CLIENT UPDATE
2016 OCTOBER

TECHNOLOGY, MEDIA & TELECOMMUNICATIONS

PRC Publishes Second Draft of Cybersecurity Law

Overview of the Draft Cybersecurity Law

On 5 July 2016, the second draft of the Cybersecurity Law of the People's Republic of China (the "**Draft Cybersecurity Law**") was published by the Standing Committee of the National People's Congress of the People's Republic China (the "**PRC**"), following the Standing Committee's second reading of the same on 27 June 2016. The Draft Cybersecurity Law contains three notable series of obligations of businesses operating in the PRC technology sphere, namely:

(i) Technology equipment restrictions (Article 22)

(ii) Obligations imposed on Network Operators (Articles 27 – 28, 39 – 48)

(iii) Obligations imposed on Critical Information Infrastructure Operators (Articles 29 – 38)

Technology Equipment Restrictions

The Draft Cybersecurity Law restricts which technology equipment may be marketed and sold within the PRC. Article 22 stipulates that products which fall within the categories of "critical network equipment" and "specialised network security products" must comply with government-issued standards of security and reliability, and must also undergo an inspection and certification process with a qualified institution, before such products and equipment are permitted to be sold in the PRC.

While the Draft Cybersecurity Law does not define specifically the ambit of the terms "critical network equipment" and "specialised network security products", it does envisage that the relevant state authority would be publishing, at an appropriate juncture, a catalogue list detailing specifically which technology products and equipment would be subject to the requirements of Article 22.

The Draft Cybersecurity Law's technology equipment restrictions would therefore be likely to create additional compliance costs for businesses which deal with the relevant technology products in the PRC. Such compliance costs would be magnified if the security standards ultimately imposed by the state authorities are so stringent that such businesses are in effect compelled to modify their products specifically for sale in the PRC.

Obligations imposed on Network Operators

The Draft Cybersecurity Law imposes two broad sets of obligations on entities that are deemed to be Network Operators. The first is a set of data security obligations (found in Articles 39 – 48) relating to the collection, storage and usage of personal data belonging to their users who are citizens of the PRC. These data security obligations would operate in tandem with other provisions of law relating to personal data found in other legislative materials.

The second and more noteworthy set of obligations (found in Articles 27 – 28) compels Network Operators to cooperate with, and provide technical support to, state authorities in the course of their investigations. It is of note that the phrase "necessary support and assistance" in the first draft has now been amended to "technical support and assistance", which has significantly broadened the scope of the support that Network Operators are required to provide. It remains entirely unclear from the expansive drafting of the Draft Cybersecurity Law what types of investigations would be sufficiently serious to compel the assistance of Network Operators. This is of particular concern given the lack of judicial oversight over investigative procedures in the PRC.

CLIENT UPDATE
2016 OCTOBER

TECHNOLOGY, MEDIA & TELECOMMUNICATIONS

Network Operators may therefore face the proposition of having to provide all state authorities with assistance in a wide, undefined array of situations, with such assistance potentially including granting access to confidential data held by the entity and allowing copies of such data to be made. Given the broad drafting of the Draft Cybersecurity Law and onerous obligations imposed on businesses in this regard, there is a real risk that data privacy and intellectual property rights may be compromised in the course of such investigations.

In conjunction with the requirement to assist with investigations, Articles 20 – 21 also require Network Operators to formulate and maintain internal cybersecurity management procedures, to keep network log records for 6 months and to notify the authorities of any security defects discovered in their systems. These obligations would serve to supplement and enable the obligations to provide technical support and assistance found in Articles 27 – 28.

Network Operators in breach of the obligations imposed on them under the Draft Cybersecurity Law may be liable to receive a fine of between 50,000 and 500,000 yuan (7,500 – 75,000USD). Managers of such Network Operators and other directly responsible personnel may also be liable to be fined between 10,000 and 100,000 yuan (1,500 – 15,000USD).

Obligations Imposed on Critical Information Infrastructure Operators

The Draft Cybersecurity Law imposes on Critical Information Infrastructure Operators"("**CIIO**") a significantly more stringent degree of data security obligations as compared to regular Network Operators, largely dealing with the establishment and maintenance of a high level of data security measures, such as setting up specialised internal bodies to handle data security, conducting regular inspections and audits of their network security, and formulating emergency response plans for network security incidents. These requirements are fairly onerous and would undoubtedly require significant costs to be expended in order for compliance to be achieved.

