China's draft data localisation measures open for comment

April 2017

Hogan Lovells

China's draft data localisation measures open for comment

On 11 April 2017 the Cyberspace Administration of China (the "**CAC**") published a circular calling for comments on its *draft Security Assessment for Personal Information and Important Data Transmitted Outside of the People's Republic of China Measures* (the "**Draft Export Review Measures**").

The passage of the *People's Republic of China Cyber Security Law* in November 2016 (the "**Cyber Security Law**") left many questions unanswered as to the practical scope and effect of this important new piece of legislation (please see our briefing **here**). With less than two months to go before the implementation of the Cyber Security Law on 1 June, many outside observers were expecting to have seen a significant volume of implementing legislation demarcating boundaries around the expansive scope and intrusive nature of the Cyber Security Law. For those familiar with China's typical approach to legislative drafting, in which implementing rules often see the light of day after the law comes into effect, the issuance of the Draft Export Review Measures at this time may come as a welcome development.

The main legislative purpose of the Draft Export Review Measures is to clarify the process and requirements relating to the data localisation requirements in the Cyber Security Law, one of the most controversial aspects of the law. While the Draft Export Review Measures do add a significant level of implementing detail as to the practicalities of compliance, we expect that for many multi-national corporations ("**MNCs**") with operations in, or doing business with, China, the nature of the clarifications do not go in the direction that they would have wanted.

Data localisation applies to all Network Operators

The Cyber Security Law regulates two key types of organisations:

- key/critical information infrastructure ("**CII**") operators ("**CII Operators**"); and
- network operators ("**Network Operators**").

The precise scope of what constitutes CII is ultimately left to be determined by the State Council, but the Cyber Security Law states that CII means key infrastructure relating to critical industries such as:

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

as well as a "catch-all" phrase which includes other key information infrastructure that may jeopardize national security, the national economy and the people's livelihoods or the public interest were it to be destroyed, experience a loss of functionality or data leakage ("**Catch-all Phrase**").

While the scope of what constitutes CII is vague and ultimately discretionary, it is possible to discern an intent on the part of the drafters of the Cyber Security Law to regulate critical, large scale systems that would have a significant impact on the national interest (as determined by the Chinese government) if disrupted by a cyber attack.

Network operators are defined under the Cyber Security Law to be the owners or managers of cyber networks and network service providers (the latter term is not defined at all). On the basis that the scope of the definition is not limited to telecommunications carriers and other telecommunications service providers, but

instead extends to a wide range of businesses operating network systems or providing "network services" which, in one interpretation, could be as broad as having a website in China as part of their business, the potential scope of "Network Operator" is significantly wider than the scope of "CII Operators".

The Cyber Security Law regulates CII Operators and Network Operators in different ways. Based on the text of the Cyber Security Law passed by the National People's Congress on 7 November, 2016, we had expected that the Draft Export Review Measures would only apply to cross-border transfers of personal data and "important data" by CII Operators, with no data localisation requirement attaching to Network Operators, unless the particular Network Operator is also a CII Operator. This, however, is not the case. Under the Draft Export Review Measures, all Network Operators will be subject to data localisation requirements. Furthermore, we now understand that subject to any watering down as the Measures proceed to final form, China's data localisation rules will have a far wider scope than was originally envisaged when the law was passed.

In addition, Article 16 of the Draft Export Review Measures goes one step further by stating that these export review requirements also apply to other individuals and organizations if they intend to send personal data and important data collected and generated in China outside of China. This means that not only are non-network operators caught by the Draft Export Measures (i.e. all entities in China are caught), but as long as they collect/generate personal data or important data in China foreign entities and individuals are also regulated. This may have significant implications for those MNCs who have significant China operations, but who use an offshore model and typically systematically export all the data to their offshore servers.

