



Llinks Corporate and M&A Bulletin
December 2018

上海
上海市银城中路 68 号
时代金融中心 16 楼和 19 楼
邮编: 200120
电话: +86 21 3135 8666
传真: +86 21 3135 8600

北京
北京市建国门北大街 8 号
华润大厦 4 楼
邮编: 100005
电话: +86 10 8519 2266
传真: +86 10 8519 2929

香港
香港中环皇后大道中 5 号
衡怡大厦 27 楼
电话: +852 2969 5300
传真: +852 2997 3385

伦敦
1F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

www.llinkslaw.com

SHANGHAI
16F/19F, ONE LUJIAZUI
68 Yin Cheng Road Middle
Shanghai 200120 P.R.China
T: +86 21 3135 8666
F: +86 21 3135 8600

BEIJING
4F, China Resources Building
8 Jianguomenbei Avenue
Beijing 100005 P.R.China
T: +86 10 8519 2266
F: +86 10 8519 2929

HONG KONG
27F, Henley Building
5 Queen's Road Central
Central, Hong Kong
T: +852 2969 5300
F: +852 2997 3385

LONDON
1F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

master@llinkslaw.com

Three Dilemmas Inherent in China's Cybersecurity and Data Law

By David Pan

Since the early 2000s, China has gradually adopted a series of laws, regulations and macro policies in the field of cybersecurity and data protection aimed at turning the country into a “cyber superpower” and boosting its digital economy. The China Cybersecurity Law (CSL) which came into effect on June 1, 2017, is a milestone in the development of China's legal framework for cybersecurity and data.

The CSL defines network operators and operations very broadly, and some key terms used in the CSL such as “important data” and “critical information infrastructure (CII)”, are too vague to grasp their precise meaning. Long-awaited supplemental regulations have yet to be published. The broad nature of the areas covered, the vagueness of terminology and uncertainties with implementation have led to an outcry from many multinational companies (MNCs) operating in China, saying that it is impossible to understand the CSL, let alone to comply with it.

Looking deeper into the CSL, it becomes clear that Chinese policymakers are confronted with three dilemmas of conflicting objectives, and are striving to find a balance. That is probably the root cause of the “nebulous” nature of the CSL.

.....
If you would like other Llinks publications, please contact:

Roy Guo: (86 21) 3135 8756
Publication@llinkslaw.com

Llinks Law Offices
www.llinkslaw.com

Three Dilemmas Inherent in China's Cybersecurity and Data Law

Privacy vs. free flow of data

Theft and sale of personal information via the internet has long been rampant in China. To crack down on the abuse of personal information, Chinese legislators decided to take drastic protective measures. First, personal information is defined by the CSL in a wide context, covering both personal identifiable information (information that can be used on its own or with other information to identify a specific individual) and personal identified information (information that is related to an identified individual, such as personal activity information). Following on from the CSL, several judicial interpretations and national standards have further expanded the scope of personal information to include a person's whereabouts, IP address and MAC address (media access control address, a hardware identification number that uniquely identifies each device on a network), IT equipment serial number and more. Secondly, although the CSL categorizes personal information into sensitive and non-sensitive information, express consent from the subject of the personal information is a prerequisite for legitimate collection and use of all types of personal information. Last but certainly not least, China sets quite a low threshold for an offense related to infringement of citizens' personal information. For example, anyone who illegally obtains, sells or provides more than 50 pieces of information on a citizen's whereabouts, communications, credit information or property information, or derives illegal income of more than US\$750 from the abuse of citizens' personal information is guilty of an offense and hence would be subject to imprisonment for up to three years.

The other side of the coin is that strict authorization requirements on the collection and use of personal information could impede the free flow of data. Driven by a huge e-commerce market, China has risen to become the second-largest digital economy. The continuous development of China's digital economy depends largely on the free flow of data and massive data use. The prevailing rule of the "impossible triangle of data transaction and flow" (the "impossible triangle") states that a data law cannot simultaneously achieve the three policy objectives of ensuring strict authorization by data subjects, promotion of massive data flows, and enhancement of data value. In the CSL legislative approval process, some advisors made proposals about the "public" status of personal information, with a view to breaking the "impossible triangle" and loosening the restraints on personal information collection and use. Although these proposals appeared "creative," their workability is doubtful because they contradict the principles underlying Chinese law.

In a nutshell, until Chinese law clearly indicates its priority between privacy protection and free flow of data, we can reasonably foresee that in the course of CSL enforcement, China will tip the scales in favor of either data privacy or free flow of data on a case-by-case basis in light of the actual situation.

Three Dilemmas Inherent in China's Cybersecurity and Data Law

National security vs. cross-border data transfer

The CSL provides that the operator of critical information infrastructure (CII) shall store within Chinese territory personal information and important data collected and generated during its operations within China. According to the CSL, CII encompasses not only traditional critical industries such as public communications, energy, transport and finance, but also other infrastructure that could significantly threaten or harm “national security,” “national economy,” “people’s livelihood” or “public interest” in the event that such infrastructure is damaged, disabled or suffered leakage of data; the CSL defines important data as “data closely related to national security, economic development, and social and public interest.” Such vagueness of terminology has only exacerbated the anxiety of MNCs.

Many MNCs, confused and concerned, complained that the data localization and transfer regulations are “unnecessarily onerous.” In a September 2017 debate at the WTO Services Council, the United States even asked China not to enforce the CSL, claiming that “China’s measures would disrupt, deter, and in many cases, prohibit cross-border transfers of information that are routine in the ordinary course of business.”

