THE
NATIONAL LAW REVIEW

Part 2 - Three Weeks On: What We Know about Enforcement of China's Cybersecurity Law

Thursday, June 22, 2017

We have previously clarified which parts of China's latest Cybersecurity Law (the "Law") are currently ready to be enforced and which parts are awaiting clarification in the form of implementing regulations or standards. In this post, we will discuss latest landscape of implementing regulations and national standards that supplement the Law.

COVINGTON

Article ByTheodore J. Karch
Yan Luo Covington & Burling LLP
Inside Privacy

Communications, Media & Internet
Global
China

Implementing Regulations

The following implementing regulations are legally binding. They provide specifics on how provisions of the Law will be applied in practice.

Finalized: Cybersecurity Review of Network Products and Services

The *Measures on the Security Review of Network Products and Services (Trial)* (the "Security Review Measures") offer guidance on how cybersecurity reviews of operators of Critical Information Infrastructure ("CII") will be conducted. Specifically, the Security Review Measures elaborate on the review's scope, substantive criteria, responsible agencies, and process.

The Security Review Measures provide that procurement of "important network products and services" related to network and information systems that implicate China's national security will be subject to the cybersecurity review. Specifically, network products and services supplied to the following entities may be subject to the review process if the procurement will affect China's national security:

- Entities in key sectors such as telecommunication and information services, energy, transportation, water conservation, finance, utilities and e-government; and
- Other operators of CII.

Further, the Security Review Measures establish a Cybersecurity Review Commission, which will be responsible for shaping policies regarding the review and addressing key cybersecurity issues. Under the Commission, a Cybersecurity Review Office will handle the actual cybersecurity reviews with assistance from third party evaluation centers, which will produce technical evaluation reports, and an expert panel, which will provide recommendations based on their assessment of security risks on the basis of the third party reports.

According to a news report, the Head Engineer of the China Information Technology Security Certification Center ("CNITSEC") (one of the third-party evaluation centers designated to conduct the cybersecurity review on the Government's behalf) explained that the security review may be triggered in one of three ways: (1) the relevant sector regulators deem the security review on certain product or service to be necessary; (2) a nationwide industry association suggests conducting the security review; or (3) the market's response (including the public and users) demands the security review.

In conducting the review, agencies will focus on whether the products and services and the related supply chain are "secure and controllable." Risk criteria that agencies will assess include:

- Security risks inherent in the products or services themselves, as well as the risk that the products or services will be unlawfully controlled, interfered with, or interrupted;

- Supply chain security risks associated with all stages of the life cycle of products and key components (i.e., manufacturing, testing, delivery, and technical support);
- The risks associated with products or services being used by their suppliers to illegally collect, store, process, or use users' data;
- The risks that product or service providers could negatively impact cybersecurity or consumers' rights and interests by leveraging customers' reliance on the products or services. (The final version removes the reference to "unfair competitive practices"); and
- Other risks that may compromise national security.

Yet to be Finalized: Cross-Border Data Transfers

The *Measures on Security Assessment of Cross-border Data Transfer of Personal Information and Important Data* (the draft "Transfer Measures") have not yet been finalized, but have gone through a public comment period. The draft Transfer Measures specify when a security assessment must be conducted for a network operator's cross-border data transfers and what substantive criteria will be used .

The draft Transfer Measures extend certain cross-border transfer obligations to "network operators," a much broader term than "CII operators." "Network operator" is defined to include "owners and managers of networks, as well as network service providers." The draft Transfer Measures provide that when network operators transfer abroad personal information and important data collected or generated in the course of operations within China, a security assessment should be conducted.

Regulators will review these assessments under certain circumstances. For example, regulators may initiate their review when personal information of over 500,000 Chinese citizens is transferred offshore or when the regulator views the transfers as "potentially affecting China's national security and public interests."

In the latest version of the Measures, the Cyberspace Administration of China ("CAC") has given network operators a grace period of 18 months to comply with the requirements for cross-border data transfers. Therefore, all network operators' cross-border data transfers must be in compliance with the Transfer Measures starting from December 31, 2018. The CAC also explained that China's National Information Security Standardization Technical Committee ("NISSTC") will release supplementing national standards to provide more guidance to companies on how to conduct a security assessment for their cross border data flows.

Yet to be Finalized: Sectorial Regulations

In addition to regulations of general applicability, China has released a series of cybersecurity rules that cover entities in certain sectors. Some of these regulations have effects that go beyond those covered entities.

