Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

What We Don't Know About China's New Cybersecurity Law

By **Grace Chen**

Grace Chen

Law360, New York (June 8, 2017, 12:19 PM EDT) -- China's Cybersecurity Law, which took effect on June 1, 2017, has been the focus of attention by companies, organizations and individuals that may be affected by this law. Since its promulgation on Nov. 7, 2016, the various stakeholders have been anxiously awaiting further guidance from the Cyberspace Administration of China ("CAC") with respect to its implementation, particularly in respect of three areas, namely (1) network products and services, (2) offshore data transfers and (3) critical information infrastructures.

The Cybersecurity Law left a number of issues open for future implementation. Although the law is already in effect, a fair number of issues remain unresolved, leaving companies and individuals seeking to comply with the law in limbo. Set forth below is a discussion of the outstanding issues and the progress to date.

Network Products and Services

Under the Cybersecurity Law, critical network equipment and cybersecurity specialty products must not only comply with mandatory standards, but must also be subject to security certification and testing. In response to this requirement, the CAC issued the "Network Products and Services Security Review Measures (Trial Implementation)" on May 2, 2017, which took effect on June 1, 2017. These trial product measures are intended to apply to key network products and services to be used in networks and information systems that are relevant to national security. These products and services, which will likely be used by critical information infrastructure operators such as those in finance, telecommunications, energy, transportation, public communications and information services, water utilities, public services, e-government, etc., must undergo security review before they are brought to market.

The security reviews will focus upon assessing the security and controllability of, as well as the transparency of security mechanisms and technology in such products and services, looking at specific risks relating to these products and services such (1) unlawful control, interference or interruption of the network product or service; (2) risks associated with the supply chain, i.e., during manufacturing, testing, delivery, and technical support; and (3) bad behavior on the part of the vendors, for example, exploiting vulnerability of users relying on the product or service to inflict cyber harm or otherwise cause injury to consumer rights and interests, for example, by collecting and using user personal data

without consent, taking control of user systems without authorization or discontinuing reasonable technical support to force users to purchase new equipment, etc.

Security review and testing of such network products and services, which will apply to all qualified products and services regardless of national origin, shall be conducted by third-party organizations designated by the CAC. Such organizations may include entities such as the China Information Security Certification Center, which specializes in handling information security certification of products to ensure compliance with mandatory state standards and information security laws and regulations, and the China Information Technology Security Evaluation Center, which specializes in testing and risk assessment of information technology products. Although the CAC has not yet designated any specific third-party organizations for this purpose to date, but it has stated its intention to push for mutual recognition of security certification and security testing, in order to avoid any duplication of such procedures.

The CAC is also working with relevant government authorities to publish a catalogue of critical network equipment and cybersecurity specialty products that must comply with mandatory national standards and be certified or tested by qualified organizations.

Offshore Transfer of Personal Information and Important Data

The Cybersecurity Law provides that personal information and important data collected or generated by critical information infrastructure operators in the course of their operations must be stored within China, and any exports of such information will be subject to security review in accordance with rules to be formulated by the CAC in conjunction with other relevant government authorities. In response to this provision, the CAC circulated a draft of the "Personal Information and Important Data Export Security Review Measures" on April 11, 2017 for public comment until May 11, 2017.

This public comment period was followed by a meeting on May 19, 2017, when the CAC invited foreign chambers of commerce, company representatives and various other stakeholders to discuss and comment on a revised draft of the data export measures. The revised draft, which had purportedly incorporated many of the comments provided by various stakeholders during the public comment period, also added location and trajectory data among the types of personal information that would require individual consent and but subject to protection under these rules, in line with a recently issued judicial interpretation on data privacy infringement which also identified trajectory data as a type of personal information subject to data privacy protection.

