ONC Lawyers

柯伍陳律師事務所

Overview of China's New Cybersecurity Law and its impacts

CISO Executive Roundtables 2017 – Hong Kong
28 November 2017

Dominic Wai, Partner, ONC Lawyers

ONC Lawyers

China's new cybersecurity law

- Effective from 1 June 2017
- On 11 April 2017 the Cyberspace Administration of China (**CAC**) released a draft Measures for Security Assessment of Outbound Transmission of Personal Information and Important Data (**Draft**) to solicit public comments
- On 19 May 2017, the CAC released an amended Draft (**Amended Draft**)
  - Effective date 1 June 2017
  - Implementation date 31 December 2018
- Draft Guidelines for security assessment of outbound data transmission (**Draft Guidelines**)
- 2nd Draft Guidelines for security assessment of outbound data transmission (**2nd Draft Guidelines**)

ONC Lawyers

China’s new cybersecurity law

Promote 2 key objectives:

- Protect China against cyber attacks
- Protect the rights and interests of Chinese citizens from cyber attacks and the misuse of personal information.

ONC Lawyers

China’s new cybersecurity law

Key provisions:

- Data localization rule: imposed an obligation on operators of “Critical Information Infrastructure” (**CII**) to store personal information and other important data collected and generated during operations within China.

ONC Lawyers

China’s new cybersecurity law

Key provisions:

- Aim at CII and not all Network Operators
- Not aim at all kinds of data, but personal information and important data.
- “Important Data” is in relation to China, and not aim at corporations or individuals.

ONC Lawyers

China's new cybersecurity law

- Data localization rule:
  - Requires CII operators to undertake security assessment before transferring such data abroad
  - The security assessment shall be conducted by the CAC and the State Council (unless permission for the transfer is already provided under another PRC law)

ONC Lawyers

China's new cybersecurity law

CII is defined broadly as "infrastructure that, in the event of damage, loss of function, or data leak, might seriously endanger national security, national welfare or the livelihoods of the people, or the public interest"

- Includes public communications and information services, energy, transportation, water conservancy, finance, public services and e-government

ONC Lawyers

China's new cybersecurity law

- CII covers:
  - Operators who operate networks used for critical public services
  - Private sector operators who operate networks which, if breached, would cause serious damage to state security, the Chinese economy or to the public at large.

ONC Lawyers

China's new cybersecurity law

- Network Operators (NO) – widely defined that may apply to any business that owns and operates IT networks in China including a computer network, website, app or other electronic platform where information collected from 3rd party users in China is stored, transmitted, exchanged or processed.

ONC Lawyers

China's new cybersecurity law

NOs need to:

- Make public all privacy notices
- Obtain individual consent for collecting and processing personal data
- Implement technical safeguarding measures to secure against loss and destruction of personal data, data minimization, confidentiality and rights to accuracy and restriction on processing of personal data.

ONC Lawyers

China’s new cybersecurity law

Personal data is defined as including:

- All kinds of information, recorded electronically or through other means which is sufficient to identify a natural person’s identity, or reflect the activity of certain natural persons, including but not limited to:
  - Full names
  - Birth dates

ONC Lawyers

China’s new cybersecurity law

- Identification numbers
- Correspondence and communication contact information
- Personal biometric information
- Addresses
- Account number and password
- Status of property
- Location and activity information

ONC Lawyers

China’s new cybersecurity law

NOs must provide internal security management systems that include:

- Appointment of dedicated cybersecurity personnel
- Retention of network logs
- Reporting risks on network services and products to users and authorities
- Having contingency plans for network security incidents and reporting such incidents to the authorities

ONC Lawyers

China’s new cybersecurity law

- Providing assistance and cooperation to public security bodies and state security bodies to safeguard national security and investigate crimes.

ONC Lawyers

China's new cybersecurity law

IT Product Suppliers are required to:

- Provide security maintenance for all services and products for the full term of the contract – security maintenance cannot be terminated within the contract term.
- Prior to being sold or produced in the PRC market, cybersecurity products and services will be required to obtain a government certification and/or meet prescribed safety inspection requirements and national standards.

ONC Lawyers

China's new cybersecurity law

Regulatory Penalties for non-compliance

- Violations of the personal data protection provisions may lead to confiscation of illegal gain and a fine of up to 10 times the illegal gain or RMB 1M (in case there is no illegal gain), and in serious cases, suspension of business or revocation of business license and fines up to RMB 100,000 for responsible individuals

ONC Lawyers

China’s new cybersecurity law

- For CII operators, unauthorized cross-border provision of data may result in confiscation of illegal gain and a fine of up to RMB 1M as well as suspension of business or revocation of business license and a fine of up to RMB 100,000 for responsible officials

ONC Lawyers

China's new cybersecurity law

The Amended Draft

- The original Draft extended the applicability of the data localization rule from CII operators to all NOs
- However, the Amended Draft removes reference to the data localization requirement and focused on security assessment of outbound data transmission. This amendment suggests that not all NOs (but only CII operators) will be required to store Local Data in China.

