Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Asia Pacific news

Gabriela Kennedy *

Mayer Brown JSM, Hong Kong

Keywords:
Asia-Pacific
IT/Information technology
Communications
Internet
Media
Law

A B S T R A C T

This column provides a country-by-country analysis of the latest legal developments, cases and issues relevant to the IT, media and telecommunications' industries in key jurisdictions across the Asia Pacific region. The articles appearing in this column are intended to serve as 'alerts' and are not submitted as detailed analyses of cases or legal developments.

1. China

Gabriela Kennedy *(Partner), Mayer Brown JSM (gabriela.kennedy@mayerbrownjsm.com);*

Karen H.F. Lee *(Senior Associate), Mayer Brown JSM (karen.hf.lee@mayerbrownjsm.com).*

1.1. *Navigating the latest developments in China's Cybersecurity Law*

On 1 June 2017, China's new Cybersecurity Law ("**CSL**") came into operation. The PRC government has issued a series of draft measures, guidelines and regulations in an attempt to provide further clarity on the application of the CSL, but many ambiguities and uncertainties remain. To help navigate them, a brief summary of several of these measures, guidelines and regulations issued over the last few months is set out below.

1.1.1. *Background*

The CSL imposes restrictions on operators of critical information infrastructures ("**CIIs**") and network operators, and has been seen as a barrier to the free-flow of data and contrary to current business practices. The most controversial provisions concern data localisation requirements, cross-border data transfer restrictions, the implementation of cybersecurity measures, and compliance and certification measures for security products and equipment. The broad definition of network operators (with limited clarification from the government) has meant that any entity that operates a Chinese website, conducts business activities through networks in China, or provides online services to customers in China may be caught by the CSL restrictions.

In addition to the above requirements, which have received the most media attention, the CSL places a large burden on network operators to screen and "police" users of their services, including messaging platforms, blogs and social media platforms. Network operators are not only required to ensure that users provide information concerning their true identity (thereby eliminating the possibility of users posting information anonymously), they are also required to stop the illegal public dissemination of any information transmitted by their users (e.g. online posts that are seen as a criticism or threat to national security or the socialist system).

The Cyberspace Administration of China ("**CAC**") has already started taking steps to crackdown on network operators. In August 2017, the CAC commenced investigations against three popular social media platforms. Users had allegedly been using the social media platforms to disseminate information that was

For further information see: www.mayerbrown.com.

* Mayer Brown JSM, 16th–19th Floors, Prince's Building, 10 Chater Road Central, Hong Kong.
E-mail address: gabriela.kennedy@mayerbrownjsm.com.

https://doi.org/10.1016/j.clsr.2017.09.006

seen as challenging national and public security, as well as public order, and the operators of the platforms were accused of failing to takedown such information in breach of the CSL. The platform operators have indicated that they will cooperate with the CAC to rectify the issue. This is likely to just be one of many investigations initiated by the CAC as part of the government's cybersecurity initiative, which has included a crackdown on virtual private networks and online news.

1.1.2. Cross-border transfers and data localisation

The revised draft of the Security Assessment Measures for the Cross-Border Transfer of Personal Information and Important Data ("**Cross-Border Measures**") was issued on 19 May 2017. Even though the Cross-Border Measures came into effect on 1 June 2017, a final version still needs to be issued by the CAC. Due to a backlash of concern raised by foreign entities on their ability to comply with the Cross-Border Measures, an 18-month grace period was granted, giving network operators until 31 December 2018 to comply with the newly introduced cross-border data transfer rules.

Unlike the earlier drafts, express reference to the data localization requirements in respect of network operators has been removed from the current version of the Cross-Border Measures. It would be naive to draw the conclusion that the data localization requirements do not apply to network operators (only CII operators as per the CSL), as network operators are still subject to restrictions under the Cross-Border Measures on the overseas transfer of personal information and "important data" collected or generated during business operations in China. Important data is broadly defined to include information that relates to national security, economic development, or social or public interest.

A CII operator or network operator may provide no personal information or important data to anyone outside of China unless:

- they have completed the required security assessment set out under the Cross-Border Measures;
- the data subject has been notified of the purpose and scope of the transfer, and the country in which the recipient is located; and
- the data subject's consent has been obtained (which can be inferred based on the data subject's actions), save when there is an emergency that may jeopardise the life or property of the relevant data subject.

Notwithstanding the above, no transfer of personal information or important data may occur if it will violate any laws or regulations; the transfer may result in risks to national security and public interest, or cause harm to the government system, economic security, scientific or technological security, information security, national defense, etc; or if any relevant regulator deems the transfer to be inappropriate.

Both a self-assessment and an official security assessment from the local authorities must be carried out and obtained before a CII operator or network operator can transfer personal information and important data outside of China. The self-assessment no longer needs to be carried out on an annual basis thereafter (as was originally required under previous versions of the Cross-Border Measures), but it must be conducted upon any significant amendment in relation to a cross-border transfer (e.g. change in scope or type of data). An official security assessment from the relevant local authorities must also be obtained in certain situations, such as where more than 500,000 individuals' personal information are being transferred, or the data concerns public health or national security sectors, and so on.

In order to complement the Cross-Border Measures, on 27 May 2017 the draft Guidelines for Cross-Border Data Transfer Security Assessment was issued for public consultation ("**Draft Cross-Border Security Guidelines**"). The Draft Cross-Border Security Guidelines sets out how a security assessment should be carried out prior to the cross-border transfer of any personal information or important data by network operators. This includes a requirement to have in place a data export plan and to assess the legality and appropriateness of the cross-border transfer, and the level of risk involved. The consultation period expired on 27 June 2017, and a final draft is pending.

1.1.3. Security review of network equipment and cybersecurity products

CII operators that procure network products and services that might affect national security must undergo a national security review organized by the relevant local authorities. On 2 May 2017, the Cyberspace Administration of China issued the Security Review Measures for Network Products and Services (Trial) ("**Security Review Measures**"). Article 10 of the Security Review Measures clarifies that products and services purchased for public communication and information services, energy, transport, water conservancy, finance, public services and electronic government affairs or other operators of CIIs are all significant network products and services that may affect national security, and are therefore subject to the national security review under the CSL. Whether these products or services affect national security is to be determined by government departments responsible for the safety of the CII. The government will set up a cybersecurity review committee and cybersecurity review office.

In addition, the CSL requires dedicated cybersecurity products and critical network equipment to obtain a certification issued by qualified institutions before they can be sold or distributed in China ("**Certification Requirement**"). Such products and equipment must also comply with national standards. The CAC has the obligation to establish a catalogue of critical network equipment and cybersecurity products that will be subject to the Certification Requirement.

On 9 June 2017, the CAC, Ministry of Industry and Information Technology ("**MIIT**"), Ministry of Public Security and Certification and Accreditation Administration, released an Announcement of the Issuance of the Catalogue of Critical Network Equipment and Dedicated Cybersecurity Products (First Batch) ("**First Catalogue**"). Despite being issued on 9 June 2017, the First Catalogue took effect as of 1 June 2017. So far, 15 items have been identified in the First Catalogue as critical network equipment or dedicated cybersecurity products, which are subject to the Certification Requirement. These include firewalls, security audit software, routers, switches, servers, intrusion detection systems, etc. The scope of the Certification Requirement therefore remains quite broad, and the CAC has the flexibility to issue further catalogues of equipment and products.