China's upgraded cybersecurity law could take a toll, by Joe Uchill, Axios, October 16, 2019

China is applying tougher cybersecurity standards more widely as of Dec. 1, requiring companies to open their networks and deploy government-approved equipment. The changes worry international organizations and underscore the difference between U.S. and Chinese approaches to cybersecurity.

The big picture: China already has a law, applying to the most secure networks, that allows the government to audit private business networks and mandates the use of government-approved security equipment. That law will now apply to all networks.

- "It's going to be incredibly invasive," said Adam Segal, director of the Digital and Cyberspace Policy Program at the Council on Foreign Relations.

Background: China's cybersecurity law has been on a slow rollout since 2017. Clarifications of standards serving as de facto regulations were introduced in May this year.

- Those included the right for China to plug into networks and check for cybersecurity, as well as mandates about securing supply chains for network security.
- Until December, those standards only technically apply to companies where breaches could cause national security problems, though Chinese officials often hold companies to regulations in advance of their formal launch dates.
- "Now the standards will apply to any company with a network," Samm Sacks, a fellow at the New America think tank, told Axios.

This puts a burden on U.S. companies that American companies are not used to. "Chinese companies won't bat an eye at it," Sacks said.

- Given China's record of using hackers to steal intellectual property from global competitors, some network owners worry — justifiably, according to experts — that allowing China access to their data puts corporate secrets at risk.
- China has a history of using any means necessary to aid domestic businesses. That could now include ruling that a foreign company has failed to meet official security muster — boxing competitors out of China's market.

But, but, but: Those worst-case scenarios might not be the problem immediately at hand, said James Lewis, who currently heads cybersecurity at the Center for Strategic International Studies and formerly served in several federal positions evaluating and negotiating with China.

- "The Cybersecurity Authority of China [CAC] insists it won't use the law to steal private information. And China has so many other ways to steal intellectual property that it probably doesn't need to," Lewis told Axios.
- As with all things China, if the party tells the CAC to steal data in the future, it will do so, Lewis added.

The most immediate problem may be that the cost of compliance can become prohibitive for some firms to operate in the country. "If you are a smaller company, you may think twice about moving into China," said Segal.

- The broader trade conflict between the U.S. and China makes it tougher for foreign firms to protest.

Chinese firms have a poor record on cybersecurity, said Lewis. The tougher law, at least ostensibly, addresses a very real issue.

The U.S. faces similar issues, but it addresses them differently. The U.S. operates using fewer top-down security requirements, choosing instead to emphasize trade groups setting industry standards.

- The U.S. is far more permissive about lower-risk networks, offers more autonomy to network administrators, and generally uses a scalpel where China uses a chainsaw.

One thing the U.S. and China have in common: "In China, network operators have to submit to 'black box' security reviews. We have no idea what it takes to pass," said Sacks. "I'm beginning to see that from the Trump administration."