COVINGTON

China Enacts Broad Counter-Terrorism Law

January 5, 2016

China

On December 27, 2015, the Standing Committee of the National People's Congress (NPC), China's top legislative body, enacted a Counter-Terrorism Law (see the Chinese version here), which took effect on January 1, 2016. The adoption of this law, a year after the first draft was released for public comment, followed closely the adoption of a new National Security Law and other legislative initiatives related to national security and cyber-security.

The Counter-Terrorism Law reinforces the government's broad powers to investigate and prevent incidents of terrorism and requires citizens and companies to assist and cooperate with the government in such matters. The law imposes additional and specific obligations on companies in certain sectors. Non-compliance or non-cooperation can lead to significant penalties, including fines on companies and criminal charges or detention for responsible individuals.

This alert summarizes the key features of the new law and explains its potential impact on foreign businesses operating in China, particularly those in the telecommunications, Internet services, and financial services sectors.

Background

Since 2013, the Chinese government, led by the National Security Commission (headed by President Xi Jinping), has prioritized developing a legal framework that can support China's efforts to meet security challenges during a time of globalization and rapidly changing information technology. Under this initiative, several broad laws have been developed.

The new National Security Law, adopted on July 1, 2015, includes a sweeping concept of national security and imposes broad obligations on citizens and corporations to assist and cooperate with the government. This law, analyzed in Covington's alert here, provides an overarching legal framework and lays the foundation for government agencies to issue follow-on measures.

Other legislative proposals moving in parallel have included a new Counter-Espionage Law (adopted November 1, 2014) and a draft Cybersecurity Law (last version released for comments in July 2015, see Covington alert here). Certain provisions in these two pieces of legislation overlap with the National Security Law, but they each have a much narrower focus.

Legislative History

The first draft of the Counter-Terrorism Law was released for public comment in November 2014, and a second draft was released in February 2015. These drafts covered the definition of terrorism, procedures to designate a terrorist organization or individual, functions and

responsibilities of counter-terrorism agencies, response plans for terrorist attacks, international counter-terrorism cooperation, and obligations on citizens and companies to assist and cooperate with the government.

In addition to imposing broad obligations to assist and cooperate, the drafts required companies operating in certain sectors to take specific actions when investigating terrorism cases. For example, providers of telecommunications or Internet services were required to (i) install "backdoors" in their products; (ii) register their encryption keys with the government before such keys could be used; and (iii) keep relevant equipment and data of Chinese users within China.

Some of these specific requirements have been modified or removed in the final version, but many remain. In the final version, companies in many sectors, such as freight, transportation, and hospitality (including car rental), as well as providers of telecommunications, Internet, and financial services, are required to conduct identity checks of their customers or clients and refuse to provide services to those that decline to provide such information (Article 21). Freight companies are similarly required to conduct security checks or inspections of packages to be delivered and must refuse to deliver products that have not passed the checks or inspections (Article 20). Other specific obligations for providers of telecommunications, Internet, and financial services are explained below.

Obligations on Providers of Telecommunications and Internet Services

The final version of the law does not mention the requirements in the drafts to register encryption keys and keep servers and user data within China, but it still requires companies in the telecommunications and Internet services sectors to:

- Provide technical support and assistance, including handing over access or interface information and decryption keys (Article 18); and
- Establish content monitoring and network security programs and adopt precautionary security measures to prevent the dissemination of information on extremism, report terrorism information to the authorities in a timely manner, keep original records, and promptly delete such messages to prevent further circulation (Article 19).

Non-compliance with the assist-and-support obligations may result in fines on both companies and responsible individuals, as well as detention or criminal charges against responsible employees (Articles 84). More generally, non-cooperation with investigations or the intelligence collection process can also result in fines or detention of responsible employees (Article 91).

Given that law enforcement authorities in China already have very broad access to information and data in national security and criminal investigations, Article 18 may not significantly change the scope of such access or affect companies' normal operations. However, Article 19 imposes an additional obligation on telecommunications and Internet service operators not specifically required in the past: they must proactively monitor their networks for terrorism information and disclose such information to the authorities. The law has not clarified what types of content monitoring and security programs will be deemed as sufficient, but implementation guidelines providing further details are expected to be issued soon.

Obligations of Financial Services Providers

Financial institutions and certain non-financial institutions, including third-party payment service providers, are required under the law to freeze funds and assets of designated terrorist

organizations and individuals, and immediately notify police, national security agencies, and anti-money laundering agencies about such freezes (Article 14). Moreover, anti-money laundering agencies may initiate investigations if terrorist financing risks are identified and temporarily freeze accounts or assets (Article 24).

Financial institutions and certain non-financial institutions have long been required by the People's Bank of China (PBOC), the agency responsible for anti-money laundering efforts, to take action if terrorist financing is suspected. The obligations specified in Articles 14 and 21 of this law are largely consistent with obligations imposed by previous anti-money laundering laws and regulations, such as the Anti-money Laundering Law (October 2006) and the Regulations on the Reporting of Suspected Transactions Involving Terrorist Financing by Financial Institutions (June 2007). More importantly, in 2014, PBOC joined other agencies in issuing a Regulation on the Freezing of Assets Involving Terrorist Actions, which sets forth detailed rules on how to freeze funds and assets of designated terrorist organizations and individuals. The new law is unlikely to change the practices of these agencies, but provides a higher level of legal authority to enforce such rules. The new law also provides tougher (and more specific) penalties for non-compliance or non-cooperation, including fines and criminal charges against financial services providers and responsible individuals (Articles 83, 86, and 91).

* * *

If you have any questions concerning the material discussed in this client alert, please contact the following attorneys:

Eric Carlson	+86 21 6036 2503	ecarlson@cov.com
Tim Stratford	+86 10 5910 0508	tstratford@cov.com
Yan Luo	+86 10 5910 0516	yluo@cov.com
Ashwin Kaja	+86 10 5910 0506	akaja@cov.com