ALSTON & BIRD

WWW.ALSTON.COM

CYBER ALERT ■

JUNE 26, 2017

Navigating the Uncertain Chinese Cybersecurity Law: What We Know and How to Steer Accordingly

By Kim Peretti , Justin Hemmings, and Emily Poole

As of June 1, 2017, China's new Cybersecurity Law came into force.[1] The Cybersecurity Law has broad implications for any company that does business in the country as the Chinese government has asserted even greater control over all data collected or generated in its territory. However, many questions remain unanswered despite several draft measures interpreting the Cybersecurity Law, causing great uncertainty about how to comply with the Cybersecurity Law and how its provisions will actually be enforced. Here are some key things to know.

Background

The enactment of China's new Cybersecurity Law, which was passed by the Chinese parliament in November 2016, marks the end of a two-year effort to replace the country's sectoral approach to data regulation with a comprehensive cybersecurity law. As is typical in China, the law passed by parliament encompasses a broad set of principles, and the scope of the law will be clarified by a series of implementation regulations (Measures) and guidelines to be issued by the relevant authorities.

A first set of draft implementing rules and regulations was released earlier this year, including the *Measures for the Security Review of Network Products and Services* (February 2017) and the *Measures on Security Assessment of Cross-border Transfer of Personal Information and Important Data* (April 2017). China's Internet regulator office, the Cyber Administration of China (CAC), has advised that all implementation regulations will be published within one year of the Cybersecurity Law's effective date. Additional regulations will cover critical information infrastructure protection, the protection of personal information, and equipment and products that have been certified as meeting national security standards.

1 Click here for an unofficial English translation of the law.

Who Is Covered?

The Cybersecurity Law contains obligations for "network operators" and "critical information infrastructure operators" (CIIOs), but these terms remain largely undefined. Article 31 gives some examples of what might be included under critical infrastructure, emphasizing public communications and information services, energy, finance, transportation, water conservation, public services, and e-governance. Statements from the CAC, which emphasize the government's risk-based approach, also suggest that any entity may qualify as a CIIO as long as a breach or loss of functionality could pose a great risk to China's national security or welfare.

"Network operators" are defined as owners and administrators of networks and network service providers in the PRC, but the CAC's guidance from May 31, 2017, suggests that the term could be interpreted broadly to include any entity that provides services and conducts business activities through a network. Indeed, a business transferring files from just one computer to another could potentially qualify as a network operator under this definition.

What Is Required?

The Cybersecurity Law imposes a wide-ranging variety of obligations, but compliance is complicated by the slow arrival of critical guidance and regulations, and the Cybersecurity Law's ambitious scope makes it unclear how extensively the Cybersecurity Law will be enforced. While some provisions will certainly be clarified in the coming months, especially as China has faced and may continue to face significant opposition from the international business community, the Cybersecurity Law's severe penalties for noncompliance make a "wait and see" approach exceedingly risky. Companies should take steps to comply as soon as possible, while understanding that Chinese political and economic interests will make strict enforcement more likely in some areas than in others.

Data localization and data transfer

In one of the Cybersecurity Law's most controversial provisions, any "personal information" or "important data" collected or generated by CIIOs must be stored domestically. Despite the initial confusion created by the recent draft *Measures on Security Assessment of Cross-border Transfer of Personal Information and Important Data*, which implied that the data localization requirement would apply to *all* network operators, a recent Q&A issued by the CAC assured that only CIIOs are implicated. That said, while the term "personal information" is defined as information that, taken alone or together with other information, is sufficient to identify a natural person's identity, including names, birth dates, identification numbers, and biometric information, the amorphous term "important data" has not been adequately defined under either the Cybersecurity Law or any draft Measures. Indeed, the use of the term "important data" is generating much confusion, given that under the recent Measures governing cross-border transfers, the term was sweepingly defined as any information that could "influence or harm the government, state, military, economy, culture, society, technology … and other national security matters." Absent significant clarification and/or narrowing by the Chinese government, provisions that govern the use of important data will have incredibly broad implications for companies operating as CIIOs in China since almost any piece of information could conceivably fit into this definition.

In addition to the data localization requirement, the Cybersecurity Law also sets tight restrictions on when data can be transferred out of the country, allowing cross-border transfers only when there is a genuine operational necessity and the entity passes a security assessment. CIIOs must also obtain consent to move personal information across borders, unless consent is implied because the subject is the one sending the information (i.e., by sending an email or engaging in international e-commerce).

While compliance with the data localization requirement is officially required as of June 1, 2017, the deadline for compliance with the rules governing cross-border transfers has been extended to December 31, 2018. Any company that is likely to be labeled as a CIIO should therefore begin to assess its data transfer practices, first considering ways to store data locally, then deciding which data is "necessary" to transfer, and drafting policies to obtain subject consent before any international transfers of personal data.

Cybersecurity measures and security incident notification

The Cybersecurity Law imposes a series of technical and organizational cybersecurity measures on all network operators. Beyond implementing technological measures to prevent breaches, operators will need to develop a system for classifying data, install adequate backups, and consider encrypting data at rest, among other measures. The Cybersecurity Law also requires operators to have an incident response plan and report all network security incidents, including any instance where destruction or loss of personal data *might* occur, as well as any security flaws and vulnerabilities in their products and services, to "relevant competent departments" in accordance with "relevant provisions"—but these terms are not yet defined.