ONC Lawyers

China’s new cybersecurity law

The security assessment of cross-border data transfer shall abide by the principles of “fairness, impartiality, objectiveness and transparency” to protect the security of the Local Data and promote the lawful, orderly and free flow of network information.

ONC Lawyers

China's new cybersecurity law

A security assessment is triggered if the intended outbound cross-border data transmission involves any of the following circumstances:

- contains or accumulatively contains Personal Information of more than 500,000 individuals
- contains, among others, data regarding sectors such as nuclear facilities, chemical biology, national defense and military and population health, as well as data related to large-scale engineering activities, marine environment and sensitive geographic information

ONC Lawyers

China’s new cybersecurity law

- Network security data relating to CII, including system vulnerabilities and security protection measures.
- Other circumstances that may affect national security or public interest.

ONC Lawyers

China's new cybersecurity law

- The Amended Draft does not provide details on how a security assessment would be conducted procedurally.
- The Amended Draft removes the 60 day timeframe for completing a government administered assessment (GAA) that was set out in the Draft – uncertainty as to timing to complete the GAA

ONC Lawyers

China's new cybersecurity law

A security assessment should focus on:

- Lawfulness, legitimacy, and necessity of such transfers;
- Amount, scope, type, level of sensitivity of important data involved;
- Data recipients' data security measures, capabilities, and their level of protection;
- Risks arising from cross-border transfers or subsequent re-transfers of data in terms of such data being leaked, damaged, tampered with, or misused; and
- Risks posed by cross-border data transfers to China's national security, societal and public interests, and Chinese citizens' rights and interests.

ONC Lawyers

China's new cybersecurity law

NOs must, according to the types, amount and importance of the cross border data transfer, conduct a security assessment on outbound data transmission.

NOs are required to conduct a new security assessment promptly each time when the purpose, scope, type and amount of cross-border data transfer:

- Is changed greatly
- Or material security incidents happens.

ONC Lawyers

China’s new cybersecurity law

The competent industry regulator or regulatory authority shall organize the security assessment.

If the competent industry regulators or regulatory authorities are unclear, the assessment shall be organized by the national cyberspace authority.

ONC Lawyers

China's new cybersecurity law

Draft Guidelines – Important Data refers to data that is closely related to national security, economic development and public interest.

The industry coverage is quite broad (oil/gas, coal, petrochemicals, power, telecommunications, steel, defence, geolocation data, digital data etc) but it seems that Important Data would not include internal corporate data generated from day-to-day operations.

ONC Lawyers

China’s new cybersecurity law

Draft Guidelines – clarified that data generated outside China and transferred through China does not fall within the scope of Local Data and would not be subject to the outbound transmission requirements, if such data has not been modified or processed in China.

ONC Lawyers

China's new cybersecurity law

- 2nd Draft Guidelines clarifies the concept of "domestic operation" (境內運營)
  - NO who is not registered within the territory of China but who conducts business within or provides products or services to the territory of China shall also be deemed as conducting "operations within the territory of China".
  - Factors to be taken into account include but not limited to: website being in Chinese language, settlement in RMB, and delivery commodities to China

  - Broaden the scope of application of the obligation of security assessment for data exports

ONC Lawyers

China's new cybersecurity law

- The 2nd Draft Guidelines also provides that:-

- NOs within the territory of China who only conduct business with or provide products or services to overseas institutions, organizations or individuals without involving personal information and important data of domestic citizens shall not be deemed conducting "operations within the territory of China"

ONC Lawyers

China's new cybersecurity law

Transparency Principle – NOs shall inform data subjects of the purpose, method and scope of collection and use of personal data and obtain data subjects' consent.

NOs shall not collect personal information irrelevant to the services provided by them

ONC Lawyers

China's new cybersecurity law

Amended Draft – in order to transmit personal data overseas, NOs must inform data subjects of the purpose and scope of the outbound data transmission, the content and the recipient(s)(countries or regions) of the information transmitted and need to obtain consent.