An issue of serious concern raised in the earlier comments and during the meeting was the fact that both drafts of the data export measures suggested that the requirement for offshore data transfers to be subject to security reviews would apply not only to critical information infrastructure operators, but also to network operators that fulfill specific criteria that are set out in the data export measures, and this was informally confirmed by the CAC during the meeting. However, based on an interview transcript published by the CAC on May 31, 2017, it appeared that the CAC had reconsidered their position and have now reverted back to the initial stance set out in the Cybersecurity Law, i.e., these security review requirements would be applicable only to cross-border data transfers by critical information infrastructure operators.

Another issue of concern raised by the stakeholders during the meeting was whether the data export measures would essentially function as a trade barrier for foreign investment in China by blocking offshore transfers of data. The CAC expressed disagreement with this viewpoint during the meeting, and

the CAC clearly reiterated this position in the CAC interview transcript, stating that the restrictions placed on offshore data transfers are not intended to stifle international commerce or inhibit the flow of data across borders, but to ensure protection of personal data privacy and national cybersecurity.

The data export measures set out the criteria for the security review, and specifies the types of data that should be subject to such security review and also the types that may not be transferred abroad as follows:

1. Security review of data to be exported entails an assessment of whether the export of such data is lawful, proper and necessary, and to the extent such transfers involve personal information, they will review and assess the volume, scope and degree of sensitivity of the personal information to be exported, as well as whether the relevant consents have been obtained. To the extent such exports involve important data, they will review and assess the volume, scope and type of data to be exported.

2. Data that should be subject to security reviews include: (1) personal information for half a million persons or more, (2) data generated in the areas of nuclear facilities, biochemistry, national defense, human health, etc.; (3) data generated in relation to large-scale construction activities, marine environments and sensitive geographic information; (4) security flaws and specific security protection measures in critical information infrastructures and (5) other data that might affect national security or the public interest.

3. Data that fall within the following categories are prohibited from export: (1) data that is not in compliance with state laws, administrative regulations, department rules, etc.; (2) personal information that have not received consent for such export; (3) personal information that if exported may injure the public or state interests; (4) data that if exported may cause injury to security of national politics, the homeland, military, economy, culture, society, technology, information, ecology, resources, nuclear facilities, etc.; (5) data that may not be exported according to laws or rules set by the CAC, the Ministry of Public Safety, or other security departments.

The National Information Security Standardization Technical Committee issued a draft of the "Information Security Technology — Guidelines for Data Cross-Border Transfer Security Assessment" for public comment on May 27, 2017. These recommended standards are intended to provide guidance for network operators seeking to conduct security assessments of cross-border transfers of their data and may serve as a reference for the CAC and other government authorities. These standards are accompanied by Appendix A, which is a standard catalogue setting out the types of important data categorized by industry type and Appendix B, which provides a risk assessment scheme that provides certain benchmarking metrics for assessing the impact of cross border transfers of personal information and important data on individual, national and public interests.

Notwithstanding the above, the CAC has expressly indicated that a safe harbor will be provided for activities that clearly do not endanger national security or the public interest, for example, certain proactive behaviors on the part of individuals such as making international calls, sending international emails, shopping on offshore Internet sites, etc. would be construed as implied consent with respect to the offshore data transfers necessary to effect such transactions.

Based on our reading of the two drafts of the data export measures and the CAC interview transcript, the legislative intention behind the issue of cross-border data transfer from a cybersecurity perspective appears to be protection of national security and individual privacy. The data export measures primarily focuses on two aspects, the first on individual consent, which must be obtained for any and all personal

information that needs to be transferred (except in emergency situations where the lives or assets of citizens are at stake), and the second on data that is important from a national security standpoint and not from a company or individual's perspective; such data must undergo advance security review by the relevant government authorities.

The data export measures, which are expected to be officially promulgated very shortly, will likely take retroactive effect from June 1, 2017. However, network operators are expected to enjoy a grace period until Dec. 31, 2018, to achieve full compliance.

Critical Information Infrastructure Operators

China's leader Xi Jinping recognized the importance of protecting China's critical information infrastructures, citing their importance as a nerve center of the nation's economy and society and potential vulnerability to cyberattacks and calling for greater efforts to be made towards strengthening cybersecurity protection of the systems to protect against data tampering, information leakage, loss of control and other network attacks.

