Crowell

CLIENT ALERT

Summary of the PRC Cybersecurity Law

May 31, 2017

The People's Republic of China is preparing to implement the first comprehensive data protection framework in its history, the PRC Cybersecurity Law. The working draft of implementing regulations was most recently revised on May 19, 2017, and is scheduled to become effective on June 1, 2017, despite concerns from businesses around the world about the law's stringency and scope. The law will carry with it the authority to impose fines up to approximately $145,000.00 per violation in addition to various administrative and criminal penalties. While the law's impact will not be fully known until additional guidance is issued, the PRC Cybersecurity Law will likely impact companies of all sizes that do business in China, including those that do not have a physical presence there.

The PRC Cybersecurity Law will require the implementation of administrative and technical security safeguards, restrict the cross-border transfer of personal information and "important data" collected through operations in China, and mandate the protection of personal information.

The PRC Cybersecurity Law marks a major change in China's data protection environment. Given the law's broad scope, companies should carefully review their practices to determine how the new requirements – particularly those relating to data localization and the PRC's potential access to that data – impact their operations in China.

Network Operators, Critical Information Infrastructure Operators, and Providers of Network Products and Services

The PRC Cybersecurity Law generally imposes obligations on three types of entities: (1) network operators; (2) "critical information infrastructure" operators; and (3) providers of network products and services.

Network Operators

The PRC Cybersecurity Law imposes a range of cybersecurity obligations on "network operators," which are defined as owners and administrators of networks and network service providers. A "network" is defined as any system comprising computers or other information terminals and related equipment for collection, storage, transmission, exchange, and processing of information. On its face, the term network operator could broadly be interpreted to encompass any company that uses a network to do business in China despite not having a physical presence in China.

Generally, network operators must:

- Develop internal security management systems and procedures, appoint personnel responsible for network security, and implement network security protection responsibility.
- Adopt measures to prevent viruses, network attacks, network intrusions, and other threats to network security.
- Monitor and record network activity and security incidents, and store network logs for at least six months.

- Implement measures to classify, back up, and encrypt data.[11]

Network operators must also provide "technical support and assistance" to law enforcement authorities to safeguard national security and investigate crimes. The term "technical support" is not formally defined, and it remains to be seen whether this includes providing backdoor and decryption assistance for encrypted data. To the extent it does, it will permit government access to data stored [and potentially to data transferred (such as data in motion) in the PRC.

Critical Information Infrastructure Operators

Critical information infrastructure (CII) operators are defined as entities providing services that, if lost or destroyed, would endanger China's national security, economy, or public interest. The PRC Cybersecurity Law lists public communication and information services, energy, finance, transportation, water conservation, public services, and e-government as examples of CII.[22]

CII operators are subject to the same cybersecurity requirements applicable to network operators as outlined above. CII operators must also sign security and confidentiality agreements with their suppliers of network products and services, and evaluate cybersecurity and other potential risks at least once a year.

Providers of Network Products and Services

Providers of network products and services must comply with relevant national and industry standards and ensure the security of their products. Products determined to be "Critical Network Equipment and Network Security Products" are required to go through testing by accredited evaluation centers prior to being marketed in China.

Cross-Border Transfers

One of the most significant and controversial provisions of the PRC Cybersecurity Law restricts the cross-border transfer of personal information and important data collected or generated through operations in China (collectively, Local Data). Specifically, a network operator may transfer Local Data outside of China only if it has a business need to do so and passes a security assessment as outlined below.

On May 19, 2017, the Cyberspace Administration of China met to discuss revisions to implementing measures entitled *Measures for the Security Assessment of Outbound Transmission of Personal Information and Critical Data* (the Measures).[33] While the cross-border transfer requirements originally only applied to CII operators, the Measures extended the requirement to apply to *network operators*. As discussed above, the definition of network operator appears to be very broad and could include virtually any enterprise that does business in China.

The Scope of Local Data

Local Data subject to the cross-border transfer requirements consists of "personal information" and "important data." Notably, the definition of "personal information" is not explicitly limited to information pertaining to Chinese citizens. While prior drafts of the PRC Cybersecurity Law expressly defined personal information as belonging to Chinese citizens, both the final version of

the law and the Measures define personal information as information that can, taken alone or in combination with other information, identify a *natural person*.[44]

While the PRC Cybersecurity Law itself did not define "important data," the Measures clarify that the term refers to data that is very closely related to national security, economic development, and societal and public interests. The specific scope of important data will be based on relevant national standards and guidelines on important data identification.

Security Assessments for Cross-Border Transfers

If a network operator wishes to transfer Local Data outside of China, it must undergo a security assessment. Self-assessments generally suffice for this requirement and must consider, among other factors:

- The legality, legitimacy, and necessity of the cross-border transfer.
- The amount, scope, type, and sensitivity of the data.
- If the transfer involves personal information, whether data subjects have consented to the transfer.
- The data recipient's security capability, measures, and environment.
- The risks associated with the data being leaked, damaged, tampered with, or misused after the data transfer or subsequent re-transfer.
- The risks to national security, societal and public interests, and the individual lawful rights and interests after the cross-border transfer.

