The Challenges of China's New Cybersecurity Law

All the nations of the world can agree: cybersecurity is crucial to national security. But what if a nation's cybersecurity laws have the effect of erecting trade barriers? That's the question being asked of China's new cybersecurity legislation, which went into effect June 1.

The new Chinese law is mind-boggling in both its breadth and its vagueness. Among its requirements:

- "Network operators" (apparently any company that maintains a computer network, but the scope is unclear) must obtain the consent of individuals before collecting their data (more of a privacy than a security requirement), keep a log of data security incidents, fix any security flaws immediately, and back up and encrypt data.
- Providers of "critical information infrastructure" must meet additional requirements, including storage of personal information and "important data" within China. (A last-minute rule change appears to have expanded this data localization requirement to network operators as well.)
- Under draft implementation rules, set restrictions on international transfers of data – including by empowering Chinese authorities to block transfers deemed to endanger China's political system, economy, security or technology. Fortunately, the Cyberspace Administration of China has decided to delay implementation of restrictions on cross-border data flows until the end of 2018.
- Cybersecurity products must meet certain standards in order to be marketed in China and must undergo inspection and verification.

National and international business groups, alarmed by these requirements and uncertain how to comply, have taken the unusual step of drafting a joint letter to the Chinese government and relevant ministries asking that implementation of the law be delayed. This letter declared that the signatories were "deeply concerned" that the law "will effectively erect trade barriers along national boundaries that effectively bar participation in your market and affect companies across industry sectors that rely on information technology goods and services to conduct business."

Of particular concern to the international business community are provisions in the cybersecurity law that mandate broad data residency requirements and restrictions on cross-data border flows, trade-inhibiting security reviews and requirements for IT products and services, and broad requirements for data sharing.

Given the huge uncertainties surrounding the intended scope of the cybersecurity law and how China intends to enforce it, a "wait and see" approach on the part of foreign tech companies is probably the best – and may be the only feasible — strategy.