ONC Lawyers

China's new cybersecurity law

Amended Draft – Exemption to the consent requirement for outbound transmission of personal information

- where the outbound transmission is necessitated by an emergency that endangers the life or property of citizens

Circumstances where consent may be inferred from the conduct of data subjects:

- Making international calls
- Sending international emails or instant messages
- Conducting cross-border online transactions

ONC Lawyers

China's new cybersecurity law

2nd Draft Guidelines provides "Notification – Consent" Requirement for the Export of Personal Data:

- The NOs must expressly notify the individuals of the purpose, type, recipient and risks of the data export as well as its contact person and contact details
- Where there is a change in the privacy policy of the NO or the recipient of exported data, or when there is a major change in the purpose, scope, type, quantity or risks of the data export, consent must be obtained again from the individuals whose personal data is to be exported

ONC Lawyers

China's new cybersecurity law

Amended Draft – subject to assessment, outbound transmission of Local Data is prohibited:

- If the cross border data transfer is in violation of relevant provisions of state laws, administrative regulation, departmental rules
- If data subject has not consented
- If it will damage public and national interests

ONC Lawyers

China's new cybersecurity law

Amended Draft – subject to assessment, outbound transmission of Local Data is prohibited:

- If the transfer will endanger the security of national politics, territory, military, economy, culture, society, technology, information, eco logical environment, resources and nuclear facilities.
- Other circumstances in which the national cyberspace, public security, security, or other relevant departments determine that the data concerned is prohibited from being transferred overseas.

ONC Lawyers

China’s new cybersecurity law

- A relevant authority such as CAC, PSB or national security authority etc determines that the data may not be transmitted abroad

ONC Lawyers

China's new cybersecurity law

- Is transferring data from Mainland China to Hong Kong a cross-border transfer of data?
- Does remote access of data amounts to a cross-border transfer of data?
  - Amended Draft – "Cross-border data transfer" means providing personal information and important data in electronic form to overseas institutions, organizations, or individuals.
  - 2nd Draft Guidelines on "data cross-border transfer" – data which is not transferred to or stored in places other than China is accessed and viewed by overseas institutions, organizations and individuals (except for public information and webpage visits)

ONC Lawyers

China's new cybersecurity law

According to the 2nd Draft Guidelines, the following circumstances shall also be deemed as data exports:-

- The personal data and important data is provided to any entity within the territory of China who is not subject to the jurisdiction of China or not registered within the territory of China;
- A NO group exports its internal data which involves personal information and important data collected and generated in the course of its operations within the territory of China

ONC Lawyers

Recent Enforcement

Investigation into Tencent Wechat, Sina Weibo and Baidu Tieba

- On 11 August 2017, the CAC announced its investigations into the three social media platforms for violation of the Cyber Security Law, accusing them of spreading prohibited information and/or failing to perform their management duties over the prohibited information posted by their users.

- On 25 September 2017, the local branches of the CAC in Beijing and Guangdong Province announced the violations, and the imposition of the maximum fine under Article 68 of the Cyber Security Law.

ONC Lawyers

Recent Enforcement

Investigation into Alibaba Cloud (Aliyun)

- The Communication Administration of Guangdong Province exercised its enforcement powers under the Cyber Security Law
- Alibaba Cloud failed to implement the real-name registration requirement
- Alibaba Cloud was ordered to rectify the problem

ONC Lawyers

Recent Enforcement

Investigation into 廣東市動景計算機科技有限公司 (a network technology company in Guangdong)

- The cloud acceleration product for the UC browser offered by the company was found to have security defects resulting in the spread of prohibited information in violation of paragraph 1 of Article 22 of the Cyber Security Law.
- The company was ordered to take immediate measures to rectify the violation and to conduct regular security assessments on its communications network as well as on any new or existing products and services.

ONC Lawyers

Recent Enforcement

The Supreme People's Procuratorate issued the 9th set of Guiding Cases in October 2017:

- 李丙龍破壞計算機信息系統案
- 李駿傑等破壞計算機信息系統案
- 曾興亮、王玉生破壞計算機信息系統案
- 衛夢龍、龔旭、薛東東非法獲取計算機信息系統數據案
- 張四毛盜竊案
- 董亮等四人詐騙案

•Criminal cases involving hacking and data alteration, ransomware extortioin, deception, data theft and domain hijacking

ONC Lawyers

Enforcement Inspection Group

- On 25 August 2017, an enforcement inspection group was formed under the NPC Standing Committee to oversee the enforcement of the Cyber Security Law and the Decision on Strengthening Network Information Protection.
- Six inspection teams were dispatched to carry out inspections in provinces and cities across China in September and October 2017.
- It is expected that a report on the enforcement of the Cyber Security Law and the Decision will be submitted to the NPC Standing Committee in December 2017.

ONC Lawyers

Q&A

ONC Lawyers

Dominic Wai
Partner
Email: dominic.wai@onc.hk
Mobile: (852) 9385 6984

ONC Lawyers
Office: 19th Floor, Three Exchange Square, 8 Connaught Place, Central, Hong Kong.
Phone: (852) 2810-1212
Fax: (852) 2804-6311
Web-Site: www.onc.hk

ONC Lawyers

THANK YOU

ONC Lawyers

solutions • not complications