China passes controversial Cyber Security Law

November 2016

Hogan Lovells

China passes controversial Cyber Security Law

China's Cyber Security Law, which will take effect from 1 June, 2017 was finally adopted on 7 November. The third draft of the law adopted by the Standing Committee of the National People's Congress, China's highest legislative authority, contained few changes from the second draft put forward for comment in July, 2016 (see our *briefing*). The net result is ongoing controversy coupled with uncertainty, with multi-national businesses in particular questioning the intent behind the law and criticising its vagueness. The final draft contains a number of broadly-framed defined terms that are critical to its interpretation which continue to leave much to be resolved through detailed measures that may or may not follow. All in all, the direction of travel is towards a much more heavily regulated Chinese internet and technology sector, with an open question as to whether China's cyber space will be truly integrated with the rest of the world in the coming years.

A Quick Recap

The Cyber Security Law's seventy-nine articles address a wide range of issues, but as previously noted we see particular focus on three main aspects:

- **Technology regulation:** The Cyber Security Law seeks to regulate what technology can or cannot be used in China's cyber space, including by: (i) imposing requirements for pre-market certification of "critical network equipment" and "specialised security products"; and (ii) designating certain systems as "critical information infrastructure" that will be subject to national security reviews and detailed measures to be issued by the State Council. The concern here is whether there will be a protectionist slant to these measures that will make it difficult for foreign players to compete.
- **Co-operation with authorities:** The Cyber Security Law imposes duties on "network operators" to provide technical support and assistance in national security and criminal investigations and to retain weblogs for at least 6 months.
- **Data Localisation:** The Cyber Security Law requires operators of "critical information infrastructure" to store personal information and "important data" within China, save where it is truly necessary to send this data offshore and the offshoring arrangements have cleared a security assessment process that is yet to be defined. Revisions in the final draft broaden the scope of personal data from "citizen's person data" to "personal data", suggesting that personal information of foreigners in China will also be subject to the localisation requirement, which does little to reassure foreign residents who may need to move data across borders for any number of good reasons.

Continuing Uncertainty as to Scope

Obligations under the Cyber Security Law attach to two main classes of business: "network operators" and operators of "critical information infrastructure." Neither of these terms are defined in any detail under the new law, leaving much room for speculation and interpretation.

"Network operators" are defined as an "owner or manager of any cyber network and network service providers," casting a potentially very wide net for the obligations to maintain weblogs and co-operate with authorities noted above.

"Critical information infrastructure" is ultimately left to be defined by the State Council, but is stated in the Cyber Security Law to be critical infrastructure relating to critical industries, being public communications and information services, energy, transportation, water conservancy, finance, public services, e-government affairs and other significant industries and sectors, as well as any other infrastructure that may jeopardise national security, the national economy, people's livelihoods or the public interest were it to be destroyed, experience a loss of functionality or data leakage. Ultimately it is a subjective test.

Following the recent inspection of critical information infrastructure carried out by the

Office of the Central Leading Group for Cyberspace Affairs, (often referred to as the Cyberspace Administration of China (the "**CAC**")) (the "**Cyberspace Inspection**"), the CAC moved to define "critical information infrastructure" by reference to a three step process, beginning with the identification of critical businesses, then identifying information systems and industrial control systems that ensure the functioning of those businesses and then finally identifying the degree to which these businesses are vulnerable to attack in relation to specific items of infrastructure forming part of their systems.

In its press release on the Cyberspace Inspection, the CAC set out a non-exhaustive list of critical businesses within each of the critical industries identified. In relation to telecommunications and internet sector, a wide swathe of facilities and non-facilities-based services are identified, from voice, data, basic internet networks and hubs, through to domain name resolution systems and data centre and cloud services. A section headed "business platforms" refers to instant messaging, online shopping, online payments, search engines, e-mail, BBS, maps and audio/video services. To give context to the degree of materiality envisaged in the wake of the Cyberspace Inspection if, for example, they have over one million average daily visitors or if a cybersecurity breach would affect the life and work of over one million people, web sites are considered to be critical information infrastructure for critical businesses. Corresponding examples applicable to online platforms are RMB10 million in direct economic loss due to a cyber security breach or the loss of personal data of one million people.

In addition to key definitions such as "network operator" and "critical information infrastructure", the scope of certain obligations under the Cyber Security Law lacks precision in many areas. It is not clear, for example, the extent of technical assistance that "network operators" will be obliged to provide in support of national security and criminal law investigations. Does this encompass, for example, directions to install "back doors" in technology that would enable uninterrupted access by law enforcement to data and communications? Similarly, what security assessment will need to be applied to proposals to offshore personal information and important business data collected or created by critical information infrastructure? These are fundamental issues for many of the foreign investors in this area.

