COVINGTON

China Solicits Comments on Draft Network Security Law

July 10, 2015

Cybersecurity

On July 6, 2015, China's National People's Congress (NPC) released for public comment a draft of the *Network Security Law* ("Draft Law," referred to in some press articles as the Cybersecurity Law). Comments can be submitted through the NPC website or by mail before August 5, 2015.

This Draft Law, initially reviewed by the NPC in June, would apply broadly to entities or individuals that construct, operate, maintain, and use networks within the territory of China, as well as those who have the responsibility to supervise and manage network security. A number of the provisions in this Draft Law, if enacted in their current form, are likely to significantly impact information technology and communication companies with business operations or interests in China.

The release of the draft follows closely on the heels of the new National Security Law that was enacted last week (see Covington e-alert here).

Impetus of the Draft Law

According to the legislative notes accompanying the Draft Law, the government views network security as crucial to national security and development. The Draft Law is intended to address a number of network-related risks, including the serious threats posed by cyberattacks on key information infrastructure, cybercrimes related to personal data or intellectual property, and unlawful online activities that could raise national security concerns.

The Draft Law thus focuses first on the security challenges facing information infrastructure in a wide range of "key" sectors, such as telecommunications, energy, transportation, finance, and national defense, particularly in light of the proliferation of new technologies and applications such as cloud computing, big data, and the internet of things. It then addresses cybercrimes such as disclosure and resale of personal data and the online infringement of intellectual property. Finally, a number of provisions in the Draft Law regulate certain online activities related to terrorism or extremism and the stability of the government and the socialist system.

The 68 articles of the Draft Law are divided into seven chapters. The first two chapters discuss general principles (Chapter 1) and the government's cyber security strategy (Chapter 2). Chapter 3 provides detailed rules on how the government intends to protect the "secure" operation of cyberspace. Chapter 4 focuses on data privacy issues, and Chapter 5 on network monitoring and emergency response. Chapter 6 provides penalties for violation of network security rules, and is followed by definitions and other supplementary provisions in Chapter 7.

Among the seven chapters, Chapters 3 and 4 merit the particular attention of IT and communications companies as they set forth a broad range of obligations and responsibilities but also leave many questions unanswered regarding their application and interpretation.

"Secure" Operation of Networks and "Critical Information Infrastructure"

Provisions in Chapter 3 provide that a wide group of entities, including network operators, suppliers of network products and services, and operators of "critical information infrastructure" (as defined below), must ensure that networks operate securely. Obligations imposed on network operators mostly relate to the data privacy of users and are discussed in further detail below together with a discussion of other data-related requirements. Rules related to "critical information infrastructure," as discussed below, may be most concerning for IT and communications companies, especially if they are classified either as operators of critical information infrastructure or as suppliers of such operators.

Critical Information Infrastructure

"Critical information infrastructure" is defined to include the following types of systems:

- Basic networks for public communications and radio and television transmission services;
- Critical information systems for:
  - key industries such as energy, transportation, water conservancy, finance;
  - public service sectors such as power, water and gas utilities, health care, social security, etc.;
  - military networks and government networks; and
  - networks and systems with a "very large" number of users.

While the first two categories of infrastructure are relatively easy to understand, what constitutes a "very large" number of users in the third category is unclear. The Draft Law offers no indication on whether this term could be interpreted expansively to cover, for example, networks within large companies with many employees in China.

Obligations of Operators of Critical Information Infrastructure

- When the operators of such infrastructure networks procure "network products and services," they must sign security and confidentiality agreements with their suppliers.
- If "network products and services" that the operators procure "may affect national security," the operators are required to ensure that such products or services have undergone a "security review" by national network administration authorities.
- Operators must store critical data, such as personal data collected in the course of their operations, within the territory of China; if transfers of data offshore are necessary for operational reasons, a "security assessment" must be conducted by national network administration authorities.

The Draft Law does not make clear what types of "network products and services" would be deemed to affect national security, and the procedures for the "security reviews" and "security assessments" referred to above are unclear. It is also unclear whether the personal data of foreign citizens collected in China would be covered by this obligation and whether this

provision applies only prospectively to new collections of personal information or also to data already collected.

As the Draft Law directs the State Council to formulate more measures for protecting the security of critical information infrastructure, some of these questions might be addressed in implementing regulations.

Network Operators and Data Privacy

The Draft Law also stipulates the obligations of network operators. "Network operators" are defined to include operators of basic telecommunication networks, internet information service providers, and key information system operators.

In addition to being responsible for the secured operation of networks, network operators also have the following obligations:

- protecting personal information, privacy, and trade secrets of users;
- notifying and obtaining the consent of users when collecting and using personal information;
- refraining from leaking, tampering, stealing, or reselling personal information;
- setting up systems to handle complaints, reports, and requests to amend erroneous personal information;
- policing the network to prevent the dissemination of false or unlawful information; and
- maintaining records of relevant activities.

When providing users with network access, domain name registration, fixed phone line installation, mobile phone services, or "network dissemination services," network operators also must require users to provide their real identities and must refuse to provide services to those that decline to provide such information.

Many of the obligations mentioned above are already imposed by other laws and regulations, such as the *Consumer Protection Law*, the *Decision on Strengthening Information Protection on Networks*, and the *Measures on Penalties for Infringing Upon the Rights and Interests of Consumers* (see Covington blog post on these regulations here and here). The Draft Law consolidates some of these obligations but leaves many questions unanswered.

For example, the Draft Law provides that "network products and services" that collect user information must notify users of such functions and obtain consents for collection. It does not clarify what types of notifications and consents would be deemed as sufficient, and whether each function would require a separate notice and consent, versus a blanket notification and consent process.

Also, the Draft Law does not stipulate how long a network provider must retain records of its activities and how network providers can determine whether the information provided to them is authentic.

Law Enforcement Access to Data; Penalties

The Draft Law provides that authorities can require network operators to provide necessary support and assistance to accommodate national security and criminal investigation needs without specifying any limit on such power.

The Draft Law also provides penalties for non-compliance with its provisions by entities or responsible individuals — including warnings, rectification orders, fines, or confiscation of illegal gains, and suspension of the business or revocation of the entity's business license. Like many Chinese laws, the Draft Law contains general, open-ended penalty provisions stipulating that any violation of the law that causes damage to others should result in civil liability, and any violation of the law that constitutes a crime should result in criminal liability. On a related note, recently proposed amendments to the *Criminal Law* include an article imposing criminal liability on network operators that fail to perform their "information and network security management" obligations.

* * *

If you have any questions concerning the material discussed in this client alert or wish to seek assistance with preparation and submission of comments, please contact the following Covington attorneys:

Tim Stratford	+86 10 5910 0508	tstratford@cov.com
Eric Carlson	+86 10 5910 0503	ecarlson@cov.com
Grace Chen	+86 10 5910 0517	gchen@cov.com
Yan Luo	+86 10 5910 0516	yluo@cov.com