Banking Business], Art. 10

(China Banking Regulatory Commission, effective Mar. 1, 2006).

“In addition to the conditions as described in Article 9 hereof, financial institutions which launch e-banking business such as online banking business and mobile banking business through the Internet shall also meet the following conditions:

…(4) The e-banking business operation systems and business operation servers of Chinese-invested banking financial institutions are located in the People's Republic of China;

(5) The e-banking business operation systems and business operation servers of foreign-invested financial institutions may be located in the People's Republic of China or overseas. Where their system and servers are located overseas, they shall set up facilities and equipment in the People's Republic of China that can record and store business data, can satisfy the requirements of field inspections by financial regulatory departments and can satisfy the requirements of investigation and evidence collection by the Chinese judicial authorities in case of legal disputes.”

[6] **非**银行支付机构网络支付业务管理办法 [Administrative Measures for the Online Payment Business of Non-Banking Payment Institutions], Art. 26 (People's Bank of China, effective Jul. 1, 2016).

“A Payment Institution shall own secure and standardized online payment business processing systems and the backup systems thereof within the territory of China and formulate emergency response plans to ensure system security and business continuity.

A Payment Institution that provides services for domestic transactions shall complete transactions via domestic business processing systems, and complete fund settlement within the territory of China.”

[7] **中央网**络安全和信息化领导小组办公室关于加强党政部门云计算服务网络安全管理的意见 [Opinions of the Office of the Central Leading Group for Cyberspace Affairs on Strengthening Cybersecurity Administration of Cloud Computing Services for Communist Party and Government Agencies], Art. 2 (Office of the Central Leading Group for Cyberspace Affairs, effective Dec. 30, 2014).

“Sensitive information should not be taken offshore. Cloud computing services platforms and data centers that provide services to Party and government departments must be located onshore. Sensitive information shall not be transmitted, processed or stored offshore without approval.”

[8] **人口健康信息管理**办法(试行) [Measures for Administration of Population Health Information (Trial)], Art. 10 (National Health and Family Planning Commission of China, effective May 5, 2014).

“A responsible entity shall, in light of service and management needs, promptly update and maintain population health information to ensure that such information is up-to-date, continuous and valid.

The responsibility entity shall neither store population health information in overseas servers, nor host or rent overseas servers.”

[9] 网络出版服务管理规定 [Provisions on Administration of Online Publishing Services], Arts. 8, 12 (State Administration of Press and Publication, Radio, Film and Television, Ministry of Industry and Information Technology, effective Mar. 10, 2016).

“A book, audio-video, electronic, newspaper or periodical publisher shall meet the following requirements if it engages in providing web publishing services:

…(3) It has necessary technical equipment needed for the provision of web publishing services and its related servers and storage equipment are located within the territory of the People’s Republic of China.”“The application materials for engaging in web publishing services shall include the following particulars:

(1) Application Form for Web Publishing Service License;

…(7) Proof of registration of the domain name of its website and the commitment that its related servers are within the territory of the People’s Republic of China.

[10] **关于征求**对《保险公司财会工作指引（征求意见稿）》意见的函 [Letter on Soliciting Opinions on the Draft Guidelines for Financial Accounting Work of Insurance Enterprises (Draft for Comments)], Art. 82 (China Insurance Regulatory Commission, released for public comment on Jul. 13, 2011; comments due by Jul. 29, 2011).

“The business and financial data on information systems of insurance enterprises should be stored within China, and have remote backup.”

[11] **保**险机构信息化监管规定（征求意见稿） [Regulation on Supervision and Administration of Informatization of Insurance Organization (Draft for Comments)], Art. 31 (China Insurance Regulatory Commission, released for public comment on Oct. 9, 2015; comments due by Oct. 31, 2015).

“[Construction Standard] An insurance institution shall establish its data center through self-construction, joint construction, or outsourcing of which the machine room’s design standard should comply with national standards and requirements of China Insurance Regulatory Commission. Where the data source comes from China, the physical location of the data center shall be within China.”

[12] **中国人民**银行关于发布《征信机构信息安全规范》行业标准的通知 [Notice of the People’s Bank of China on Issuing the Industrial Standards on the Information Security Standards for Credit Reporting Institutions], Art. 9.9 (People’s Bank of China, effective Nov. 17, 2014).

“Cross-border flow of information shall be subject to the following requirements:

a) The production database and backup database of credit reporting institutions engaging in crediting business and related activities in China shall be located within China.

b) The organization, storage, and processing of information by credit reporting institutions shall be conducted within China, and information collected by such credit reporting institutions is prohibited from transferred overseas online or through carrying storage media.

c) The provision of information to overseas entities and individuals by credit reporting institutions should be in compliance with laws and regulations and relevant regulations of the People’s Bank of China.”

