# Living with and Thriving under Increasing Data Security Scrutiny in China

Elizabeth Chien-Hale

In the world where data is becoming the hot new commodity for commercialization, China, along with the rest of the world, is enacting laws to protect national cybersecurity and commercialization of personal data.

A series of interconnected laws

In 2017, China enacted the first of the three laws on cybersecurity and data privacy, the Cybersecurity Law of the PRC ("CSL," 中华人民共和国网络安全法). [1] The CSL came into effect on June 1, 2017. This law offers guiding principles for issues that are of long-term importance for network security and cyberspace activities. The CSL sets required obligations for network operators in the PRC to safeguard security and integrity of its network, thus allowing more cybersecurity legislation to be built on top of it. The term critical information infrastructure ("CII") became a term of art and is used in subsequent laws and regulations, and a CII Operator("CIIO") is subject to special requirements with respect to cross-border transfer of data of products and services.

Next came the Data Security Law ("DSL," 中华人民共和国数据安全法) of 2021.[2] This law came into effect on September 1, 2021, and governs the collection, storage, use, processing, transmission, provision, and disclosure within China. The law has significantly impacted Chinese technology companies (and their stocks prices) such as Meituan, Alibaba and Didi which may collect or utilize data on Chinese citizens. Not only does the DSL define data very broadly as "any record of information in electronic or any other form,"[3] this law may also apply to data processing activities outside of the territory of the People's Republic of China under certain situations.[4] The law prohibits the export of data without first completing a "cybersecurity review," a procedure which is still being refined. Furthermore, the government must be a part of handling requests for data made by foreign judicial or law enforcement. Without government approval, organizations or individuals in China may not provide data stored within China to any overseas judicial or law enforcement body.[5]

Finally, the Personal Information Protection Law ("PIPL," 中华人民共和国个人信息保护法) became effective on Nov. 1, 2021.[6] China's PIPL has received wide attention and is sometimes compared to the European Union's General Data Protection Regulation ("GDPR"), one of the world's earliest data privacy and security laws.

Like the GDPR, the PIPL applies to all individuals, organizations, and corporations that handle the personal information of individuals within China's borders. The PIPL may be seen as stricter than the GDPR. For example, while the GDPR allows companies to process personal data if the data is collected legally and with a justifiable basis, the PIPL does not provide a "legitimate interest" processing basis; the PIPL uses consent as the primary basis for data processing even though there were efforts to include a similar "legitimate interest" basis for data processing.[7] In other words, companies that do business in China must obtain an individual's consent before handling their personal information, except for the six exceptions outlined in Article 13.

Some observers would say that these laws-CSL, DSL, and PIPL- are enacted in a period of increasing competition in laws between China and the United States in the areas of trade, intellectual property and national security, and in the context of the US-China trade war started by the Trump Administration. However, ironically, the most famous punishment under the application of the CSL, DSL, and PIPL is the Chinese tech company DiDi, a Chinese ride-hailing app company similar to *Uber*. Citing unspecified violations of the cybersecurity, data security, and personal information, Didi was ordered to pay a US$1.2 billion fine; [8] of course, DiDi was also forced to delist itself from the US New York Stock Exchange.[9]

Continuing developments

The PIPL continued to take shape in 2022 when the Cyberspace Administration of China ("CAC") issued a wide range of regulations and draft proposals. For example,

*Cybersecurity Review Measures* – These Measures were issued in conjunction with various other Chinese authorities in January 2022; they seek to broaden the scope of circumstances that trigger a cybersecurity review. The Measures also specify the nature of the cybersecurity reviews.

In July 2022, the CAC also finalized *Measures for Security Assessment for Cross-Border Data Transfers*. These measures provide specific circumstances and a catch-all situation for mandatory data security assessment.

In addition to the above examples, there are and will be many other regulations to be issued and revised in these areas, suggests that the Chinese government is still shaping the principles in the CSL, DSL, and PIPL to suit its development needs.

Another problematic trend is that the Chinese government is likely to delegate enforcement and rule-making powers on a sector-by-sector basis: automotives, telecommunication, health care, etc. As a veteran IP attorney, I have observed this same tendency to delegate powers horizontally and widely in the intellectual property arena, which has led to a complicated

enforcement system involving multiple agencies with overlapping jurisdictions, thus creating a difficult system to understand and to utilize.

Implications beyond compliance hurdles

Multinational organizations should view data protection, privacy, cybersecurity laws and regulations in the larger context of geopolitics: Nations use data protection in order to assert policies, influence diplomacy, enforce national security, and further economic competitiveness.

Data localization, transportation, and typography are challenging activities that require concerted effort and significant investment from a company's Board, executives, and management teams, just as IP protection has been for companies in the past.

Work arounds

Companies should build compliance teams to execute and to keep companies up to date with respect to data security, transfer, and localization requirements. At the same time, there are a few channels that may serve as workarounds for compliance demands:

1. Anonymization of data: Strip personal information from the critical or personal data collected.
2. As AI tools become increasingly powerful, can the commercial projects be accomplished by synthesized data, rather than collected personal data or critical data?
3. Push the governments to negotiate reciprocal data transfer rights in multilateral or bilateral trade agreements between trade blocks.

[1] Cybersecurity Law of the PRC, issued by the Standing Committee of the National People's Congress on November 7, 2016 and effective as of June 1, 2017; *see Chinese version at* http://www.cac.gov.cn/2016-11/07/c_1119867116_3.htm.
[2] Data Security Law of the PRC, issued by the Standing Committee of the National People's Congress on June 10, 2021 and effective as of September 1, 2021; *see an official for-reference translation at* http://www.npc.gov.cn/englishnpc/c23934/202112/1abd8829788946ecab270e469b13c39c.shtml.
[3] *Id*. Art. 3.
[4] *Id*. Art. 2.
[5] *Id*. Art. 26
[6] Personal Information Protection Law of the PRC, issued by the Standing Committee of the National People's Congress on August 20, 2021 and effective as of November 1, 2021; *see Chinese version at* http://www.cac.gov.cn/2021-08/20/c_1631050028355286.htm,
[7] *Id*. Art. 13
[8] *See* http://www.cac.gov.cn/2022-07/21/c_1660021534306352.htm;
[9] *Didi Says It Will Proceed With Delisting From NYSE*, WALL STREET JOURNAL (May 23, 2022), https://www.wsj.com/articles/didi-says-it-will-proceed-with-delisting-from-nyse-11653310564.