Cybersecurity review and new ideas for listing in Hong Kong

By Dennis Fong | Xun Yang | Bosco Leung | Jianqi Yang

On the evening of 30 June 2021(Beijing time), Didi was officially listed on the New York Stock Exchange. Two days after Didi's listing, the PRC Cybersecurity Review Office published an announcement regarding the launch of cybersecurity review against Didi (the "**Review Announcement**"), announcing that the review would be conducted according to the *National Security Law of the People's Republic of China* (the "**National Security Law**"), the *Cybersecurity Law of the PRC* and the *Cybersecurity Review Measures* which came into effect on 1 June 2020 ("**Cybersecurity Review Measures**"). The PRC Cybersecurity Review Office also announced that during the cybersecurity review, no new user was allowed to register with the Didi application. On 4 July 2021 and 9 July 2021, Cybersecurity Administration of China ("**CAC**") issued two consecutive circulars, announcing that since Didi Chuxing, Didi Enterprise, and 25 other applications (collectively referred to as "**Didi Apps**") had severe violations of rules against personal data collection, those Didi Apps were required to be removed from app stores. Subsequently, CAC issued the Cybersecurity Review Measures (Revised Draft for Comment) (the "**Revised Draft**") to further clarify the direction for future cybersecurity review. The Revised Draft directly links cybersecurity review with listing in the United States (the "**U.S.**") or other jurisdictions.

We have already briefly discussed the impact of the Revised Draft on the overseas listings. In this article, we will analyze the potential data risks of Didi's listing in the U.S., combine the policy trend of cross-border data governance in U.S. and PRC, make recommendations and conduct analysis on cyber/data security of high-tech companies that would like to list in Hong Kong in light of the cross-border data regulation in the PRC and the U.S.

如果您需要本出版物的中文本,
请联系:

Publication@llinkslaw. com

For more Llinks publications,
please contact:

Publication@llinkslaw.com

1. The Revised Draft substantially addressed the "regulatory requirements" of the securities regulator

Article 6 of the Revised Draft proposes that "Operators holding the personal information of more than 1 million users and new listing on **overseas ("国外" in Chinese)** markets must report for cybersecurity review with the PRC Cybersecurity Review Office". In the context of the review and regulatory action taken by CAC against Didi Apps, the release of the Revised Draft appears to be a piece of "retrospective" legislation enacted by the cybersecurity regulatory bodies to give "legal justification" to the cybersecurity review of the Didi Apps.

In fact, under the current PRC legal framework, both the securities regulator and the cybersecurity regulator have the legal basis to review the overseas listings (particularly in the U.S. capital market) that may give rise to data security issues.

First, Article 15 of the Cybersecurity Review Measures issued by CAC in 2020 provides that "if a network product or service is deemed by the member entities of the working mechanism for cybersecurity reviews to affect or potentially affect national security (of PRC)", a cybersecurity review can be initiated. This constitutes the basis for cybersecurity review conducted by the cybersecurity regulator. The wide application of the Cybersecurity Review Measures obviously does not exclude the scenario where overseas listings which may lead to the disclosure of information to foreign authorities. However, the member entities of the working mechanism listed in the Cybersecurity Review Measures do not include Chinese securities regulatory bodies, therefore, China Securities Regulatory Commission ("**CSRC**") cannot initiate cybersecurity reviews on its initiative. Accordingly, one of the key amendments to the Revised Draft is the inclusion of CSRC into the member entities of the national security review mechanism to ensure its legitimacy in terms of enforcement authority in the future.