The export review process and the thresholds for triggering a review

The CAC is charged with the overall co-ordination of the export review process. Article 6 of the Draft Export Measures suggests, however, that it is the industry sector regulators who will be tasked with administering the reviews. This is an issue with respect to consistency of approach, as well as procedural fairness, given that some regulators in China are known to be more foreign-investor friendly than others, and the most foreign-investor friendly organisations like the Ministry of Commerce ("**MOFCOM**") will not have a significant role to play in this regard as MOFCOM regulates foreign trade and foreign direct investment rather than specific industries, as compared to the industry-specific regulators such as the Ministry of Industry and Information Technology ("**MIIT**") (for telecoms and Internet and industry players), the China Food and Drug Administration (for pharma and medical devices) or the China Insurance Regulatory Commission (for insurance sector companies). It is possible that some regulators may take a harder or softer line in administering the Draft Export Measures once they are finalised. The CAC itself will take the lead in sectors where there is no clear industry regulator. It is likely that it will adopt a fairly hard line given its mandate and focus.

Network Operators are expected to conduct self-assessments prior to undertaking any data export, and in any of the circumstances set out in Article 9 of the Draft Export Measures, apply to their industry sector regulators for review prior to undertaking any export. As noted above, where there is no applicable industry regulator, Network Operators will have to apply to the CAC.

Review triggers raise concerns

Article 9 of the Draft Export Measures sets out the triggers for a review: satisfying any one of these is sufficient to trigger a review:

- contains or in aggregate contains the personal data of 500,000 people or more;
- involves a volume of over 1,000 GB;
- involves nuclear facilities, bio-chemistry, national defence and military sectors, public health and other such fields, as well as data on large-scale engineering projects, marine environments and sensitive geographical information;
- involves system vulnerabilities and security safeguards for key information infrastructure or other such-like cyber security information;
- constitutes personal data and important data sent overseas by operators of key information infrastructure1; and
- any other data which is likely to adversely impact national security and the public interest and which industry supervisory or regulatory departments determine needs to be assessed.

The review triggers are of concern because they are something of a blunt instrument due to the size of file criteria in the second leg of the test – any transmission overseas of 1,000 gigabytes (equal to one terabyte) of data that either contains personal data or contains non-personal data but includes important data (it is not clear whether all the data has to be in a particular category, but presumably the assumption must be that including any data falling into either category in the packet would trigger the review) will generate the need for a security assessment. There is no indication as to how the volume of a data transfer is assessed. Presumably, the threshold relates to the aggregate volume of exported data "at rest" transferred from China and not to the volume of one time transfers, but there is no clarity on this point within the draft.

The review trigger outlined in the third bullet point above appears to be driven by the fact that data relating to large scale engineering projects or mapping data may be considered to constitute state secrets under Chinese law. Network Operators may find themselves pushed into over-submitting on the basis of the sweep-up clause set out in the sixth bullet point, which necessitates a 'second guess' as to what the industry regulators may determine to be "other data which could adversely impact national security and the public interest". This puts an unreasonable burden on them.

The standard of review: heavily driven by discretion

Article 8 sets out the focus areas for self-assessments and assessments by industry sector regulators as follows:

- the necessity for the overseas transmission of data;
- whether any personal data is involved, including its volume, scope, nature, sensitivity level and so forth
- whether or not the data subject of the personal data consents to his/her personal data being transmitted overseas;
- whether any important data is involved, including its volume, scope, nature, sensitivity level and so forth;
- the security protection measures adopted by data recipients, the extent to which the data recipients are able to protect the security thereof and the cyber security environment and so forth of the destination country(ies) or region(s);
- the risk of disclosure, destruction, tampering or misuse in the course of overseas transmission o or on subsequent retransfer and similar risks;

[1] Reflecting the original requirement under the Cyber Security Law.

- potential risks to national security, the public interest and lawful personal rights and interests as a result of overseas transmission of data or aggregation of such data ; and
- any other important factors requiring assessment.

