COMPUTER LAW & SECURITY REVIEW ■■ (2017) ■■–■■

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

ABSTRACT

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).

Qi Chen *(Associate), Mayer Brown LLP* (qchen@mayerbrown.com).

1.1. *New developments relating to China's Cybersecurity Law*

1.1.1. *Background*

China's Cybersecurity Law ("**CSL**") has been in force since 1 June 2017, but a more important deadline for many multinational corporations ("**MNCs**") that operate in China has been deferred to 31 December 2018. This is because the Security Assessment Measures for Cross-Border Transfer of Personal Information and Important Data ("**Cross-Border Measures**") granted an 18 month grace period for network operators to comply with the data transfer rules.[1] Given the uncertainty over how the CSL and the related measures ("**CSL Measures**") will be interpreted and enforced when the grace period ends, new guidelines, measures or regulations are awaited with a certain degree of anticipation. We look at two recent developments relating to the CSL Measures below.

1.1.2. *Enforcement actions under the CSL*

The Cyberspace Administration of China ("**CAC**") announced the commencement of investigations into three of China's largest social media platform operators, Tencent's WeChat, Baidu's Tieba and Sina's Weibo, on 11 August 2017[2] on the grounds that users of these social media platforms had disseminated information that involves violence or terror, false rumours, and pornography or that would otherwise endanger national security, public safety and social order. On 25 September 2017, the Beijing and Guangdong Cyberspace Administration Offices found the three companies to have violated Article 47 of the CSL and fined each company for the maximum amount of fines allowed under Article 68 of the CSL, or 500,000 yuan[3] (about 75,600 USD) ("**Enforcement Actions**"). The fines were based on each company's violation of Article 47 of the CSL, which requires network operators to manage the

[1] For more details on the Cross-Border Measures, please see "Navigating the Latest Developments in China's Cybersecurity Law", Asia IP & TMT Quarterly Review, 2017 Q3, https://www.mayerbrown.com/files/Publication/8f839a9a-104f-4942-afff-e9f0c3d81cbd/Presentation/PublicationAttachment/30e85e12-599b-4db7-b5b5-a68f8793457c/170914-ASI-IP-TMT-QuarterlyReview-2017Q3.pdf.

[2] See http://www.cac.gov.cn/2017-08/11/c_1121467425.htm; Chinese language only.

[3] See http://www.sohu.com/a/194422338_260616 and http://www.sohu.com/a/194423923_260616; Chinese language only.

* Mayer Brown JSM, Hong Kong.
E-mail address: gabriela.kennedy@mayerbrownjsm.com.

https://doi.org/10.1016/j.clsr.2017.12.005

Please cite this article in press as: Gabriela Kennedy, Asia Pacific news, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.12.005

information released by their users and immediately cease the transmission of, and delete or take any other appropriate actions to prevent the spreading of, information which is prohibited by any law or administrative regulations.

Articles 47 and 68 of the CSL apply to network operators and not the more restrictive class of operators of critical information infrastructure ("**CII**").[4] The broad definition of network operator under the CSL potentially extends the applicability of the CSL to any MNC that uses IT systems in China or operates a Chinese website, irrespective of the industry in which the MNC conducts its business. While the companies involved in the Enforcement Actions are amongst the largest Internet companies in China, the same regulations would also apply to any MNC operating in China currently and which uses an IT system that would allow its users to transmit information to others (e.g., an internal company chat room or bulletin board). MNCs operating in China are well advised to immediately start reviewing and monitoring their existing policies and practices to ensure compliance with these and other obligations placed on network operators under the CSL.

