CLIENT UPDATE
2016 JANUARY

TECHNOLOGY, MEDIA & TELECOMMUNICATIONS

# China's New Anti-Terrorism Law: Implications for Firms Dealing with Data in China

- Broadly drafted provisions grant Chinese authorities significant scope of powers to access and deal with data.
- Data security and privacy potentially at great risk.
- Significant impact warrants consideration by all companies doing business in China with data such as data centre operators, internet service providers and telecoms companies.

## Introduction

On 27 December 2015, China's National People's Congress Standing Committee passed a new anti-terrorism law (the "**Law**") that creates a legal framework providing Chinese authorities with wide-ranging powers to compel the cooperation and assistance of technology firms in the country's war against terrorism. The Law came into effect on 1 January 2016.

This client update will analyse the Law and the specific obligations and restrictions imposed by its relevant cybersecurity provisions, examining its impact on pertinent issues such as data privacy and discussing the broader implications stemming from this law for technology firms seeking to do business in the People's Republic of China (the "**PRC**").

## The Cybersecurity Provisions

The purpose of the Law is to prevent and punish terrorist activities, strengthen counter-terrorism efforts and to safeguard the security of the state, the public, and the lives and properties of the people.

The term "terrorism" has been defined in the Law to mean "propositions and actions that create social panic, endanger public safety, violate person and property, or coerce national organs or international organizations, through methods such violence, destruction, intimidation, so as to achieve their political, ideological, or other objectives". The specific terrorist acts targeted by the Law are:

(1) Activities that seriously harm society such as the organizing, planning, preparing for, or carrying out any of the following conduct so as to cause injuries to persons, major property damage, damage to public facilities, or havoc in public order;

(2) Advocating terrorism, inciting others to commit terrorist activities, unlawfully possessing items that advocate terrorism, or compelling others to wear or bear clothes or symbols that advocate terrorism in a public place;

(3) Organizing, leading, or participating in a terrorist organization;

(4) Providing information, capital, funding, labour, technology, venues or other support, assistance or facilitation to terrorist organizations, terrorist activity personnel, or the commission of terrorist activities;

(5) Other terrorist activities.

# CLIENT UPDATE
# 2016 JANUARY

**TECHNOLOGY, MEDIA & TELECOMMUNICATIONS**

While most of the Law deals with broad national security and counter-terrorism initiatives, the provisions that have received the most global scrutiny and bear the most relevance to foreign technology companies which do business in the PRC are Articles 18 and 19, which impose certain statutory restrictions and obligations on technology companies:

> **Article 18:** Telecommunications operators and internet service providers shall provide technical support and assistance, such as technical interfaces and decryption technology, to public and national security agencies in the prevention and investigation of terrorist activities in accordance with the law.
>
> **Article 19:** Telecommunications operators and internet service providers shall, in accordance with provisions of law and administrative regulations, implement network security systems, information content monitoring systems, and technical prevention and safety measures, to prevent the dissemination of information with terrorist or extremist content. Should information with terrorist or extremist content be discovered, its dissemination shall immediately be halted, with relevant records saved and the relevant information deleted, and a report shall be made to public security agencies or other relevant departments.
>
> Where departments responsible for network communications, telecommunications, public security, state security and other such departments discover any information with terrorist or extremist content, they shall promptly order the relevant units to stop its transmission, to delete the relevant information, to close the relevant websites, and to terminate relevant services. The relevant units shall immediately enforce such orders and save relevant records to assist in investigations. Departments responsible for network communications shall adopt technical measures to disrupt the cross-border transmission of information with terrorist or extremist content.

## Impact of the Law

The Law has drawn much criticism and controversy from human rights groups and technology companies ever since the draft version of the Law was published in early 2015. Critics of the Law have voiced concerns about two main elements in particular – the Law's onerous and invasive cybersecurity restrictions, and its broadly worded definition of "terrorism". There are fears that this law potentially heralds the death of data security and privacy in the PRC as it ostensibly confers upon Chinese authorities the ability to compel technology companies to hand over all of their data, private or otherwise, in the name of national security and prevention of terrorism. This may result in technology companies eventually having to decide whether they want to stay in the PRC and basically submit to governmental surveillance, or to stop doing business in the PRC altogether.