Second, CSRC has long been conservative about the provision of data relating to "securities business" due to high sensitivity of its regulatory field. *The Provisions on Strengthening the Confidentiality and Archives Management Works Relating to the Overseas Issuance of Securities and Listing* (Announcement No. 29 [2009]) issued in 2009 by CSRC, among others, stipulates that state secrets cannot be made available to the public during the overseas listing procedures and the working papers of securities business cannot be provided to any overseas parties without the consent of the competent authorities. Article 177 of the *Securities Law of the PRC*, as amended in 2019, further clarifies these requirements by stating that without the consent of CSRC and other competent authorities, no entity or individual shall provide documents and materials related to securities business activities to any overseas parties. In a similar vein, Article 36 of the *Date Security Law of the PRC* enacted on 10 June 2020 specially provides that "without the approval of the competent authority of the PRC, a domestic organization or individual shall not provide data stored within the territory of the PRC to any foreign judicial or legal enforcement authority", which re-emphasizes that securities business information in electronic form shall not be provided to foreign governmental authorities without the approval of the PRC regulatory authorities.

After reviewing and understanding the regulatory history of CAC and CSRC, it is easy to find that the re-emphasized issue of "data security" during the overseas listing procedure of Chinese companies in the Revised Draft is not a completely new legal requirement, but rather a re-enactment of CSRC's constituent legal baseline in the "Global Internet Age". This point can also be found in the "*Opinions on A Strict Crackdown on Illegal Securities Activities in Accordance with PRC Laws*" published by CSRC on 6 July 2021, which emphasizes "further strengthening cooperation in cross-border regulation and enforcement", "improving the laws and regulations relating to data security, cross-border data flow and management of confidential information". On the other hand, as the major responsible authority in the area of network and data security regulation and enforcement, CAC has the authority and obligation to coordinate the cybersecurity work with other different government departments, including CSRC. It is therefore "reasonable and within the law " for CAC to repeatedly emphasize the issue of "data security" in securities business activities in the Revised Draft.

As a data-driven company with more than 100 million registered users, Didi collects and processes a vast amount of personal information on identity, location, and travel records, which requires a high level of security for its data processing activities. Once the information held by Didi is leaked or misused, it can have a negative impact on national security. Therefore, the fact that CAC chose Didi to formally kick off the implementation of China's cybersecurity review system is of great practical value and exemplary effect, regardless of the outcome of the review.

2. The U.S. government has strengthened its verification of the authenticity of data provided by Chinese concept stocks

Corresponding to the Chinese government's strengthening regulation over data provision to overseas parties, the U.S. government has strengthened its verification of the authenticity of data provided by Chinese concept stocks. After stepping into the 21st century, the U.S. capital market, led by Nasdaq, has been a favored destination for Chinese innovative and technology companies due to its relaxed listing conditions, good capital liquidity, and flexible exit mechanism. However, as the number of Chinese companies listed on the U.S. exchanges has increased dramatically, the U.S. Securities and Exchange Commission ("**SEC**") has strengthened its information disclosure requirement for Chinese concept stocks, for example, the Division of Corporation Finance of the SEC published the Disclosure Considerations for China-Based Issuers on 23 November 2020, which addresses the information disclosure issue for China-based issuers to the attention of public investors.

SEC has a long history of imposing a higher standard of disclosure requirements on Chinese concept stocks. Back in the year 2011, when Longtop Financial Technologies was accused of financial fraud, the SEC requested auditing working papers and other documents from Deloitte Shanghai, the firm responsible for the financial auditing of Longtop Financial Technologies. However, Deloitte Shanghai refused to provide the relevant materials due to "restrictions stipulated by Chinese laws", and the SEC filed a subpoena seeking enforcement against Deloitte in the U.S. court. Subsequently, the SEC entered into negotiation with CSRC,

and through a government-to-government negotiation mechanism, CSRC allowed Deloitte's provision of auditing working papers concerning Longtop Financial Technologies.

