Financial institutions
Energy
Infrastructure, mining and commodities
Transport
Technology and innovation
Life sciences and healthcare

NORTON ROSE FULBRIGHT

Cyber security in China

Draft law strengthens regulation of internet and data privacy

Briefing

July 2015

Summary

China's draft Cyber Security Law demonstrates the Chinese government's ongoing commitment to enhance the security and supervision of Internet and telecommunication networks. The law, if adopted in its current form, will apply to both Chinese and international businesses for their operations in China. Public consultation for the draft law is open until August 5, 2015.

Introduction

The National People's Congress, the top legislature of China, published a draft Cyber Security Law (the Draft Law) on July 6, 2015 for the purpose of receiving comments from the general public. The Draft Law, if enacted in its current form, will have far-reaching consequences for businesses (both domestic and international) operating in China.

The Draft Law provides that its objectives are to:

- safeguard China's cyber sovereignty
- put protections in place against cyber attacks
- augment Internet safety
- regulate the use of personal data.

The Draft Law is an important regulatory development that follows on from the recent implementation of the People's Republic of China's (PRC) National Security Law (published on July 1, 2015). The deadline for submitting comments in relation to the Draft Law is August 5, 2015.

Scope and application

The Draft Law has wide application. It covers the construction, operation, maintenance and usage of networks, as well as the supervision and management of cyber security within the mainland of the PRC.

Under the Draft Law, 'network operator' is widely defined. It includes owners, administrators and network service providers who use a network owned or administrated by another in order to provide relevant services, including telecommunications operators, Internet information services providers and important information system operators.

The Draft Law expressly provides that it will apply equally to both Chinese and international businesses.

Augmenting cyber security requirements

Under the Draft Law, network operators are required to comply with new stringent obligations in connection with cyber security. Specifically, network operators:

- Must formulate internal cyber security system and operation protocols and must adopt strong technical measures in order to prevent computer viruses and cyber invasions and attacks.
- Can only procure network products or services that comply with the relevant national and industry standards, and the suppliers of network products and services are prohibited from installing any malicious computer programs within such products and services. Where network operators are aware of any security flaws or other risks in network products or services, they must take responsive action immediately and promptly notify affected users.
- Are obliged to verify the identity of users when providing services such as landline and mobile subscription, Internet access and domain name registration. Network operators are prohibited from providing such services until a user has sufficiently disclosed its identity.
- Must set up an emergency response system and have the emergency plans in place. The Draft Law empowers the State Council, and provincial governments upon approval by the State Council, to restrict Internet communication where public security emergencies occur.

In addition, the Draft Law provides that 'key network equipment' and 'specialised network security products' must be either certified or tested by licensed security certification institutions (in order to ensure compliance with mandatory requirements under applicable national and industry standards) before such equipment or products can be put onto the market.

According to the Draft Law, a cyberspace regulator (the Cyberspace Administration of China (CAC)), will work jointly with other Chinese regulators in order to formulate and publish a catalogue of what will constitute 'key network equipment' and 'specialised network security products' for certification purposes. CAC will also promote the recognition and simplification of the certification process.

Special requirements for crucial information infrastructure facilities

The Draft Law provides for strengthened protection in relation to the operation of crucial information infrastructure facilities.

According to the Draft Law, 'crucial information infrastructure facilities' refers to the following:

- basic information networks that provide services such as public communications and radio and television broadcasts
- crucial information systems for key industries such as energy, transportation, water, financial institutions and public utilities (such as electricity supply, water supply, gas supply, medical/healthcare and social security)
- military networks for the PRC military
- networks of governmental departments at or above city level
- internet networks and systems owned or managed by network service providers with massive numbers of Internet users.

The wide scope of what could constitute 'crucial information infrastructure facilities' means that the Draft Law could cast a wide net over a broad range of sectors, and both network operators and network products and services providers will be affected.