Of particular note are the data localisation obligations found in Article 35, which require CIIOs to store PRC citizens' personal data and other important business data within the geographical boundaries of the PRC. Such critical data is not to be transferred out of the PRC unless it is "truly necessary" and only after the CIIO has conducted the appropriate security risk assessments in accordance with the rules that are eventually to be published by the relevant state department.

CIIOs in breach of the obligations imposed on them under the Draft Cybersecurity Law may be liable to receive a fine of up to 1,000,000 yuan (150,000USD). Managers of such CIIOs and other directly responsible personnel may also be liable to be fined between 10,000 and 100,000 yuan (1,500 – 15,000USD).

Impact Assessment

The PRC government's recent slate of cybersecurity-related laws, including the Draft Cybersecurity Law, generally share a number of common features – the granting of extensive executive powers to state organs, coupled with broadly-drafted legislative provisions and definitions that may impose onerous obligations on businesses and could potentially be utilised to clamp down on online criticism of the PRC government. These broad definitions and provisions will undoubtedly be the source of a great deal of business risk and uncertainty for businesses operating in the PRC technology sector.

With regards to the Draft Cybersecurity Law, a key concern to be highlighted is that the term "Network Operator" is not defined with any clarity. The term has been vaguely defined to mean an "owner or manager of any cyber network, and a network service provider". This definition, when read with the scope of the Draft Cybersecurity Law as stated in Article 2, would arguably be sufficiently broad to cover practically any business that has a presence on the Internet, including any company that merely operates a website which is hosted on a Chinese server or is accessed by users located within the PRC

In a similar vein, it is also unclear which entities exactly would fall within the definition of a CIIO and would be bound by the onerous obligations that CIIOs are subject to. While the first draft of the Law

included a broad list of types of network operators that would be considered CIIOs, this list was removed in the second draft. In its place is a provision stating that the PRC State Council would make a separate enactment detailing the specific scope and ambit of the term "CIIO".

The above points notwithstanding, it must be noted that the Draft Cyber Security Law will have to undergo at least one further round of amendments before it is formally enacted, and it is difficult to predict what further changes the PRC government may make following its analysis of the public response to this second draft. Further, as is usually the case in the PRC, the full impact of the Draft Cybersecurity Law cannot be determined with full certainty until the relevant executive and judicial state authorities have had an opportunity to enforce and interpret the legislative provisions. With that in mind, businesses operating in the technology sphere in the PRC should therefore continue to pay close attention to further developments in the PRC cybersecurity arena.

Contacts

Benjamin Cheong
Partner
Rajah & Tann Singapore LLP

D (65) 6232 0738
F (65) 6428 2233
benjamin.cheong@rajahtann.com

Linda Qiao
Senior International Counsel
Rajah & Tann Singapore LLP
Shanghai Representative Office
D (86) 21 6120 8818
F (86) 21 6120 8820

linda.qiao@rajahtann.com

Please feel free to also contact Knowledge and Risk Management at eOASIS@rajahtann.com

ASEAN Economic Community Portal

With the launch of the ASEAN Economic Community ("**AEC**") in December 2015, businesses looking to tap the opportunities presented by the integrated markets of the AEC can now get help a click away. Rajah & Tann Asia, United Overseas Bank and RSM Chio Lim Stone Forest, have teamed up to launch "Business in ASEAN", a portal that provides companies with a single platform that helps businesses navigate the complexities of setting up operations in ASEAN.

By tapping into the professional knowledge and resources of the three organisations through this portal, small- and medium-sized enterprises across the 10-member economic grouping can equip themselves with the tools and know-how to navigate ASEAN's business landscape. Of particular interest to businesses is the "Ask a Question" feature of the portal which enables companies to pose questions to the three organisations which have an extensive network in the region. The portal can be accessed at http://www.businessinasean.com/.