[13] Draft Cybersecurity Law, Art. 25.

“The State gives priority to the protection of basic information networks providing public communications and radio & TV transmission services, important information systems of key sectors such as energy, transportation, water resources and finance and public service fields such as power supply, water supply, gas supply, healthcare and social security, military networks, government networks used by state organs at or above the level of a city with districts, and networks and systems having large numbers of users and owned or managed by network service providers (hereinafter referred to as the “Critical Information Infrastructure”). The measures for the protection of the Critical Information Infrastructure shall be formulated by the State Council.”

[14] 中央网络安全和信息化领导小组办公室关于加强党政部门云计算服务网络安全管理的意见 [Opinions of the Office of the Central Leading Group for Cyberspace Affairs on Strengthening Cybersecurity Administration of Cloud Computing Services for Communist Party and Government Agencies], Art. 2 (Office of the Central Leading Group for Cyberspace Affairs, effective Dec. 30, 2014).

“Sensitive information should not be taken offshore. Cloud computing services platforms and data centers that provide services to Party and government departments must be located onshore. Sensitive information shall not be transmitted, processed or stored offshore without approval.”

[15] 国务院关于促进云计算创新发展培育信息产业新业态的意见 [Opinions of the State Council on Promoting Innovation and Development of Cloud Computing to Cultivate New Types of Information Industry], Art. 2(6) (State Council, effective Jan. 6, 2015).

“Strengthen the capability of security protection. Research on relevant laws and systems of protection on personal information and enterprise information and online information security, formulate administration rules on collection, storage, transfer, deletion, and cross-border flow of information, and accelerate legislation process in terms of information security.”

[16] 电子银行业务管理办法 [Measures for the Administration of Electronic Banking Business], Art. 10 (China Banking Regulatory Commission, effective Mar. 1, 2006).

“In addition to the conditions as described in Article 9 hereof, financial institutions which launch e-banking business such as online banking business and mobile banking business through the Internet shall also meet the following conditions:

…(4) The e-banking business operation systems and business operation servers of Chinese-invested banking financial institutions are located in the People's Republic of China;

(5) The e-banking business operation systems and business operation servers of foreign-invested financial institutions may be located in the People's Republic of China or overseas. Where their system and servers are located overseas, they shall set up facilities and equipment in the People's Republic of China that can record and store business data, can satisfy the requirements of field inspections by financial regulatory departments and can satisfy the requirements of investigation and evidence collection by the Chinese judicial authorities in case of legal disputes.”

[17] 中国人民银行关于《银行卡清算机构管理办法（征求意见稿）》公开征求意见的通知 [Notice of the People's Bank of China on Soliciting Public Opinions on the Administrative Measures for Bank Card Clearing Institutions (Draft for Comments)], Art. 7 (People's Bank of China, released for public comment

on Jul. 2, 2015; comments due by Aug. 3, 2015).

“Bank card clearing agencies and overseas agencies shall keep confidential the identity information, account information, transaction information, other relevant sensitive information and other financial information of the parties concerned that are obtained from bank card clearing services, and shall not provide such information for external parties without authorization by the parties concerned, unless otherwise prescribed by laws and regulations.

Where a bank card clearing agency, for the purpose of processing cross-border bank card transactions and upon authorization by the parties concerned, transmits relevant personal financial information collected within the Mainland to overseas card issuers or acquirers, the bank card clearing agency shall ensure that the overseas card issuers or acquirers keep confidential the personal financial information obtained.”

[18] **保**险机构信息化监管规定（征求意见稿） [Regulation on Supervision and Administration of Informatization of Insurance Organization (Draft for Comments)], Art. 58 (China Insurance Regulatory Commission, released for public comment on Oct. 9, 2015; comments due by Oct. 31, 2015).

“[Data Security] … The overseas transfer of data stored in the information systems of foreign invested insurance institutions shall comply with China’s relevant laws and regulations.”

[19] 计算机信息系统安全专用产品检测和销售许可证管理办法 [Regulation on Administration of Testing and Sales License of Security Products Exclusively Used for Computer Information System] (Ministry of Public Security, effective Dec. 12, 1997).

[20] Id., Art. 4.

“When applying for a sales license, a producer of security products shall conduct testing and certification of the security functions of its security products.”

[21] **政府部**门信息技术外包服务机构申请信息安全管理体系认证安全审查程序（暂行） [Procedures of Security Review of Application for Authentication of Information Security Management System by Outsourcing Institutions Providing Information Technology Services to Government Agencies (Trial)] (Ministry of Industry and Information Technology, effective Jul. 20, 2011).