The Cybersecurity Law defines critical information infrastructures (CII) broadly, as "infrastructures that, in the event of damage, loss of function, or data leak, might seriously endanger national security, national welfare or the livelihoods of the people, or the public interest." The Cybersecurity Law provides examples of CII operators, including network operators in the areas of public communication and information services, energy, transportation, water utilities, finance, public services, e-government, but leaves the issue open, indicating that the State Council will provide guidance with respect to the specific scope of the definition of CII, along with the corresponding security protection measures.

Although the CAC interview transcript envisages the issuance of the "Critical Information Infrastructure Protection Measures," no draft has been issued for public comment to date. As CII operators are subject to additional cybersecurity obligations in comparison with other network operators that are not deemed as CII operators, many of the stakeholders are quite anxious to review and learn about the CII Measures so that they may understand how CII will be defined and whether they will fall within that definition. In order to understand how CII will be defined and which type of business operations will fall under that definition and become subject to the more stringent requirements applicable to them, to date, many have been relying on the guidelines used by local authorities to conduct cybersecurity inspections of CIIs of local government- and party-affiliated organs, as well as enterprises and institutions registered in that locality, pursuant to a CAC notice issued in July 2016. The CAC notice called for its local counterparts to launch efforts to look into critical operations that affect the people's livelihood, and to overhaul the information systems and industrial control systems that may impact such operations as needed. The stated objectives of this project are to accurately grasp the overall cybersecurity situation of CIIs nationwide and scientifically assess the potential cybersecurity risks, in order to use these inspections to promote management, prevention, modifications and construction of CII, and at the same time, providing basic data and references for establishing CII security assurance systems.

According to the guidelines, CIIs are generally divided into three categories, websites (such as government websites, enterprises or institution websites, news websites, etc.), platforms (such as online service platforms such as those for instant communications, online shopping, online payments, search engines, emails, forums, maps, audio-visual programs, etc.) or production operations (such as office and operational systems, industrial control systems, large-scale data centers, cloud computing platforms, television broadcast systems, etc.). The guidelines provide a list of criteria for each of these three categories, along with a list of industries and the critical operations associated with each industry.

Companies that fall within the listed industries should look into the critical operations for that industry, and identify the information infrastructures used to support such critical operations. To be deemed as CIIs, these information infrastructures would need to fulfill specific criteria that would qualify as a CII, for example, the characteristics of the infrastructure, the number of users and the potential for damage in the event of a cybersecurity incident (as determined by the number of jobs and lives affected, disclosure of personal or sensitive information or other important data up to a certain level or whether there would be serious damage to social and economic order or harm to national security), etc.

The aforementioned guidelines, which have been published on various local government websites, were purportedly taken from operational guidelines for cybersecurity inspections prepared by the CAC with reference to the recommended standard "Information Security Technology — Government Department Information Security Management Basic Requirements" (GB/T 29245-2012). But since these guidelines have not been specifically endorsed for use in relation to the Cybersecurity Law, they can only serve as a point of reference as to how the CAC and other relevant government authorities may structure the CII measures.

What's Next

According to the Legislative Law, the CAC and other relevant government authorities have one year after the official promulgation of the Cybersecurity Law, or June 1, 2018, to put in place the auxiliary rules and regulations necessary for full implementation of this law. The CAC is working with relevant government authorities (which are likely to include the Ministry of Industry and Information Technology and Ministry of Public Security to draft the implementing rules for the Cybersecurity Law, as well as working with the National Information Security Standardization Technical Committee to formulate relevant standards.

In light of this one-year statutory extension for the implementing rules to be put in place, and the possibility that these rules may additionally provide grace periods to achieve full compliance, we anticipate that China's cybersecurity regime will continue to be in flux for at least the next 18 months, if not longer.

Grace Chen is of counsel with Covington & Burling LLP in Beijing.