There is a notable amount of discretion built into the "focus areas" in Article 8 where nearly all the legs of the test include the word "等" ("etc" in Chinese) which means the list is not exhaustive, giving rise to the possibility of subjective interpretations of what is included (in the same way as with the Catch-all Phrase). As is also typical of Chinese legislative drafting, the provision also includes its own "sweep up" version of the Catch-all Phrase "other important factors requiring assessment", allowing for unrestricted subjective interpretation of the scope of review.

When can data not be exported?

Article 11 lists a number of circumstances in which data will not be allowed to be exported:

- the data subject concerned has not consented to his or her personal data being transmitted overseas, or the transmission of such information overseas is likely to prejudice the interests of the individual;
- the overseas transmission of data would give rise to risks with respect to the security of national politics, the economy, scientific and technological matters, national defence and so forth, and is likely to adversely impact national security and/or harm the public interest; and
- any other data the State network information departments, public security departments, security departments or other relevant departments determine should not be permitted to be exported from the PRC.

Again we have two (relatively) concrete tests which are then rendered somewhat meaningless by the "sweep up" allowing government bodies to block exports of data on subjective grounds.

What type of consent is needed?

Article 4 of the Draft Export Review Measures separately states that data subject consent is required for offshore transfers of personal data, and this consent must be obtained after informing the data subjects of the purpose, scope, content, recipient and destination country(ies) or region(s) of the data export. This may mean any existing consents for transfers overseas to unspecified "affiliates" of the transferor will no longer be valid going forward unless the affiliates and their jurisdictions of incorporation are specifically listed. Exports of a minor's personal data are subject to the consent of the minor's parents or guardian. Anyone under 18 years of age would therefore need his or her guardian's consent. Article 4's brief statement on the consent requirement does not elaborate on whether consent must be explicit or may be implied, or whether consent given may subsequently be withdrawn.

Definitions of "personal data" and "important data"

The definition of "personal data" under the Draft Data Export Measures is identical to that under the Cyber Security Law, which defines "personal data" as information, recorded electronically or otherwise, which either on its own or when used in combination with other information identifies an individual. "Personal data" for these purposes includes, but is not limited to, name, date of birth, identification card number, biometric information, address and telephone number. This definition is very similar to definitions of personal data seen in other legislation in this area.

The Cyber Security Law does not provide any definition for the "important data" subject to

the localisation requirement. The Draft Data Export Measures address this omission to some extent by defining "important data" as data that is closely related to national security, economic development, and the social and public interest, with reference to relevant national standards and important data classification guidelines. Such national standards and data classification guidelines must, in some shape or form, point to existing and any future rules on state secrets. These rules, or at least the definition of "state secrets", are by their very nature nebulous, and the formulation raises the issue of how to assess what is "important data" when the rules are not in public domain.

Annual and supplemental reviews

Regardless of whether a self-assessment was carried out or an export review was undertaken by the relevant industry sector regulators, Network Operators are thereafter required to conduct security reviews of their cross-border transfers no less frequently than annually and report the results of these reviews to their respective industry sector regulators. Annual reports generate additional risk for Network Operators, including where failures to carry out assessment processes may be uncovered as a result. Practically speaking it is difficult to see how a Network Operator like a telecommunications company could possibly monitor and prevent any exports in violation of the rules.

Supplemental reviews are required where the recipient of the transfer changes, where there is a relatively large change to the purpose, scope, volume or nature of data being exported or there is a major security incident in relation to exported data or its recipient.

Bilateral or multilateral data transfer agreements

Article 15 makes provision for international agreements concerning data transfers to essentially prevail over inconsistent provisions of the Draft Export Review Measures, providing a chink of light whereby an international data transfer agreement with say the US or the EU (and other major trading partners with the most negotiating clout) could override the Draft Export Review Measures to the extent of any inconsistency. This is consistent with the general position under Chinese law that an international treaty commitment prevails over any inconsistent provision of domestic law (e.g. a double tax treaty prevails over the domestic tax law provisions). MNCs should, therefore, be lobbying hard for their governments to enter into such treaties as soon as is reasonably practical although realistically it will be hard to even start that conversation until the final text of the Draft Export Review Measures is known.

