Surveying the Impact of China's New (and Toothy) Data Privacy Laws on the WeChat Generation of Employees

By T. Markus Funk, Mason Ji, and Huijie Shao

Foreign companies and their lawyers conducting internal investigations in China have long been aware of the challenges of collecting, storing, and reviewing data coming in and out of China.

The country is ramping up investment in technology and data, and passed two data privacy laws in 2021 as part of this effort—the Personal Information Protection Law and the Data Security Law.

This scrutiny presents significant new challenges that foreign companies and their lawyers with Chinese business interests must be aware of. One salient area of risk to monitor is business use of third-party messaging apps like WeChat.

China's New Data Laws

China's recently enacted data laws govern data originating or used inside China. But they also seek to regulate data processing activities taking place outside of China that have the potential to adversely impact its national security, public interest, or the legal interests of any citizen or organization.

The laws establish a regulatory hierarchy for all impacted data. For example, they refer to "important data" that requires elevated protection protocols—i.e., firewalls—localization, and security assessment of cross-border data transfers by data processors, including critical information infrastructure operators.

An additional class of data is highlighted as "national core data," or data that represents a "serious threat" to China's national security. Foreign lawyers conducting investigations in or involving China must keep up to date on what currently falls within the ever-shifting scope of this regulatory hierarchy in their industry and region by consulting—through third parties, as advisable—relevant local governments and regulatory agencies prior to starting their investigations.

Failing to get it right can be costly. Those running afoul of the new data laws should also bear in mind that "violation of the national core data management system or endangering China's national sovereignty, security, and development interests" is punishable by an additional fine of up to 10 million Chinese yuan (approximately $1.56 million), revocation of business licenses, suspension of the business, and, in aggravated cases, criminal liability.

WeChat Use Is Widespread

Another point of discussion is how employees in China tend to connect. Business communications and the corresponding data in China—unlike, say, in the US or Western Europe—are generally not transmitted through corporate-controlled and regulated environments.

Instead, third-party messaging platforms are the preferred way that China-based employees tend to connect. Foreign lawyers with experience conducting investigations in China likely already understand the ubiquity of WeChat use. And, as a study by Stanford economist Nick Bloom found, work-from-home has significantly increased the use of electronic communication among Chinese workers; a learned habit that persists even when those employees return to work.

It is no overstatement to say that WeChat is used by virtually every Chinese employee in virtually every aspect of their lives, including for hiring transportation, paying for goods and services, and sending business communications.

The ubiquity of WeChat for business activities represents a unique risk factor for companies with offices or relationships in China. Although Chinese companies may have policies and regulations that seek to limit the use of WeChat for company business, in the real world, most employees use WeChat for at least some of their business communications. In short, a more practical approach is required.

Data Security Compliance Implications

The upshot of WeChat's dominance in China is that corralling "business communications" for investigative purposes is exceptionally challenging—especially in light of the stringent requirements of the new data laws. Even companies that spend millions on cutting-edge networks to protect their internal data and comply with the laws cannot overcome the risk that employees will routinely send sensitive, confidential business information over WeChat to their friends or contacts.

As a result, alert investigators should always at the outset examine whether company information was passed to individuals not authorized to view the information via WeChat, and sending such information over WeChat violated company policy or governmental regulation.

These risks are compounded when individuals commonly have multiple WeChat accounts. The good news is that accounts

---

Markus Funk is a partner and Mason Ji and Huijie Shao are associates at Perkins Coie. Portions of this article are reprinted with Bloomberg Law's permission.

are linked with individuals' phone numbers or national identification numbers, so lawyers who prepare for employee interviews and conduct investigations should always try to use these identifiers to check whether an individual has multiple WeChat accounts.

Navigating Investigations

Prior to the new data laws, companies and investigating lawyers had leeway to finesse how they obtained WeChat data from a suspected violator. Now, they must obtain written consent before such information can be accessed. Although WeChat messages are generally stored for at least six months by Tencent, the company that owns WeChat, such information is generally only obtainable by the Chinese government upon request.

Chinese authorities, in turn, will likely only allow access to WeChat messages by companies if those messages do not relate to "important data" or "national core data," and the agency or department granting the request will depend on the requesting company's geography and industry in making these decisions. This process will almost always significantly delay any investigation.