HUNTON& WILLIAMS

Lawyer Insights

November 21, 2016

China's data localization provision is bad for the nation

by Manuel E. Maisog

Published in IAPP's Privacy Perspectives

On Nov. 7, 2016, a new cybersecurity law was finally passed in China. The law will go into effect on June 1, 2017. The passage of the law followed the publication of two earlier drafts for public comment, and while it differs from the preceding second draft in particular details, its general gist does not differ fundamentally from that of the preceding draft.

The actual name of the law (translated very literally from the original Chinese text) is the "Network Security Law" of the People's Republic of China. The law is fairly wide-ranging and has multiple aspects. Specifically, here, I am going to focus on its data localization provisions.

The final data localization requirement requires enterprises that operate "key information infrastructure" to store personal information and critical data collected and generated in the course of their operations within the territory of the People's Republic of China. Where there is a genuine need, resulting from business necessities, for the enterprise to provide this information and data to places outside of China, a "security assessment" will be conducted in accordance with procedures formulated by National Cyberspace Administration acting in cooperation with relevant governmental departments under the State Council.

The changes to the final data localization requirement actually materially expand the scope of the requirement from that which had been presented in the preceding draft. In the final law, the enterprise is required to store personal information within the territory of China. Therefore it applies to all personal information collected and generated by the enterprise in the course of its operations within the territory of China, regardless of the citizenship of the persons identified by it.

In the preceding draft, the enterprise was required to store critical business data within the territory of China. In the final law, the enterprise is required to store critical data within the territory of China. The final data localization therefore applies to all critical data collected and generated by the enterprise in the course of its operations within the territory of China, regardless of whether it is business data.

I have written before about the deleterious effect that a data localization requirement would have in China. That assessment has not changed.

> *Data localization is a bad deal for China. It is the product of the same sort of excessively introspective, navel-contemplating mentality that led to the claustrophobically walled-in, politically correct neuroses of the Cultural Revolution.*

China's data localization provision is bad for the nation
by Manuel E. Maisog
IAPP's Privacy Perspectives | November 21, 2016

Data localization is a bad deal for China. It is the product of the same sort of excessively introspective, navel-contemplating mentality that led to the claustrophobically walled-in, politically correct neuroses of the Cultural Revolution. If allowed to crystallize in an unadulterated, pure form, it will have the effect of isolating China from the participation in global economic activities. The eventual price will arrive in the form of lower competitiveness for China in relation to the outside world.

A digital and commercial reincarnation of the HMS Nemesis could be on its way.

That the data localization requirement has survived into the final law is therefore regrettable. It is something neither I nor anyone who wishes the best for China, or for the enterprises that invest and do business here, should have wanted to see.

But there may be a mitigating factor. The data localization obligation applies to "operators of key information infrastructure." This is defined as information infrastructure of which damage, loss of functionality or data leakage would seriously jeopardize national security, the national economy, and the people's livelihood and the public interest. Though this is not an exhaustive list, it specifically includes public communication and information services, energy, transportation, water conservancy, finance, public service and e-government affairs.

This does not appear to result in a blanket application to all enterprises everywhere. To become subject to the data localization requirement, an enterprise must not merely be within one of these industry sectors; it has to be the operator of information infrastructure within that sector that has truly macroeconomic significance. Operating one's own enterprise-level internal information network might not rise to this level.

As an example, and just to speculate for the time being, an enterprise in the energy sector that operates an individual wind farm and includes a SCADA system and internal email may be operating an information infrastructure that is important to it at its own microeconomic level, but to find the enterprise that has truly macroeconomic significance and is therefore an "operator of key information infrastructure." One might have to look to the level of the provincial or regional grid operator, or to the operator of the regional wholesale electricity spot market.

In other words, the data localization obligation may be restricted to a relatively limited scope of enterprises. Those not within this scope may be permitted to transmit information to overseas destinations as before. The existence within the same statute of the separate term, "network operators," alongside the term "operators of key information infrastructure," does suggest that the scope of the latter is narrower than the scope of the former. This will clarify only upon the issuance of implementing regulations and actual interpretation and application over time by the relevant enforcement authority.

As the practical impact of this law unfolds, containment of the scope of the term "operators of key information infrastructure" is therefore the best result to hope for at this point. If this can be done, losses and damage deriving from the data localization provisions might be minimized, both for those enterprises, which have invested and still operate in China, and for China herself.

Manuel Maisog is a partner and Chief Representative of Hunton & Williams' office in Beijing. Bing's practice focuses on sophisticated cross-border transactions involving Asia and especially China, with an emphasis on energy, mergers and acquisitions, foreign direct investment, and personal information protection. Prior to the establishment of the Beijing office, he was resident in both Bangkok and Hong Kong, and worked on significant project finance and project acquisition transactions in many countries across Asia. He may be reached at +86 10 5863 7507 or bmaisog@hunton.com.

