Client Alert: China's New Cybersecurity Law

Related Services

Data Strategy, Privacy and Security

CLIENT ALERT | 3.29.2017

The People's Republic of China has passed a new cybersecurity law that is set to take effect on June 1, 2017. While the law's stated purpose is to fight hackers and is primarily aimed at internet companies, it has potentially far-reaching consequences for companies doing business in China.

Who is impacted?

The law primarily regulates business classified as "network operators" and imposes data security requirements on them. "Network operators" are defined as owners or providers of any "network," which is any system of "computers or other information terminals" that gather, store, transmit and process information. While this definition likely does not impact many businesses, the law also introduces the concept of "critical information infrastructure" (CII), and imposes additional and enhanced data security requirements on businesses that operate CII as determined by China. While not explicitly defined, CII includes any businesses operating in the communications, finance, water, power or traffic sectors. It also includes any other businesses using infrastructure that "might seriously endanger national security, national welfare and the people's livelihood, or the public interest" if such infrastructure malfunctions, is damaged or causes data leak.

Critics argue that the loosely defined concept of CII is far too broad and will capture almost any modern business dealing with China, thereby exposing them to expensive and time consuming regulation.

How are network operators impacted?

The law imposes specific cybersecurity obligations on network operators, as well as on the businesses that provide network products and services, including:

- network operators must implement certain stringent data security procedures, including the requirement to maintain network logs for at least six months, and must implement those procedures according to China's "tiered system of network security protections;"

- network operators may only utilize a limited group of pre-approved equipment and services in China, such as those that "comply with the relevant national and mandatory requirements" and that which is deemed "critical network equipment and specialized network security products;"
- network operators are required to provide technical support and assistance to state security authorities and national security authorities for security and criminal investigations; and
- network operators are also required to maintain the confidentially of user information that they collect and are subject to other identity verification protocols.

How is critical information infrastructure impacted?

In addition to the above, businesses that operate CII are subject to even heavier data security regulation, including the following:

- CII operators are subject to data localization requirements, whereby CII operators with certain important information "gathered or produced by [it] during operations within mainland" must store that information "within mainland China," and that businesses may transfer such information overseas only after passing an undefined security assessment;
- CII operators must implement *additional* data security procedures, such as background checks, education, training and formulating emergency response incident plans;
- CII operators are required to annually inspect and assess their network's security and risks; and
- CII operators must undergo a national security review before purchasing any products or services that "may affect national security." The law, however, provides no explanation as to what a national security review entails, and does not specify the types of products or services that may affect national security. Not surprisingly, questions remain as to the review's intrusiveness and whether it will require disclosure of intellectual property or trade secrets.

How does the law address the protection of personal information?

The law imposes requirements on network operators that collect personal information, which is defined as any type of information "that taken alone or together with other information, is sufficient to identify a natural person's identity, including, but not limited to, natural persons' full names, birth dates, identification numbers, personal biometric information, addresses, telephone numbers and so forth." Generally speaking, the law requires network operators that maintain the confidentiality of the user data that it collects, and to otherwise "abide by the principles of legality, propriety and necessity." Accordingly, network operators will be prohibited from:

- gathering personal information unrelated to the services they provide;
- disclosing, tampering with or destroying the personal information of an individual that they've gathered; and
- providing an individual's personal information to third parties without the individual's consent, unless such information has been permanently depersonalized or disassociated so as to not identify the particular individual.

Individuals may request that network operators delete their personal information if they discover that the collection or use of their information is in violation of the law. An individual may also request that network operators correct any inaccurate personal information.

The law also seems to require network operators to have data security policies and incident response plans by requiring them to "adopt technological measures and other necessary measures to ensure the security of personal information they gather, and [in the event that a leak occurred] or might occur, remedial measures shall be immediately taken, and provisions followed to promptly inform users and to make report to the competent departments in accordance with regulations." Similarly, the law requires network operators to "establish network information security complaint and reporting systems, publicly disclose information such as the methods for making complaints or reports, and promptly accept and handle complaints and reports relevant to network information security."

What are the penalties for non-compliance?

Violations of the law can result in a host of penalties, including warnings, suspensions and fines in amounts up to RMB 1,000,000 (≈$144,579.71). The law even provides specific penalties applicable to foreign business operating in China, for example, freezing assets and sanctions.

Conclusion

Given the potentially broad application of this law and its burdensome requirements, particularly its data localization, access and review requirements for critical information infrastructure, companies doing business in China need to be aware of the law's requirements and how it may impact them. Additionally, companies doing business with Chinese vendors should consider engaging in discussions with them regarding the applicability of the law to their business and any services they provide to you once the law takes effect. For questions about the law, please contact Heather Enlow-Novitsky, Scott Guttman or your Vorys attorney.