The Challenge of Complying with China's New Cybersecurity Law

By Dan Whitaker
May 2017

In a bid to assert control over cyberspace, China passed a sweeping cybersecurity law that affects virtually every company doing business in that country. The law is set to go into effect June 1, 2017. Despite its broad reach and potential for disruption, it appears that very few legal professionals are aware of the law.

A 2017 survey by Consilio showed that just a quarter of legal tech professionals are aware of the law. Just 2% are “very aware” and a scant minority (14%) are “very concerned.”

More worrying, the majority of the respondents (57%) said they had at least one legal matter that touched China within the last two years. More than a quarter of respondents (27%) said their organizations were involved in at least 10 legal matters that touched China over the same period.

Given the fact that the law affects virtually every company that does business in China and carries harsh penalties, it could be time for a fast ramp-up. For many companies, their legal and compliance departments will be at the forefront of compliance efforts. It’s hard to overstate just how comprehensive the law is. A key aspect applies to all “critical information infrastructure” operators — a term that has yet to be clearly defined but appears to apply across the board to public and private businesses and sectors. The law also applies to any business using telecommunications networks, which includes all the tools of modern commerce, such as email, cloud computing, data centers, e-payments, search, office enterprise systems, music, mapping and video, among others.

Every foreign business will have to comply with the major tenets of the law, including data localization and transfer, software review, and cooperation in criminal probes.

Rigid Rules for Data Transfer, Technology and Investigations

Under the data localization requirement, Critical Information Infrastructure (CII) operators must store in Mainland China any data on Chinese citizens and businesses gathered there. They must also comply with strict guidelines, including ensuring the data contains no “state secrets, prior, to transferring the data outside the country. That is a complete shift for companies accustomed to a global, relatively boundary-free Internet.

In addition to the data localization requirements, the law also gives the Chinese

government unprecedented access to the technology of foreign companies. Specifically, the law provides that “critical network equipment” and “specialized cybersecurity products” — both of which are still being defined — must meet national standards and be certified by the Chinese before they can be distributed or sold in China.

The provision has sparked strong fears in the foreign business community that it could compromise the security of hardware and software. For example, companies could be required to supply a decryption key or backdoor access.

Finally, under the law, Internet operators must cooperate with criminal and national security investigations. If criminal activity is suspected, they must give government investigators free access to their data.

Multinationals Face New and Complex Challenges

Given the broad scope of the law and China’s growing prominence as the world’s second largest economy, there is great potential to severely crimp how foreign businesses operate in China and around the world.

When the law was proposed, it drew widespread resistance from foreign businesses. Critics saw it as arbitrary, anti-competitive and a drag on cross-border innovation. Many companies objected on the grounds it would be used to favor Chinese companies, such as software providers, over international businesses.

There was also concern it would be used as a tool of political control or retribution to advance the business and economic interests of the Chinese government

However, the law was enacted despite these objections and multinational corporations ignore it at their peril. Organizations that do not adhere to the law will face potential financial penalties, including the possible loss of their ability to conduct business in China. Individuals can face civil and criminal penalties, up to and including imprisonment and the death penalty for particularly egregious cases.

Evolving Landscape Complicates Compliance

Despite the added risk and cost, most global companies (or those that aspire to be global) won’t step away from the economic opportunities China offers. Therefore, they must have a full understanding of the new cybersecurity law and evolving regulatory landscape.

This is complicated by the fact that critical guidelines are still being developed. The State Council, the Cybersecurity Administration of China and the Ministry of Industry and Information Technology must still issue implementing regulations and standards. Also, as the law has yet to go into effect, it is impossible to know how widely it will be

enforced.

Further, it's important to understand that the cybersecurity law reflects a changing mindset. Since 2012, cyber walls have been going up in multiple regions around the world including in the European Union. As countries continue to create new regulations, organizations must continually educate themselves on the evolving nuances of data privacy laws in every jurisdiction, specifically as it relates to the ability to move data in and out of the countries in question

China has taken the position that its data is a state asset, similar to any other national resource, and that asset must be vigorously protected. Violations of acceptable use of that data could be construed as espionage or other crimes against the Chinese government — with severe punishment for infractions.

Litigation Clampdown Expected

It's unclear how the law will play out, but there is one area where China seems determined to launch a major clampdown — litigation proceedings. The government appears to be signaling its strong preference to keeping data, including discovery materials, inside China and adding an extra layer of review by Chinese law firms to ensure "state secrets" do not cross the border.

Strategies for Working Within the Law

While it can be challenging to work within the law's parameters, some multinational companies and their attorneys are finding ways. To begin with, they acknowledge that there are cultural and language gaps that can create misunderstanding. For example, documents that seem innocent to Americans, such as customer lists, weather reports or pricing spreadsheets, can, under certain circumstances, considered to be state secrets in China.

Second, they have begun to develop a full understanding of their company's data and technology infrastructure. This triage process can be complex and time-consuming, but it is absolutely necessary. If the data must go through a security protocol it would be helpful; the fewer surprises, the better.

Third, some companies doing business in China have found that independent service providers can offer useful services. There are companies that will host the data, perform a document review and do a state secrets review in cooperation with a Chinese law firm, all within mainland China. Only after those steps have been completed, can the data potentially leave China. It is important that multinational law firms work with a third party that understands and "lives" the data regulations to ensure their discovery efforts remain defensible in both litigation and investigation matters.

Conclusion

The soon-to-be-implemented cybersecurity law is a game-changer. It severely restricts the free flow of information across borders, constructing new legal boundaries that carry severe penalties if they're breached. Legal teams will be the first line of defense. It's important they get up to speed quickly and don't underestimate the massive legal and business implications of China's unprecedented cybersecurity law.

***** **Dan Whitaker** is a managing director for Consilio's China Operations. He works with senior partners at law firms and general counsels at global Fortune 1000 companies to help them with document collection, storage, management and review for FCPA investigations, self-investigations, and litigation.