Under the Draft Law, operators of 'crucial information infrastructure facilities' are subject to the following obligations (in addition to the general network security responsibilities already described):

- Procurement of network products or services that may give rise to national security concerns will be subject to a security review jointly conducted by CAC and other relevant governmental agencies.
- Operators must enter into a security and confidentiality agreement with suppliers of network products and services.
- Where operators collect or generate personal information or other important data in the course of network operation in China, such information or data must be stored in China, subject to an exception. That exception is potentially available where an operator wishes to store such information or data outside China for business purposes, but in such a case such storage must first be approved by a security review conducted by CAC.
- Operators of crucial information infrastructure facilities must conduct an annual security review either by themselves or by appointing a qualified third party and must adopt proper measures for security risk mitigation.

Data privacy

In the absence of a comprehensive data privacy law in China, the Draft Law contains certain provisions in relation to personal data privacy and data protection to supplement existing data privacy rules which are scattered in various administrative regulations and judicial interpretations.

The Draft Law stipulates that network operators must improve protection for personal data, privacy and commercial confidentiality. Where network operators collect and use personal data, they must follow principles of legality, propriety and necessity. Data collectors must notify data subjects of the purpose, manner and scope of data collection and usage, and express consent must be obtained from the data subjects.

The Draft Law also provides that network operators:

- are obliged to safeguard the secrecy of personal data collected
- must take technical and other appropriate steps to avoid data leakage or loss (reporting to relevant authorities and notification to data subjects are required in case of data leakage or loss).

Perhaps in order to address concerns recently expressed by IT suppliers and network operators that are required to file their network encryptions or source codes with regulators, the Draft Law provides that governmental officials in charge of supervision and administration of network security must protect the secrecy of personal data, privacy and confidentiality of information to which they have access.

Legal liability

Businesses will be subject to liability and to various sanctions for breach of the requirements under the Draft Law.

For example, an operator of crucial information infrastructure facilities may face a fine of up to RMB500,000, and suspension of its business licence, if it stores data overseas without first undergoing the security review as required under the Draft Law.

Practical implications

The Draft Law demonstrates the Chinese government's ongoing commitment to enhance the security and supervision of Internet and telecommunication networks. As noted above, the law, if adopted in its current form, will apply to both Chinese and international businesses for their operations in China. The new requirements in relation to cybersecurity standards and procurement requirements will therefore have significant operational and business implications for domestic and international network operators, as well as for suppliers of network products and services.

While IT, Internet and telecommunication industries will clearly be affected, the implications of the Draft Law may also extend to businesses operating in the energy, financial services, transport, medical/healthcare and other public services sectors.

The Draft Law is open to public discussion and feedback from interested parties until August 5, 2015. According to the Xinhua News Agency, the legislator had received more than 1,000 submissions by July 10, just three days after the Draft Law had been made public. We intend to monitor progress of the Draft Law and to provide updates of significant developments.

Contacts

If you would like further information please contact:

Barbara Li
Partner, Beijing
Tel +86 10 6535 3130
barbara.li@nortonrosefulbright.com

Rachel Xia
Senior associate, Beijing
Tel +86 10 6535 3132
rachel.xia@nortonrosefulbright.com

Norton Rose Fulbright

Norton Rose Fulbright is a global legal practice. We provide the world's preeminent corporations and financial institutions with a full business law service. We have more than 3800 lawyers and other legal staff based in more than 50 cities across Europe, the United States, Canada, Latin America, Asia, Australia, Africa, the Middle East and Central Asia.

Recognized for our industry focus, we are strong across all the key industry sectors: financial institutions; energy; infrastructure, mining and commodities; transport; technology and innovation; and life sciences and healthcare.

Wherever we are, we operate in accordance with our global business principles of quality, unity and integrity. We aim to provide the highest possible standard of legal service in each of our offices and to maintain that level of quality at every point of contact.

Norton Rose Fulbright US LLP, Norton Rose Fulbright LLP, Norton Rose Fulbright Australia, Norton Rose Fulbright Canada LLP and Norton Rose Fulbright South Africa Inc are separate legal entities and all of them are members of Norton Rose Fulbright Verein, a Swiss verein. Norton Rose Fulbright Verein helps coordinate the activities of the members but does not itself provide legal services to clients.