Conclusions

The publication of the Draft Export Review Measures represents an important development for the implementation of China's controversial Cyber Security Law. The unexpected extension of the application of the data localisation rules to all Network Operators and to businesses that are not Network Operators (potentially including foreign entities without a presence in China) that collect or generate personal data or "important data" in China is a significant new and unwelcome twist that will mean that all MNCs collecting and/or generating data in China (regardless of business model) will need to apply fresh scrutiny to the law.

There are many significant points for commentary on the Draft Export Review Measures from the perspective of business impact, including:

– What will the standard of review be and the relationship with existing similar provisions? Noting that some industry sector regulators, such as the China Banking Regulatory Commission, already have data export review processes in place,

it will be important to understand how these new provisions will impact existing standards of review that have come to be understood in these industries.

- Noting that different regulators will be administering the reviews, and noting the degree of discretion granted to these regulators, will there be consistency as to approach and to standards? Will CAC step in to ensure this is the case and will it have the authority to do so?
- How will specific points of the review be assessed? For example, how will the "necessity" of a data export be judged? How will the security standards expected of data recipients be judged? Or the "cyber security environment" of the export destination? Will experts on the recipient jurisdiction need to be brought in? Will politically motivated distinctions between various jurisdictions or regions develop as part of the review?
- How costly and time-consuming for businesses will the self-assessment process and review process be, both in terms of initial reviews and in terms of annual and supplemental reviews that follow?
- How will existing data exports be addressed, given that many MNCs with a presence in China have operating models that involve the leveraging of offshore regional and global operating platforms? If efficiency does not equate to "necessity", then these exports may not be permitted going forward. There may well be business models that are altogether not viable without offshoring data processing operations to other jurisdictions. The Draft Export Review Measures do not provide for a transition period or any "grandfathering" measures.
- What will the standard of consent be for exports of personal data? It will generally be impracticable for businesses to operate separate onshore and offshore servers based on the choice of the relevant data subjects, so a consent requirement effectively becomes a localisation requirement, without even reaching the stage of analysing the necessity or security of the export.

While there are some useful clarifications on the triggers for review and the criteria for the security assessments, there are many key points left unanswered. The unexpected scope of the Draft Export Review Measures is likely to overshadow all other issues, both in terms of the expansiveness of the scope and its vagueness. If brought into force in the form as drafted, would require virtually every MNC with a presence in or dealing with China to reassess its data collection and processing arrangements and form a view on compliance that would necessarily be tempered by ongoing uncertainty. The potential business cost of achieving compliance with these draft standards could be unsustainable for businesses in a number of sectors. We anticipate, therefore, that a significant number of MNCs will wish to submit comments either individually or through various Chambers of Commerce in China.

Public comments are open through 11 May, 2017.

Contacts

Jun Wei
Partner, Beijing
+86 10 6582 9501
jun.wei@hoganlovells.com

Roy Zou
Partner, Beijing
+86 10 6582 9596
roy.zou@hoganlovells.com

Liang Xu
Partner, Beijing
+86 10 6582 9577
liang.xu@hoganlovells.com

Philip Cheng
Partner, Shanghai
+86 21 6122 3816
philip.cheng@hoganlovells.com

Andrew McGinty
Partner, Shanghai
+86 21 6122 3866
andrew.mcginty@hoganlovells.com

Mark Parsons
Partner, Hong Kong
+852 2840 5033
mark.parsons@hoganlovells.com

Alicante
Amsterdam
Baltimore
Beijing
Brussels
Budapest
Caracas
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Rio de Janeiro
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar
Warsaw
Washington, D.C.
Zagreb

Our offices
Associated offices

www.hoganlovells.com