LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Data Privacy, Security & Cybercrime Practice 14 April 2017 | Number 2119

# China Publishes Draft Measures Restricting Outbound Data Transfers

***The current draft grants Chinese regulators broad discretion to prohibit data transfers.***

**Key Points:**

- The draft requires both the consent of the data subjects and/or the permission of the regulators for any transfer of personal information and critical data out of China.
- The draft mandates a self-evaluation for all outbound transfers of personal information and critical data and sets out several conditions that would trigger a mandatory regulatory assessment.
- The draft is open for comments until 11 May 2017 so it may change in its scope and application.

## Background

The Cyberspace Administration of China (CAC) has published a draft law that places wide-ranging restrictions on companies seeking to transfer personal information and critical data, as defined below, (collectively, Relevant Data) out of China. The draft legislation, *the Measures on Security Assessment for Outbound Transmission of Personal Information and Critical Data* (the Draft), expands the scope of the new Chinese data localization requirements including prohibiting the transfer of Relevant Data outside of China in certain circumstances. Under the Draft, companies must apply for permission from the regulator of each industry (ultimately coordinated by CAC) to transfer Relevant Data internationally if such Relevant Data is potentially damaging to the Chinese state or exceeds certain thresholds based on volume or the number of data subjects. The Draft grants the government unfettered discretion to reject applications for such transfers. The Draft is currently open for public consultation until 11 May 2017, which means it may change from its current form, but as drafted it introduces the two-tier security assessment mechanism in response to the risks from increasing cyber-security threats. The Draft is one of several implementation measures to be adopted by CAC under the delegated authority set out in the Network Security Law (NSL), which takes effect on 1 June 2017. The timing of the proposal suggests that the CAC aims to finalize and adopt the measures in the Draft on or around the effective date of the NSL.

## Restrictions on Data Transfers

The Draft prohibits the transfer of data internationally in the following three circumstances:

- **Transfer without consent**: As contemplated in the Draft, informed consent of data subjects is required before personal information can be transmitted out of China. "Personal information," as defined consistently in the NSL and the Draft, refers to any information recorded electrically or by other means that can be used solely or with other information to identify a natural person, including

but not limited to name, birth date, personal identification number, personal biological information, address, phone number *etc*. In certain circumstances, personal information may be restricted from being transferred even *with* informed consent, if doing so would infringe the civil rights of the individual under the General Provisions of the Civil Law of China.

- **Risk exposure**: Data cannot be transferred out of China if doing so would expose the state to political, economic, scientific or defense risks, adversely impact national security or damage public interests.

- **Discretionary refusal to transfer**: The Draft provides the CAC, public security agencies, national security agencies and other agencies the right to refuse or to prohibit the transfer of any data out of China, at their discretion.

The Draft defines "the outbound data transfer" to mean the provision of any personal information and critical data collected and generated by network operators, which in NSL and the Draft refer to network owners, administrators and service providers, within China to any institutions, organizations or individuals located outside of China. The definition does not specify what would be viewed as "located out of China" and whether this would mean physically or virtually remains unclear. "Critical data" is also defined in the Draft as any data relevant to national security, economic development or social public interests; the Draft points to relevant (but unspecified) standards and guidelines for reference.

## Expanded Scope of Data Localization Laws

The Draft requires that all network operators store Relevant Data gathered in China inside China and conduct a security assessment before transferring it out of China, if such transfer is required because of business need. This requirement expands on the earlier NSL, which had previously only applied the data localization and security assessment requirements to critical information infrastructure operators (CIIOs), a subset of all network operators.