It is not unusual that each country competes to keep as much data as possible within its borders because data is the oil of the digital era. For China, there is one more fundamental reason to do so: China, lagging behind in high technology, wants to protect its data from spying by foreign forces. For example, China’s market for automation software is dominated by foreign MNCs. By means of aggregation and algorithms, the operational data of production lines collected by such software can be used to deduce the output and the spread of manufacturing facilities of China’s most important industries. Therefore, without control measures, China is concerned that national security will be threatened or endangered by the free flow of important data abroad.

An anecdote can well demonstrate China’s determination to localize important data. In the second draft of the CSL for discussion, the scope of data subject to local storage requirements included personal information and important business data. Global business groups petitioned China to remove the requirement of data localization. Despite the petition, in the final adopted version, the legislators broadened the data scope to include personal information and important data.

Weighed against its national security concerns, China must consider its commitment to free cross-border data transfers made under WTO rules. Also, China will have to assess whether Chinese companies will face retaliation in data practices in their business operations outside of China if it implements this local data storage policy ruthlessly.

Three Dilemmas Inherent in China's Cybersecurity and Data Law

Big data economy vs. big data monopoly

One of the major objectives of the China cybersecurity and data law is to develop China's big data economy through top-down and state-led efforts. In 2015, China's State Council promulgated the Action Plan for Facilitating Big Data Growth which called for expediting the process of opening and sharing governmental data, and for enhancing the ability of digitized industries to amass and exploit data; CSL also provides that the state encourages the development of technologies for network data protection and use and enhances the availability of public data resources.

Spurred by these incentive policies, the big data-based economy has boomed in China and many unicorns have mushroomed in e-commerce, social media and communications, artificial intelligence, robotics and quantum computing. Against this backdrop, Chinese legislators seemed hesitant to touch on the problem of big data monopoly, a controversial downside of the big data economy. It is probable that the legislators were inclined to believe that a firm cannot gain a sustainable competitive advantage in a data-rich environment simply by amassing big data. Moreover, data-rich companies are not a threat to market competition, but rather are conducive to innovation. Therefore, policymakers should encourage but not limit the data-rich companies.

In reality, however, the danger of big data monopoly looms large in China. On the November 11 (11/11) sales day in 2017, Tmall and Taobao (Alibaba online sales platforms) pressed their contractual online shops to choose either Tmall and Taobao or their competitors for the sales. This act was seen by some as an abuse of Alibaba's dominant position, which would ultimately limit market competition. In August, it was reported that Lianjia and Zillow, one of the largest realtor agencies in Beijing, had monopolized data on apartments available for rent and driven up rental prices in Beijing's market by taking advantage of information asymmetry between them and tenants. Later, after having been castigated by Beijing's city government, Lianjia and Zillow released 80,000 "idle" apartments in an effort to bring down the market rental price.

The existing antitrust laws cannot regulate big data monopoly effectively. Moreover, in practice, the agencies display reluctance in carrying out investigations, even though they have received complaints about suspected acts of abuse of market dominance. Will China's agencies lean toward controlling big data monopolies through law enforcement? Perhaps, but only time will tell.

Conclusion

It was reported that China's top legislative body, the National People's Congress, plans to deliberate and promulgate new laws covering personal information and data protection during its 13th National Congress (2018 - 2023). However, MNCs should not have high expectations of China's cybersecurity and data law becoming

Three Dilemmas Inherent in China's Cybersecurity and Data Law

much clearer as new laws and implemental regulations come into effect. In the legislation and enforcement process, Chinese legislators and law enforcement agencies may continue to act in the spirit of “crossing the river by feeling the stones,” taking a balanced and flexible approach. MNCs should watch for the balances struck by Chinese legislators and agencies from time to time between conflicting policy objectives and make “informed” judgements accordingly.

Want to know more about “personal information” under the CSL? Click "Read more" at the footer to view our view our video interview with David Pan.

Pick up your copy of the November/December issue of Insight magazine at the AmCham Shanghai reception desk or download the PDF version from our publications page.

Three Dilemmas Inherent in China's Cybersecurity and Data Law

Contact Details

If you would like to know more information about the subjects covered in this publication, please feel free to contact the following people or your usual Llinks contact.

Author	
David Pan Tel: +86 21 3135 8701 david.pan@llinkslaw.com	
Shanghai	
David Yu Tel: +86 21 3135 8686 david.yu@llinkslaw.com	Bernie Liu Tel: +86 21 3135 8678 bernie.liu@llinkslaw.com
Selena She Tel: +86 21 3135 8770 selena.she@llinkslaw.com	Nicholas Lou Tel: +86 21 3135 8783 nicholas.lou@llinkslaw.com
Dali Qian Tel: +86 21 3135 8676 dali.qian@llinkslaw.com	Kenneth Kong Tel: +86 21 3135 8777 kenneth.kong@llinkslaw.com
David Wu Tel: +86 21 6043 3711 david.wu@llinkslaw.com	David Pan Tel: +86 21 3135 8701 david.pan@llinkslaw.com
Elyn Jiang Tel: +86 21 6043 3710 elyn.jiang@llinkslaw.com	
Beijing	
David Yu Tel: +86 10 8519 2266 david.yu@llinkslaw.com	Bernie Liu Tel: +86 10 8519 2266 bernie.liu@llinkslaw.com
Yuhua Yang Tel: +86 10 8519 1606 yuhua.yang@llinkslaw.com	
Hong Kong(in Association with Dennis Fong & Co., Solicitors)	
David Yu Tel: +86 21 3135 8686 david.yu@llinkslaw.com	Sandra Lu Tel: +86 21 3135 8776 sandra.lu@llinkslaw.com
London	
Yuhua Yang Tel: +44 (0)20 3283 4337 yuhua.yang@llinkslaw.com	