Considering the enormous amount of information that would need to be reported under this provision (security incidents happen, and security vulnerabilities are discovered, on a continuous basis, and the provision applies to any entity using more than a single machine), full enforcement seems nearly impossible. Until the relevant regulating authorities are specified and more guidance is given on how to comply with the state's "tiered system of network security protections," companies should take steps to implement as many of the outlined precautions as possible, taking into account the amount and types of data involved.

Cybersecurity review regime

Effective June 1, 2017, under the *Measures for the Security Review of Network Products and Services*, all network products and services used in critical infrastructure will be subject to a national security review by the CAC to ensure that national standards are being followed and that all potential risks to national security are minimized. There are still many open questions about how exactly these reviews will be implemented. The stated focus of the reviews will be on the risk of a product being illegally controlled or interfered with, as well as the illegal collection of a user's information. The catch-all provision which covers "other risks that could endanger national security and public interests," however, means that focus could be expanded in the future. CIIOs should remain alert for further guidance on what these reviews will entail and how they will be performed.

Regulation of personally identifiable information

The provisions pertaining to the collection and processing of personal data are similar to those contained in the EU's General Data Protection Regulation (GDPR). Network operators must obtain consent before collecting or processing personal data and cannot use personal data for any other purpose than that for which it was collected. Entities also may only collect, use, or store personal information that is necessary for business purposes. If an individual discovers improper collection or use of their data, they have the right to demand deletion or correction of their data if the collected information contains errors.

User identification and transmission of illegal information

Two additional provisions serve to provide the Chinese government with greater control over the use of the country's networks. First, under Article 24, network operators managing network access (mobile or otherwise) and domain registration services or providing information publication services must require users to provide real identity information upon agreeing to any provision of services.

Adding to this "network identity credibility strategy," Article 46 establishes that all individuals and organizations shall be held responsible for the use of their websites and bear responsibility for stopping the transmission of illegal information. The CAC has clarified that this does not pertain to the content of personal communications but only to information that is publicly disseminated. Companies operating in China should therefore prepare to remain vigilant over their websites and block or take down any information relating to the perpetration of fraud, the creation or sale of prohibited items, or other unlawful activities.

Complying with the Chinese Cybersecurity Law: Practical Steps

The Chinese Cybersecurity Law is a game-changer in its breadth and scope of regulating cybersecurity practices of entities doing business in China, and the details and specifics of how it will be interpreted and enforced remain unknown. Here are four tips for navigating this uncertain transition period:

Follow advances in implementing regulations

While the Cybersecurity Law lays a framework, other Chinese political organs retain the authority to promulgate implementing rules and regulations. There has already been movement from the China Securities Regulatory Commission and the CAC's drafts of implementation measures for security reviews and guidelines for cross-border data transfers, and other implementing rules and regulations could follow. Consequently, it is important to make sure your organization receives reliable and regular updates when new drafts are published or new regulations go into effect.

Submit comments on government drafts when appropriate

The CAC's draft guidelines and implementations were both published alongside an open period for parties to submit comments. Taking advantage of this period can be helpful in requesting vital clarification and lobbying the relevant ministries for important changes to published drafts. Working with counsel familiar with the Chinese government can help maximize the effectiveness of comments and help pick and choose where best to direct those efforts.

Monitor the Ministry of Public Security in particular

One issue that remains unknown is whether the Chinese Ministry of Public Security will assert authority under the new Cybersecurity Law. The Ministry of Public Security is roughly equivalent to a domestic police force and consequently has more manpower, resources, and bandwidth to conduct investigations and enforcement measures. Given its greater investigatory resources, and its authority to detain subjects for questioning pursuant to an investigation, the Ministry of Public Security has the potential to be a significant enforcer of the new Cybersecurity Law. Understanding how the ministry operates and being prepared to respond if it asserts authority can help minimize potential enforcement risks.

Coordinate international legal compliance efforts

Many companies are currently working through updating their global cybersecurity compliance infrastructure to comply with various new international regulations. As you are addressing compliance with the EU's GDPR, or Japan's and Australia's new data privacy laws, those compliance efforts can help inform your compliance with the new Chinese legislation. For example, accurate and up-to-date data mapping is crucial to demonstrating compliance with each of these legal frameworks. Knowing what data you have in what locations is instrumental for demonstrating compliance with restrictions on cross-border data transfers, for one example. Coordinating these compliance efforts can help save significant time and resources.

As these new regulations and oversight begin, organizations operating in China have an opportunity to ensure compliance and get involved in the process going forward to smooth out any future uncertainties.

If you have any questions or would like additional information, please contact Kimberly Peretti, Jim Harvey, Uni Li, or Justin Hemmings.

Cybersecurity Preparedness & Response Team Co-Chairs

Kimberly Kiefer Peretti | 202.239.3720 | kimberly.peretti@alston.com
Jim Harvey | 404.881.7328 | jim.harvey@alston.com

Follow us: @AlstonPrivacy | www.AlstonPrivacy.com

www.alstonsecurity.com

ALSTON & BIRD

WWW.ALSTON.COM

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86 10 8592 7500
BRUSSELS: Level 20 Bastion Tower ■ Place du Champ de Mars ■ B-1050 Brussels, BE ■ +32 2 550 3700 ■ Fax: +32 2 550 3719
CHARLOTTE: Bank of America Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: 2828 North Harwood Street ■ 18th Floor ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RESEARCH TRIANGLE: 4721 Emperor Blvd. ■ Suite 400 ■ Durham, North Carolina, USA, 27703-85802 ■ 919.862.2200 ■ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ 415.243.1000 ■ Fax: 415.243.1001
SILICON VALLEY: 1950 University Avenue ■ 5th Floor ■ East Palo Alto, CA 94303-2282 ■ 650-838-2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333