Our regional presence

Our regional contacts

RAJAH & TANN | *Singapore*

Rajah & Tann Singapore LLP
9 Battery Road #25-01
Straits Trading Building
Singapore 049910
T +65 6535 3600 F +65 6225 9630
sg.rajahtannasia.com

R&T SOK & HENG | *Cambodia*

R&T Sok & Heng Law Office
Vattanac Capital Office Tower, Level 17, No. 66
Preah Monivong Boulevard, Sangkat Wat Phnom
Khan Daun Penh, 12202 Phnom Penh, Cambodia
T +855 23 963 112 / 113 F +855 963 116
kh.rajahtannasia.com
**in association with Rajah & Tann Singapore LLP*

RAJAH & TANN REPRESENTATIVE OFFICE | *China*

Rajah & Tann Singapore LLP
Shanghai Representative Office
Unit 1905-1906, Shui On Plaza, 333 Huai Hai Middle Road
Shanghai 200021, People's Republic of China
T +86 21 6120 8818 F +86 21 6120 8820
cn.rajahtannasia.com

RAJAH & TANN NK LEGAL | *Myanmar*

Rajah & Tann NK Legal Myanmar Company Limited
Myanmar Centre Tower 1, Floor 07, Unit 08,
192 Kaba Aye Pagoda Road, Bahan Township,
Yangon, Myanmar
T +95 9 73040763 / +95 1 657902 / +95 1 657903
F +95 1 9665537
mm.rajahtannasia.com

RAJAH & TANN | *Singapore*

ASSEGAF HAMZAH & PARTNERS | *Indonesia*

Assegaf Hamzah & Partners

Jakarta Office
Menara Rajawali 16th Floor
Jalan DR. Ide Anak Agung Gde Agung Lot #5.1
Kawasan Mega Kuningan, Jakarta 12950, Indonesia
T +62 21 2555 7800 F +62 21 2555 7899
www.ahp.co.id

Surabaya Office
Pakuwon Center, Superblok Tunjungan City
Lantai 11, Unit 08
Jalan Embong Malang No. 1, 3, 5, Surabaya 60261, Indonesia
T +62 31 5116 4550 F +62 31 5116 4560

** Assegaf Hamzah & Partners is an independent law firm in Indonesia and a member of the Rajah & Tann Asia network.*

CHRISTOPHER & LEE ONG | *Malaysia*

Christopher & Lee Ong
Level 22, Axiata Tower, No. 9 Jalan Stesen Sentral 5,
Kuala Lumpur Sentral, 50470 Kuala Lumpur, Malaysia
T +60 3 2273 1919 F +60 3 2273 8310
www.christopherleeong.com
**in association with Rajah & Tann Singapore LLP*

RAJAH & TANN | *Thailand*

Rajah & Tann (Thailand) Limited
973 President Tower, 12th Floor, Units 12A-12F
Ploenchit Road, Lumpini, Pathumwan
Bangkok 10330, Thailand
T +66 2 656 1991 F +66 2 656 0833
th.rajahtannasia.com

RAJAH & TANN | *Lao PDR*

Rajah & Tann (Laos) Sole Co., Ltd.
Phonexay Village, 23 Singha Road, House Number 046/2
Unit 4, Saysettha District, Vientiane Capital, Lao PDR
T +856 21 454 239 F +856 21 285 261
la.rajahtannasia.com

RAJAH & TANN LCT LAWYERS | *Vietnam*

Rajah & Tann LCT Lawyers

Ho Chi Minh City Office
Saigon Centre, Level 13, Unit 2&3
65 Le Loi Boulevard, District 1, HCMC, Vietnam
T +84 8 3821 2382 / +84 8 3821 2673 F +84 8 3520 8206

Hanoi Office
Lotte Center Hanoi - East Tower, Level 30, Unit 3003,
54 Lieu Giai St., Ba Dinh Dist., Hanoi, Vietnam
T +84 4 3267 6127 F +84 4 3267 6128
www.rajahtannlct.com

Rajah & Tann Singapore LLP is one of the largest full service law firms in Singapore, providing high quality advice to an impressive list of clients. We place strong emphasis on promptness, accessibility and reliability in dealing with clients. At the same time, the firm strives towards a practical yet creative approach in dealing with business and commercial problems. As the Singapore member firm of the Lex Mundi Network, we are able to offer access to excellent legal expertise in more than 100 countries.

Rajah & Tann Singapore LLP is part of Rajah & Tann Asia, a network of local law firms in Singapore, Cambodia, China, Indonesia, Lao PDR, Malaysia, Myanmar, Thailand and Vietnam. Our Asian network also includes Singapore-based regional desks focused on Japan and South Asia.