WINSTON & STRAWN LLP

CLIENT ALERT

New Provisions Covering Enforcement Under the PRC Cybersecurity Law

OCTOBER 22, 2018

Approximately one year after the PRC Cybersecurity Law (the "CS Law") went into effect the Ministry of Public Security of the People's Republic of China issued the Provisions on the Supervision and Inspection of Cybersecurity by Public Security Organs (the "Provisions"). Effective from November 1, 2018 the Provisions are significant in that they add detail to the role that the Public Security Bureaus (the "PSB") will play in enforcing the CS Law going forward.

By way of background, the CS Law requires "network operators" to:

- Develop internal security management rules and operating procedures, appoint network security personnel, and generally be responsible for cybersecurity protection;
- Take technical measures to prevent computer viruses, network attacks, network intrusions, and other acts which may endanger cybersecurity;
- Take technical measures to monitor and record the status of network operations and cybersecurity incidents, and preserve relevant weblogs for not less than six months as required;
- Take measures such as data categorization, and back-up and encryption of important data; and
- Perform other obligations as prescribed by laws and administrative regulations; and
- Provide "technical support and assistance" to law enforcement authorities to safeguard national security and investigate crimes.

Under the Provisions, the PSB are granted the right to, among others and without a warrant: (1) conduct on-site inspections including computer rooms and work areas and (2) interrogate employees, (3) review and copy information relevant to cybersecurity, and (4) inspect an operation's cybersecurity protection measures in order to ensure compliance with the CS Law.

The PSB has had similar rights since at least since 2006. However, the fact that the PRC Ministry of Public Security issued these Provisions now would seem to indicate that they take the CS Law seriously and are basically warning residents of China to make sure that they are compliant. On the other hand, the Provisions may also have a more sinister effect.

On its face, the PSB is limited to the purpose of preventing crimes, protecting cybersecurity, and protecting legal interests of citizens and legal entities. However, China's far-reaching inspection and supervision power coupled with a lack of detailed procedural requirements may put multinational companies' sensitive information and trade secrets at risk of exposure. This is especially true in the case of the CS Law, which defines a "network operator" as any entity or person that owns, administers, or provides services through a network. This means that a network operator can be any individual or entity that has access to or uses a network in its business or operations.

The potential that the Provisions may be abused as a tool to require any and all companies within China to grant the government access to its networks, under the guise of undefined "national security" as well as "public security," will surely be weighed when companies are deciding whether to store technology, trade secrets, and confidential information within China.

Tip: Lawyers, compliance officers, and multinational companies who do business in China should (1) pay close attention to the promulgation and enforcement of the Provisions by the PSB and (2) assess its impact to sensitive information stored and transferred to China, as well as (3) assess compliance of the internal cybersecurity policy with the requirements set forth under the Provisions.

2 Min Read

Related Topics

Privacy and Data Security | Compliance Programs | Asia

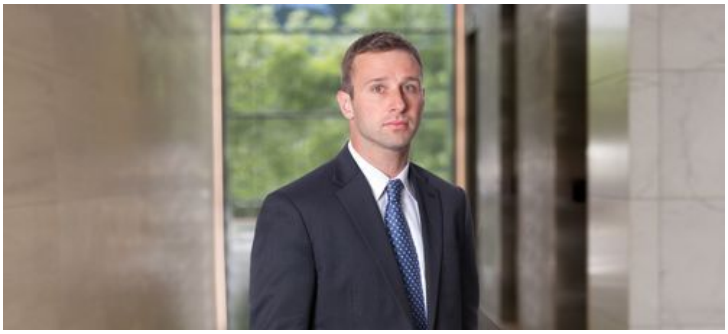
Related Capabilities

Privacy & Data Security | Compliance Programs

Related Regions

Asia

Related Professionals



Steven Grimes