1.1.3. *United States tells WTO that it is concerned with China's Cybersecurity Law*

The United States submitted a communication to the World Trade Organization's Council for Trade in Services (the "**Services Council**") on 25 September 2017[5] (the "**Communication**") outlining its concerns with the CSL as part of the Service Council's next agenda. The Services Council is the WTO's council responsible for overseeing the functioning of the General Agreement on Trade in Services (GATS), a trade agreement between all members of the WTO relating to the cross-border trade for services.[6] Under the GATS, member nations agree to adhere to certain principles as they relate to the trade of services such as transparency in trade governance, treating all other member nations equally, and having no discriminatory measures to the detriment of foreign services or service suppliers.[7] While the WTO has a set of dispute resolution rules to help its member nations resolve their differences, this Communication will not trigger the commencement of the dispute resolution process. Instead, the United States may seek to exert more political pressure on China during Services Council meetings and thereby achieve its goal without having to submit a formal WTO complaint.

The Communication notes that the CSL Measures "could have a significant adverse effect on trade in services, including services supplied through a commercial presence and on a cross-border basis." In particular, the United States is concerned that the CSL Measures would: a) encompass any foreign company that has a website or uses the Internet in its business operations; b) place overly burdensome conditions on cross-border transfer of personal information, including the security assessment and obtaining the consent of each individual data subject; and c) create very broad and vaguely defined obligations such as restrictions on cross-border transfer for risks to "national security" or "economic development".

The United States believes the CSL Measures as they are currently written would affect China's "market access and national treatment commitments under the General Agreement on Trade in Services" and China's cross-border commitments to sectors ranging from accounting to travel services. This echoes the same concerns expressed by many MNCs during the public consultation process in the lead up to the passing of the CSL that the CSL Measures will significantly impact their ability to operate in China. In parallel to the Communication, the United States is also feeding through these concerns directly to high level officials in China in the hope of dissuading China from enforcing the CSL Measures in the form in which they are currently written.

2. India

Stephen Mathias *(Partner), Kochhar & Co. (*stephen.mathias@bgl.kochhar.com*).*

Suhas Srinivasiah *(Partner), Kochhar & Co. (*suhas.srinivasiah@bgl.kochhar.com*).*

Naqeeb Ahmed Kazia *(Associate), Kochhar & Co.(*naqeeb.ahmed@bgl.kochhar.com*).*

2.1. *Privacy law updates – Committee issues white paper*

2.1.1. *Introduction*

In August 2017, a constitutional bench of the Supreme Court of India delivered a landmark judgment holding that the right to privacy is a fundamental right under the Constitution of India. Even as arguments were being heard in the case, the Government of India proceeded to appoint a committee to suggest principles to be considered for a data protection regime in India and to draft a new data protection law.

On 27 November 2017, the Committee released a white paper on a data protection framework for India.[8]

2.1.2. *First impressions*

The 200 page white paper covers a wide range of issues concerning privacy and data protection including territorial scope, grounds for processing personal information, individual participation rights, governance issues and remedies. Our first impression is that the committee has done a comprehensive

[4] For more details on the definitions for network operators and CII operators, please see "China Passes Cybersecurity Law" Asia IP & TMT Quarterly Review, 2016 Q4, https://www.mayerbrown.com/files/Publication/4e76421b-7c12-4d24-afe4-620ce0a41b34/Presentation/PublicationAttachment/7e947d52-0a47-4544-b2da-babaf665e476/161222-ASI-IP-TMT-QuarterlyReview-2016Q4.pdf.

[5] Communication From the United States – Measures Adopted and Under Development by China Relating to its Cybersecurity Law, https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspxlanguage=E&CatalogueIdList=239041,239040,239013,239016,239050,239002,238968,238967,238925,238913&CurrentCatalogueIdIndex=7&FullTextHash=371857150&HasEnglishRecord=True&HasFrenchRecord=True&HasS.

[6] See The Services Council, its Committees and Other Subsidiary Bodies, https://www.wto.org/english/tratop_e/serv_e/s_coun_e.htm.

[7] See "The General Agreement on Trade in Services An Introduction" https://www.wto.org/english/tratop_e/serv_e/gsintr_e.pdf.

[8] White Paper of the Committee of Experts on a Data Protection Framework for India, http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf.

Please cite this article in press as: Gabriela Kennedy, Asia Pacific news, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.12.005