Articles 18 and 19 of the Law specifically target "telecommunications operators and internet service providers". It should be noted that the Law itself, and indeed PRC laws in general, do not define the terms "telecommunications operators" and "internet service providers" and therefore these terms can be interpreted widely to include any company providing technology, internet or telecommunications services in the PRC and to companies and individuals in the PRC, such as providers of e-commerce, mobile application, data storage, or cloud services. It is also unclear whether the Law only applies to companies located in the PRC or whether it also applies to technology companies located outside its borders. Although traditionally the PRC authorities only exercise jurisdiction over companies located within the PRC, Article 11 of the Law provides, almost as a warning, that "the PRC exercises criminal jurisdiction and lawfully pursues criminal responsibility for terrorist activity crimes committed against the State of the PRC or its citizens or organizations thereof outside the territory of the PRC, as well as terrorist activity crimes committed that are stipulated in international treaties concluded with or joined by the PRC". The Law also provides for a wide scope of international cooperation on anti-terrorism activities, which may provide a legal basis for drawing foreign technology companies within the PRC government's reach.

Under the Law, telecommunications operators and internet service providers are required to hand over any and all relevant technical information or decryption technology when required for the investigation or prevention of terrorist acts. The Law also requires technology companies to actively disrupt and prevent the dissemination of any terrorist messages whenever such activities are discovered. Not only are these

broadly worded obligations which have the potential to be highly onerous, there is a risk that the disclosure of technical data and decryption technology may lead to intellectual property rights being compromised.

In the event that telecommunications operators or internet service providers:

(1) fail to provide technical interfaces, decryption and other technical support assistance to public security organs and state security organs conducting prevention and investigation of terrorist activities in accordance with law;

(2) fail to follow a competent department's request to stop transmission, delete information that has terrorist or extremist content, store relevant records, close down relevant websites, or shut down related services; or

(3) fail to put into place systems for network security and supervision of information content, technological security precautionary measures, causing the transmission of information with terrorist or extremist content; where the circumstances are serious,

the competent authorities may fine these companies between 200,000 and 500,000 yuan (30,000 – 75,000USD), and fine directly responsible managers and other directly responsible personnel up to 100,000 yuan (15,000USD). Where the circumstances are serious, the fine for companies is 500,000 yuan (75,000USD) or more, and directly responsible managers and other directly responsible personnel may be fined between 100,000 and 500,000 yuan (15,000 – 75,000USD). Public security organs may also detain directly responsible managers and other directly responsible personnel for between 5 and 15 days. The fact that there is personal liability for managers, including possible detention, should certainly be cause for alarm for technology companies.

While this is a step back from the initially released draft provisions, which required technology companies to install security back-doors into their networks and software and to store all encryption data with Chinese authorities, the present iteration of the Law still confers upon Chinese authorities broad powers and a stronger legal basis to demand and access sensitive data. This is especially so in light of how, under the Law, terrorism and extremism are defined in a manner that could even include political criticism and dissidence of a non-violent nature. The exercise of intrusive powers to monitor and suppress dissidents is nothing out of the ordinary for the Chinese government, but in this regard, the passing of the Law gives it greater legal impetus to do so.

The Chinese government has responded to criticisms of the Law by noting that Western governments, such as the UK and the US, have been making similar demands for technology companies to disclose encryption data for years. The Chinese government has also issued a public statement reassuring foreign businesses that the new rules would not inordinately affect any company's ordinary business activities .

## Implications for Firms

In response to the passing of this law, it would be prudent for technology firms who operate in the PRC to review their data security and encryption measures, and to consider how they might want to respond to any demands made of them by Chinese authorities in the exercise of their powers under the Law. While technology firms have previously been able to rebuff demands made by UK and US authorities for sensitive information and encryption data, the commercial repercussions of such an approach in the PRC may be substantial. Such issues warrant greater consideration by foreign technology companies who have large stakes in the PRC and who are thus likely to bear the brunt of Chinese governmental scrutiny.

In a similar vein, the true overall impact of the Law remains to be seen, and much would likely depend on how much restraint the Chinese authorities will exercise in using its newfound powers. Nevertheless, the passing of this new law serves as a clear signal of the Chinese governement's desire to exercise greater oversight and control over the technological and informational networks within its territory, and is a signal that foreign businesses, and technology and telecoms firms in particular, would do well to heed.

# CLIENT UPDATE
2016

## Contacts

**Rajesh Sreenivasan**
Head, Technology, Media & Telecommunications

D (65) 6232 0751
F (65) 6428 2204
rajesh@rajahtann.com

**Steve Tan**
Deputy Head, Technology, Media & Telecommunications

D (65) 6232 0786
F (65) 6428 2216
steve.tan@rajahtann.com

**Lionel Tan**
Partner

D (65) 6232 0752
F (65) 6428 2119
lionel.tan@rajahtann.com

**Benjamin Cheong**
Partner

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**
Office Suite 007, Inya Lake Hotel No. 37, Kaba Aye
Pagoda Road, Mayangone Township, Yangon, Myanmar
T +95 9 73040763 / +95 1 657902 / +95 1 657903
F +95 1 9665537
mm.rajahtannasia.com

**ASSEGAF HAMZAH & PARTNERS** | *Indonesia*

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

**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

**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 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