Changes in the Third Draft

The final version of the Cyber Security Law passed on 7 November contains few changes from the second draft presented in July, but there are nonetheless some important points to note. The first two drafts of the law defined "personal information" by reference to Chinese citizens. The version of the law adopted by the Standing Committee eliminates this reference, meaning that provisions in the Cyber Security Law addressing personal data will apply to citizens and foreign nationals alike. In some respects this amendment is non-controversial. For example, obligations on network operators to keep personal data secure and a general prohibition on the unlawful sale of personal data, both of which now provide assurances to foreign nationals. The data localisation requirement applying to the personal data of foreign nationals as well as Chinese citizens is, conversely, more controversial.
Amendments to Article 12 expand on the previously tabled requirement that cyber networks not be used to threaten national security by including a prohibition against using such networks to pose threats to the reputation or interests of the state.

An amendment to Article 21 clarifies that specific regulations will be issued prescribing how weblogs are meant to be maintained by "network operators" for at least 6 months.
In several cases there have been increases to the level of fines applicable to offences under the Cyber Security Law. A notable amendment to Article 64 extends the liability of "network operators" infringing privacy rights to personal liability for individuals directly in charge of the operator and other directly responsible persons,

a formulation more often seen in the criminal law context.

Implications

China's Cyber Security Law has drawn significant criticism since the first draft was tabled. Multi-national businesses have expressed grave concerns over the potential for discriminatory application of the law to foreign technologies and equipment, as well as over data localisation requirements that hamper efficiencies and may be counter-productive to information security. Human rights and free speech advocates see in the Cyber Security Law a further tightening of state control of China's media and communications infrastructure, especially against the broader background of new restrictions or internet publishing (see our *briefing*).

It is difficult to reconcile the Cyber Security Law with China's move to integrate with the global economy and gradually open the technology services sector to wider foreign participation. It is not clear, for example, whether or not foreign technologies will continue to meet the requirements for use in critical information infrastructure in China, and to what extent there will be official or unwritten requirements for "back doors" that may ultimately compromise security and intellectual property rights. There are also worrying parallels between the requirements under the Cyber Security Law and requirements for the use of state-approved "secure and controllable" technologies in the financial services sector (see our *briefing*), the concern here being that foreign technologies may be deemed incapable by their nature of being "secure and controllable" or that achieving certifications against such standards may involve the disclosure of source code and other trade secrets or standards that only domestic players can meet.

More broadly, the Cyber Security Law escalates concerns that China is pursuing a course where its domestic internet becomes something isolated and detached from the global internet. This is already true to a degree in relation to internet content, which is heavily censored in China. The thrust of the Cyber Security Law is to expand the monitoring to the infrastructure level, with implications for technical standards and interoperability. If the result is that businesses in China are required to operate using technologies that meet China's security standards but do not meet international standards, there is a threat that networks in the rest of the world will be even more reluctant to interconnect due to security concerns. What this could mean for the international growth of China's fast-growing technology sector remains to be seen.

There is some evidence that China is alive to the need to react to the widespread international criticism. Chinese Premier Li Keqiang remarked during his August 2016 visit to the US that China will communicate with foreign companies to seek to find effective approaches to co-operation in cyber security matters. Some progress on this front may be seen in the CAC's opening of its Technical Committee 260 to participation by foreign technology businesses. Amongst other responsibilities, Technical Committee 260 is tasked with developing standards that will be applied under the Cyber Security Law.

Practical Next Steps

It is clear that businesses operating in China must review their technology and data arrangements in the light of the implications of the Cyber Security Law coming into effect on 1 June 2017. Technology businesses will need to review their Chinese business strategies and evaluate whether or not their products and services fall within the scope of the new requirements and if so, for example, will be subject to some form of certification or worse still, face exclusion from the market. They also need to consider matters such as the nature of personal data collected in China and how and where this data is stored.

Businesses in other sectors will need to evaluate their technology use in China across a range of fronts, including:

— the impact of the Cyber Security Law on the available options for technology procurement in China and what the range of options means in terms of performance,

functionality, cyber security and other matters;
- the interoperability of onshore systems with offshore networked systems;
- options for data server locations; and
- potential knock-on effects of the Cyber Security Law for related areas of regulation, such as the encryption regulations and telecommunications licensing.

Businesses in the financial services sector, in particular, will need to consider the Cyber Security Law in the context of their specific technology risk management regulations, with an eye in particular to the move towards "secure and controllable" technology requirements, which to those in the know, have set something of a worrying precedent.

Contacts

Jun Wei
Partner, Beijing
jun.wei@hoganlovells.com

Roy Zou
Partner, Beijing
roy.zou@hoganlovells.com

Liang Xu
Partner, Beijing
liang.xu@hoganlovells.com

Philip Cheng
Partner, Shanghai
philip.cheng@hoganlovells.com

Andrew McGinty
Partner, Shanghai
andrew.mcginty@hoganlovells.com

Mark Parsons
Partner, Hong Kong
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