## Two-tier Security Assessment Mechanism: Self-assessment and Assessment by the Regulators

As noted above, the Draft requires all network operators to conduct a self-assessment to evaluate the safety of Relevant Data prior to transferring it out of China. The Draft outlines a number of factors to be evaluated including:

- Necessity for outbound data transmission (there should be a clear business need for any export of data from China)
- The nature of personal information in question (*e.g.*, volume, type, scope, sensitivity and data subjects' consent)
- The nature of critical data in question (*e.g.*, volume, type, scope and sensitivity)
- The recipient's security measures and capability to protect the data (including the network security environment of the destination country)
- Potential risks of a breach impacting the confidentiality, availability or integrity of the data, and the potential for it to be misused outside of China
- Potential risks to national security, public interest and the legitimate interests of the individual

All network operators shall apply to their regulators to be assessed and must pass the assessment if one of the following conditions is met before exporting Relevant Data:

- **Number**: if the personal information relates to 500,000 or more individuals (though, notably the Draft fails to specify the time period or frequency for the calculation of this number)

- **Volume**: if the data contains more than 1000 Gigabytes (though again, there are no specifics regarding how to calculate this amount based on a certain time period or frequency of the transfer)

- **Types of Data**: if the data relates to nuclear facilities, bio-chemistry, military defense, general health, large-scale project activities, marine environments or sensitive geographic information

- **Level of Network Security**: if the data relates to network security information of CIIO's systematic vulnerabilities or security solutions

- **Industry and Sector**: if the data relates to personal information or critical data of CIIOs, or

- **Other**: if the data relates to other information which might affect national security, public interests or information in the discretion of the regulators

Therefore, any CIIOs must apply for and pass an assessment by a regulator before it can transfer any data out of China. For a non-CII network operator, it should go through a regulator's assessment if it meets one of the other five conditions remunerated above.

## Requirement for Ongoing Assessment and Reassessment

A network operator is also required to conduct a security assessment for outbound data transfer at least once per year. A re-assessment is required more frequently if there are (i) changes in data recipients, or (ii) material updates of the purpose, scope, volume, type, etc. of data to be transmitted abroad, or (iii) significant security breach occurs in data recipients or related to transferred data.

## Potential Implications for Other Individuals and Entities

After introducing a two-tier security assessment mechanism applicable to all network operators, the Draft further called upon "*all* other individuals and organizations" to "reference and implement" the mechanism contemplated in the Draft when handling outbound transfers of relevant data gathered and generated inside China. Thus, as is currently drafted, there is room for an interpretation that these new measures could potentially apply to all individuals and entities that collect Relevant Data in China, regardless of whether they gather Relevant Data through using computer networks or paper files, though it requires further clarification.

## Conclusion

The brief proposal set out in the Draft contains measures that are likely to significantly impact all multinational companies, across all industries and sectors, with significant operations in China. The Draft expands the scope of the companies affected by the data localization requirements under the NSL and imposes the burdensome requirement to seek consent from all data subjects. The Draft provides the Chinese government with significant discretion to restrict data transfers out of China which may result in increased involvement in the affairs of private companies, and delays in being able to take on new business and systems whilst the exports are assessed. Helpfully, one provision in the Draft does leave open the possibility for bilateral or regional treaties to govern cross-border data transfers. The draft is open for consultation and we will provide an update once the text is finalized.

If you have questions about this *Client Alert*, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

**Hui Xu**
hui.xu@lw.com
+86.21.6101.6006
Shanghai

**Gail E. Crawford**
gail.crawford@lw.com
+44.20.7710.3001
London

**Wei-Chun (Lex) Kuo**
lex.kuo@lw.com
+852.2912.2511
Hong Kong

**Andrea E. Stout**
andrea.stout@lw.com
+44.20.7710.5843
London

**Sean Wu**
sean.wu@lw.com
+86.21.6101.6013
Shanghai

**You Might Also Be Interested In**

**Keeping Your Company's Data Safe This Tax Season**

**European Commission Proposes ePrivacy Regulation**

**NYSDFS Revises Cybersecurity Rules to Accommodate Industry Concerns**

**Financial Institutions Await Response to Concerns Over NYSDFS' Proposed Cybersecurity Rules**