
China Forecasts 2017 (#4): New Laws Create New Risks

December 27, 2016 By [Gordon Orr](#)
Board Member at Lenovo, Swire Pacific

This post is the fourth in a series I'll be publishing here over the coming week with some of my forecasts for the Chinese economy in 2017. Follow me to read more of my predictions for China in the new year.



China's lawmakers and regulators were active in 2016, with multiple new laws affecting businesses. Ensuring compliance will be a significant headache, especially for multinationals, as what the laws mean in practice will only be defined over time.

Take one example: the Anti-Unfair Competition Law, which overlaps with the Anti-Monopoly Law, had significant changes proposed in 2016 to prohibit the "abuse of a relative advantageous position." This is open to a wide interpretation, potentially allowing small retailers and suppliers to pursue claims against larger business that they deal with.

The law also means employers become liable for bribes and inducements offered by their employees, even if they didn't know bribes were being offered. Multinationals will complain, but these standards are little different from those they are required to follow in many other countries and which are part of corporate ethics commitments.

In November, a new cybersecurity law was published, with implementation due in mid-2017. Requirements on data localization, reporting cyber incidents to the government, the usage and sharing of personal information, and constraints on the publishing of any content online mean almost every multinational operating in China will have to change aspects of its operating model.

Maybe companies will need a network architecture that no longer backs up data outside China or a team within IT that simply reports network events to the Ministry, as required. Enterprises that publish content online in China may need to meet new local ownership requirements and understand the review and monitoring obligations that ensure content is deemed acceptable by the government.

The law is creating lots of uncertainty and work, and even some larger enterprises will find themselves inadequately prepared and made examples of. Rather than simply being deported, last year saw more cases of foreign business executives being detained (most recently Australian casino employees)—and we'll likely see more this year.

China is likely to soon suffer a massive public breach of consumer data. Many corporations are lax with regard to cybersecurity: for example, the China Banking Regulatory Commission recently criticized several banks for allowing their employees to sell personal information without any corporate oversight.

Chinese consumers tend to be quite relaxed about how their personal information is shared and used, partly because a large-scale leak has not yet happened. Yet it's easy to imagine global hackers entering the systems of a bank or an Internet company that handles payments and making the data obtained public. Public opinion could then change very quickly, leading to a heavy-handed government reaction and a major clampdown on how data is protected or sold.

The impact on many leading Chinese companies could be that they invest much, much, more in cybersecurity. And some Chinese business leaders may be prosecuted for failing to protect their customer's information sufficiently well.