Transfers of a large amount of data and transfers involving highly sensitive information (*e.g.*, information related to nuclear facilities or national defense) require a government-administered security assessment. Generally, these will be conducted by the agency with regulatory or supervisory authority over the transferor's industry sector.

Prohibited Cross-Border Transfers

Cross-border transfers of Local Data are prohibited in the following circumstances:

- The transfer does not comply with state laws, administrative regulations, or departmental rules.
- Data subjects do not consent to a transfer involving personal information.
- The transfer poses risks to China's national security or public interests.
- The transfer could endanger China's security of national politics, territory, military, economy, culture, society, technology, information, ecological environment, resources, and nuclear facilities.
- Other circumstances where the Chinese government determines that the data involved in the transfer is prohibited from being transferred offshore.

Consent

If a network operator wishes to conduct a cross-border transfer that includes personal information, it must explain to the data subjects the cross-border transfer's purpose, scope, type, and country or region in which the recipient is located. The network

operator must also obtain data subjects' consent except in emergencies (*i.e.*, when the life or property of a data subject is in danger). The Measures provide that consent can be inferred in certain scenarios, including where the data subject makes international phone calls related to the network operator, sends emails or instant messages to individuals or organizations overseas, and conducts cross-border e-commerce transactions, as well as other activities initiated by data subjects.

Data Localization Requirement

Article 37 of the PRC Cybersecurity Law requires that CII operators store Local Data within China. While the April 11 draft of the Measures expressly reiterated this data localization requirement and expanded it to network operators, the May 19 revision of the Measures removed this reference to the data localization requirement. Instead, the current Measures focus on security assessments in connection with cross-border transfers of data. It is not clear whether future implementing regulations will mandate data localization. Again, if there is a localization requirement there is no guarantee that such data will be protected from government access.

Protection of Personal Information

In addition to the cybersecurity and cross-border transfer requirements discussed above, the PRC Cybersecurity Law provides for various protections of personal information. Network operators may not disclose, tamper with, or destroy personal information that they have gathered. Individuals have the right to request that network operators delete unlawfully collected personal information and amend any incorrect personal information. Network operators must also obtain informed consent prior to providing personal information to others. These requirements do not apply to information that has been irreversibly de-identified. The PRC Cybersecurity Law also imposes breach notification obligations in the event of a breach of personal information.

Penalties

Both organizations and individuals face penalties from various regulatory departments for violations of the PRC Cybersecurity Law, including warnings, suspensions, license revocations, and fines of up to RMB 1,000,000 (approximately $145,000), which have prescribed ranges based on the nature of the violation. Violators may also face criminal penalties. Foreign businesses that attack any CII in China are subject to specific penalties such as sanctions and freezing of assets.

Effective Date

The PRC Cybersecurity Law is set to take effect on June 1, 2017. The May 19 revision of the Measures includes a grace period for the cross-border transfer requirements. If, as expected, the current version of the Measures is implemented, network operators will have until December 31, 2018 to comply with the cross-border transfer provisions.

Implications

Businesses operating in China should evaluate how the PRC Cybersecurity Law might impact their operations and amend their policies and procedures as necessary. Companies should pay close attention to their data transfer practices to meet the new restrictions on cross-border transfers. Companies should also understand the implications of data localization requirements and

the ability of the government to access private and proprietary data stored and transferred in China. China is still in the process of developing implementing regulations, so companies should closely monitor developments and provide input to regulators as appropriate.

---

[1] In April 2017, China's State Cryptography Administration released for public comment a draft Encryption Law addressing encryption in more detail.

[2] Ultimately, the State Council will define the scope of CII.

[3] A draft of the Measures was originally issued for public comment on April 11, 2017. The Measures have an intended effective date of June 1, 2017, and the May 19 revision is likely to be the final form.

[4] The Measures extend this definition to include information that can, independently or in combination with other information, *reflect the activity of a natural person*. Examples provided in the Measures include a natural person's name, date of birth, identity certificate numbers, correspondence and communication contact information, personal biological identification information, address, account number and password, status of property, location, and activity information.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Jeffrey L. Poston
Partner – Washington, D.C.
Phone: +1.202.624.2775
Email: jposton@crowell.com

Paul M. Rosen
Partner – Los Angeles, Washington, D.C.
Phone: +1.213.443.5577, +1.202.624.2500
Email: prosen@crowell.com

Evan D. Wolff
Partner – Washington, D.C.
Phone: +1.202.624.2615
Email: ewolff@crowell.com

Brandon C. Ge
Counsel – Washington, D.C.
Phone: +1.202.624.2531

Email: bge@crowell.com