Client Alert

January 20, 2016

China's Anti-Terrorism Law Raises Data Security Concerns

By Paul McKenzie, Gordon Milner, and Wei Zhang

As discussed in our March 2015 alert, China's legislature, the National People's Congress (the "NPC"), had issued a November 2014 draft Anti-Terrorism Law (反恐怖主义法) that included relatively far-reaching data privacy and data localization provisions that caused widespread concerns among international businesses. The NPC finally passed the Anti-Terrorism Law (the "Law") on December 27, 2015, following its third reading, and the Law came into effect on January 1, 2016. The NPC adjusted the controversial provisions in the Law, as promulgated, but provisions that remain are only slightly less controversial.

Morrison & Foerster's unofficial English translation of the provisions of the Law discussed in this Alert are available by contacting us through this email.

REGULATORY BACKDOORS CLOSED – OR NOT

Two features of the November 2014 draft law that caused particular concerns were requirements that "telecommunications service providers" and "internet service providers":

- file their encryption solutions with the Chinese government and embed a "technical interface" in the construction of their networks – vague language that commentators understood to mean that PRC government authorities would have broad rights to monitor network use;
- keep relevant equipment and data in respect of local users within the territory of China.

Under the final version of the Law:

- the data localization requirement has been completely removed; and
- the requirement to file encryption solutions with the Chinese government and embed a technical interface in relevant networks has been replaced by a vaguer and more general requirement under Article 18 of the Law for telecommunications service providers and internet service providers to "provide technical support and assistance, such as technical interface and decryption, to support the activities of the public security and state security authorities in preventing and investigating terrorist activities."

The official position is that the more general language of the final version of the Law ought to address concerns about the network security provisions of the draft. An official of the NPC's Legislative Affairs Commission, Li Shouwei, commented during a press conference held in relation to promulgation of the Law that the Article 18 requirement to provide technical support and assistance "will not affect companies' normal business operation or require installation of backdoors permitting infringement of intellectual property rights." Businesses might not take significant comfort from

Mr. Li's comments, given the breadth and vagueness of Article 18.

Article 18 applies broadly to telecommunications service providers and internet service providers, terms that are not defined in the law itself but that, as understood under PRC telecommunications regulations, ought to refer broadly to, respectively, any company that provides telecommunications services subject to issuance of a telecommunications license, including companies engaged in value-added telecommunications, and any company that operates a website or engages in other services via the Internet utilizing servers located in China. As such, a broad range of companies with an internet presence in China are subject to Article 18.

It may be good news that the Law as promulgated does not expressly require the filing of encryption solutions or mandate backdoors. Nonetheless Article 18 seems to leave local public security and state security authorities with broad discretionary authority to require companies to provide access to their equipment and decryption support in particular cases. Potentially that discretionary authority will be circumscribed somewhat in future implementing rules issued under the Law. Nonetheless, the wording of Article 18 is at least worrisome. Failure to comply with Article 18 can attract penalties, if the circumstances are serious, that include fines of more than RMB 500,000 for the company and fines of up to RMB 500,000 and criminal detention of up to 15 days for the relevant responsible person (Article 84).

TERRORIST CONTENT TARGETED

The Law as promulgated retains language from the November 2014 draft in regard to content censorship. Article 19 requires telecommunications business operators and Internet service providers (again broadly defined) to implement network security and content censorship measures to prevent dissemination of any information with terrorist or extremist content and to report to the public security or other government authority when identifying such information. These requirements largely mirror requirements in regard to illegal information provided under existing telecommunication regulations. The definition of "terrorism" in the Law is broad, including "propositions and actions that create social panic, endanger public safety, violate person or property, or coerce national organs or international organizations, through methods such as violence, destruction, intimidation, so as to achieve their political, ideological, or other objectives." The Law does not provide a definition of "extremism".

REAL-NAME REGISTRATION

The real-name registration requirement of Article 21 of the Law is also notable. Article 21 requires a broad range of businesses, including business operators and services providers in the telecommunications, Internet, financial, lodging, long-distance passenger transportation, and vehicle rental sectors to verify the identities of customers and prohibit the provision of services to customers whose identities are unclear or who refuse to cooperate in the verification process. This requirement builds on the real-name registration requirement applicable to internet service providers providing internet information services such as blogs, microblogs, instant messaging tools, and forums under the Administrative Provisions on the Account Names of Internet Users (互联网用户账号名称管理规定), which took effect on March 1, 2015.

LOOKING FORWARD

As noted above, it will be interesting to see if implementing rules are issued under the Law to clarify the obligations of telecommunications and internet services providers and the enforcement powers of relevant authorities, in regard to network security.

Promulgation of the Law is only one element of a sustained focus by the Chinese government on network security. The State Security Law (国家安全法) promulgated on July 1, 2015, provides the State with broad authority to implement a system for maintaining the security of networks and information. A draft Cyber Security Law (网络安全法(草案)) published for comments on July 6, 2015, proposed various specific information security and network security measures to enhance "cyber sovereignty" (see our Client Alert on July 20, 2015). 2016 will doubtless witness continued efforts by the Chinese government to enhance information and network security that will significantly impact the operating environment for companies that are doing business in China.

Contacts:

Paul McKenzie
+86 (10) 5909-3366
pmckenzie@mofo.com

Gordon Milner
+852 2585-0808
gmilner@mofo.com

Wei Zhang
+86 (10) 5909-3382
weizhang@mofo.com

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer*'s A-List for 12 straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.