For example, in February 2017, the Civil Aviation Administration of China ("CAAC") proposed *Rules for the Administration of Civil Aviation Cyber Information Security (Draft for Comment)* ("CAAC Rules"). Although the CAAC Rules govern covered entities (*e.g.*, domestic aviation entities under CAAC's direct supervision), they also apply more broadly to entities that access networks and systems of those covered entities.

In May 2017, the China Securities Regulatory Commission ("CSRC") proposed *Measures for Securities and Fund Institutions on Information Technology Management (Draft for Comment)* ("CSRC Measures"). Similar to the CAAC Rules, while the CSRC Measures' substantive obligations are largely intended for covered entities within the financial industry, some provisions also apply more broadly to "information technology service providers" serving the covered entities.

These developments make clear that providers of network equipment and companies that interface with covered entities in these and other sectors cannot ignore sectoral regulations in China. Even though a network equipment provider may not be the primary covered entity, sectoral regulations such as these may impact providers of technology and other services nonetheless.

National Standards

China's NISSTC, a standard-setting committee jointly supervised by the Standardization Administration of China ("SAC") and the CAC, has released draft national standards that supplement the Cybersecurity Law. While these standards are not legally binding, they will likely serve as reference points for the CAC and other regulators when enforcing the Law.

Yet to be Finalized: Protection of Personal Information

The *Information Security Technology – Personal Information Security Specification* (the draft "Personal Information Standard") will likely be used to judge corporate data protection practices in China. While the public comment period has ended, the draft Personal Information Standard has not yet been finalized.

As far as personal information is concerned, the draft Personal Information Standard is more comprehensive in scope than the Cybersecurity Law. It is comparable to modern data protection rules and standards in other countries, such as the EU's General Data Protection Regulation ("GDPR"), EU-U.S. Privacy Shield, as well as relevant ISO/IEC, NIST, and CWA standards.

The draft Personal Information Standard's definition of "personal information" mostly parallels the term's definition in the Law, namely "various types of electronic or otherwise recorded information that can be used separately or in combination with other information to identify a natural person." But the draft Personal Information Standard explicitly includes a natural person's biological identification data, geographical location data, and behavior data within the scope.

Further, the draft Personal Information Standard treats differently "sensitive" personal information, defined as "personal information that may lead to bodily harm, property damage, reputational harm, personal health, or discriminatory treatment of a person if such information is disclosed, leaked or abused." Examples of sensitive personal information include a person's National Identification Number, bank information, medical records, and biological identification information.

The draft Personal Information Standard also sets out eight substantive principles of personal information protection, which are meant to parallel international norms. For example, it contemplates that the primary legal basis for processing personal data in China is consent (it does not provide for other legal bases such as, as in the EU, "legitimate interests"). As in some other jurisdictions, it contemplates that data subjects have a right to delete their personal information. It also expects that organizations will adhere to principles of data minimization.

Yet to be Finalized: Security Assessment of Cross-Border Data Transfers

On May 27, 2017, the NISSTC released *Information Security Technology – Guidelines for Data Cross-Border Transfer Security Assessment (Draft Version)* (the draft "Transfer Standard") for public comments. The comment period is open until June 27, 2017. The draft Transfer Standard supplements the draft Transfer Measures discussed above.

The draft Transfer Standard, elaborating on the substantive criteria mentioned in the draft Transfer Measures, details the risk factors regulators are likely to analyze when reviewing or conducting security assessments of companies' cross-border data transfers flowing out of China.

As a threshold matter, the regulator determines whether the transfers at issue are "lawful and legitimate." Transfers for a genuine business purpose should generally meet this threshold. If this bar is met, regulators are instructed to evaluate security risks associated with transfers focusing on four elements: data being transferred, data controllers' data protection program, data recipients' level of protection, and the "political and legal environment" of the country or region in which the data recipient is located.

Based on these risk factors, regulators can determine the overall risk level of the data transfers. If these assessments reveal major risks, regulators may require a company to step up its data protection efforts, or such transfers may be blocked entirely. Once a company conducts a self-security assessment, the record of such an assessment must be retained for at least five years.

Part 1 - Three Weeks On: What We Know about Enforcement of China's Cybersecurity Law

Final Part 3 - Three Weeks On: What We Know about The Enforcement of China's Cybersecurity Law

Source URL: https://www.natlawreview.com/article/part-2-three-weeks-what-we-know-about-enforcement-china-s-cybersecurity-law