GOWLING WLG

SECOND DRAFT OF CHINA'S NEW CYBERSECURITY LAW RAISES CONCERNS FOR FOREIGN ENTERPRISES

10 October 2016

In July 2016, a second draft of a new cybersecurity law was released in China, which strengthens controls over the flow of online information and enhances protection of personal data. This law has important implications, given that China has the largest and fastest growing e-commerce market in the world.

The first draft of this law was released in July 2015 and sparked significant opposition from foreign investors, as it was felt that certain provisions restricted trade and were particularly discriminative against foreign companies. The second draft fails to resolve these concerns and has led to a significant number of global associations petitioning Premier Li Keqiang, urging Beijing to revise the draft.

So, what's changed?

The major concern from foreign companies is that the new draft unprecedentedly addresses the cyberspace sovereignty principle over internet information. Under the new draft law, internet operators (including owners, network administrators and online service providers) in "Key Infrastructures" are required to store:

- "important business information" (which is currently undefined);and
- any personal data relating to their internet users which is generated in China on their Chinese servers.

Any transfer of such data out of China for commercial purposes will be scrutinised by Chinese authorities who have the power to deny any international transfers of such information. This could affect, for example, the transfer of data between parents and subsidiaries in global companies.

In the first draft, the definition of "Key Infrastructures" included references to some specific sectors such as TV-broadcasting, energy and social security. However, critically, it also included an "internet, or system run by any internet operators that has a significant number of users". The concern was that such language could be interpreted extremely broadly.

The second draft modifies the definition of "Key Infrastructures" and, positively, removes the language concerning "significant number of users" - perhaps in an attempt to appease the concerns mentioned above. The new definition now includes "industries that relate to national security, citizen's wellbeing, and public interests". However, the ambiguity of such wording still raises major concerns for foreign companies. For example, including a "public interest" and/or "citizen's wellbeing" criteria in the definition could still be construed very broadly, which would allow companies to be easily categorised into the "Key Infrastructures" definition. If a company falls under this definition, it potentially creates significant restrictions and delays when exchanging China-generated information internationally from China.

Addressed concerns

It is speculated that the scrutinisation of such data may lead to the exposure of sensitive information which could somehow be leaked to domestic competitors. This is due to the requirement for those companies defined as "Key Infrastructures" to store "important business information" and "personal data" of users on servers in China. To address this concern the revised draft has expressed that "any data obtained by the authorities from Key Infrastructures will be used for the sole purpose of safeguarding internet security" - in order to provide some comfort and reassurance to companies operating in China. It remains to be seen if this wording will appease foreign companies but it is unlikely to be sufficient.

Even for those not categorised within the "Key Infrastructures" definition, the use and sale of personal data under the cybersecurity law draft is restricted. This is because, over the last decade, illegal trading and use of personal data and contact information has become more prevalent, opening the floodgates to frauds which have long been plaguing China's cyberspace and telecommunication channels.

A recent case drew intense public attention when a high-school graduate died of a heart attack after being swindled out of all her family's savings for her college education. The schoolgirl's personal details had been obtained by an imposter claiming to be from the Ministry of Education. This case is one of many which show how easy it is to access

personal information online and the potentially severe repercussions for improper handling of personal data.

The government has tackled this problem by issuing a series of new laws which focus on reducing the illegal selling and use of personal data including the proposed cybersecurity law. The first draft of the law particularly emphasised the prohibition of the sale or use of personal data without the person's consent and imposed ground-breaking penalties. These penalties are repeated in the second draft and include:

- a fine ranging between one and ten times the profits resulting from the illegal use of personal information;
- a fine of CNY 500,000 (approximately £58,000) if no profits were gained; and
- the possible suspension or revocation of a company's business licence.

Given that it is common practice for companies to exchange anonymised personal data, after the publication of the first draft of the law, many internet operators argued that the transfer or sale of such anonymised data should be exempted from the prohibition of sale without consent. The second draft clarifies this position and confirms that anonymised personal information shall not be subject to the sale without consent prohibition. This offers companies reassurance that, going forward, the transfer of information, such as consumer behaviour statistics, is permitted - provided the data is anonymous. Additionally, this provision ensures that internet users are protected, as any information - which relates to that user - that is sold or transferred will not be directly associated with their true identities.

Next steps...

The second draft has entered the final round of revision by the National People's Congress and the cybersecurity law is expected to be promulgated, at the latest, by the end of 2017. A close eye needs to be kept on any updates to this law. However it seems likely that many provisions from the second draft will remain materially unchanged, such as the new restrictions on those within the "Key Infrastructures" definition and the enhanced restriction over the use and sale of personal data.

Whilst there are many provisions in the second draft of the cybersecurity law that appear to be relatively uncontroversial, foreign companies looking to invest in China - or indeed those with an established business in China - should be mindful of the new cybersecurity law changes. They should begin to consider how internal measures can be implemented in order to comply with the new law, particularly those discussed above. A few points worth

considering include:

- The need for companies in China to obtain consent from internet users for the transfer or sale of their personal data; and
- The need for companies in China, which may potentially fall under the "Key Infrastructures" definition, to store and record all business information and personal data generated on servers within China.

Gowling WLG has a wealth of cyber incident legal support expertise. We're equipped to investigate any cyber incident, minimise and/or mitigate its effects, identify the culprits and deliver fast, effective solutions.

Related Tech, Dispute Resolution, IT Litigation, Intellectual Property, ThinkHouse

Author

Jamie Rowlands

Partner - London

Email

jamie.rowlands@gowlingwlg.com

Phone

+44 (0)20 7759 7891

vCard

Jamie Rowlands