In recent years, the SEC has kept amending its legislation to solve the potential issue of "financial fraud" (for example, Luckin Coffee was reported by Murky Waters to have 2.2 billion fabricated sales) for U.S.-listed companies and to strengthen its data access authority of Chinese concept stocks. For instance, the *Holding Foreign Companies Accountable Act* (the "**Act**"), an amendment to the 2002 Sarbanes-Oxley Act and the 2010 Dodd-Frank Act, was signed into law on 18 December 2020. According to the Act, the Public Company Accounting Oversight Board ("**PCAOB**") is granted the authority to obtain complete auditing documentation (e.g. auditing working papers) of listing applicants from foreign accounting firms and to impose sanctions on foreign accounting firms that violate relevant requirements. For cases that exclude the authority of PCAOB to inspect the auditing report due to foreign jurisdiction, the "covered issuer" must submit supporting documentation to the SEC to prove that there is no ownership or control of the issuer by any governmental entities under a foreign jurisdiction. Moreover, for those cases, if SEC determines that a covered issuer has 3 consecutive non-inspection years, the SEC has the power to prohibit the securities of the covered issuer from being traded on a national securities exchange of the U.S. or to regulate through any other method that is within the jurisdiction of the SEC. The Act requires additional disclosure from a covered issuer in a non-inspection year, i.e. the covered issuer shall disclose: (a) the name of each official of the Chinese Communist Party who is a member of the board of directors of the issuer or the operating entity concerning the issuer; and (b) whether the articles of incorporation of the issuer (or equivalent organizing document) contains any charter of the Chinese Communist Party, including the text of any such charter. The aforesaid provisions are undoubtedly specific regulatory measures for China-based issuers. China-based issuers in the U.S. stock exchange will be subject to more stringent requirements from the U.S. securities regulators in the future concerning the provision of information and materials of their securities business.

3. Illustration of Article 6 of the Revised Draft and opportunities for listing in Hong Kong

As aforementioned, on the one hand, the Chinese government repeatedly emphasizes its demand for cross-border retrieval restrictions on information and materials concerning securities (such as working papers) and data originating within Chinese borders. On the other hand, U.S. securities regulation institutions establish grave consequences for resisting to provide information about securities practices. Thus, companies wishing to list in the U.S. may face conflicting legal demands under Chinese and U.S. laws in the future.

It is worth mentioning that on 5 July 2021, five days following the Review Announcement, CAC announced its implementation of cybersecurity review on Yunmanman (Full Truck Logistics Information Co., Ltd), Huochebang (Truck Alliance), and Boss Zhipin o. Given that 3 out of the 4 companies under cybersecurity review belong to 'transportation' companies, this may reflect CAC's particular concern over the cybersecurity issues of these types of Internet companies. Without doubt, these regulatory signals triggered concerns for 'transportation' companies, for instance, according to media coverage, the online vehicle-hailing platform Huolala is considering changing their IPO destination from New York City to Hong Kong at

the moment after submitting their IPO application documents to the U.S, in order to avoid a prolonged IPO process.

Although Huolala has not officially provided a direct reply, Article 6 of the Revised Draft stipulates that 'Operators holding the personal information of more than 1 million users and new listing on **overseas** ("国外" in Chinese) markets must report for cybersecurity review with the Cybersecurity Review Office'. The term '**overseas**' is used, instead of the more common legal term 'abroad'("境外" in Chinese), which may reflect a relatively more lenient attitude on the"cyber & data security" issue for Chinese companies which wish to list on exchanges in Hong Kong from CSRC's perspective. In fact, according to Article 89 of the *Exit and Entry Administration Law of the PRC*, departure from Mainland China towards the Hong Kong Special Administrative Region is defined as 'exit'. It is thus certain that the term 'abroad' must include Hong Kong, Macau, and Taiwan regions. Even though the term '**overseas**', is in want of a clear definition in legal documents, according to general understanding, terms like 'overseas' and 'domestic' involve the setting of national borders so that it is under the umbrella of the concept of sovereignty. Hong Kong is certainly included within the sovereign borders of the PRC. Thus, we believe that the application for inspection requirements for 'overseas listed' companies in the Revised Draft may provide an 'exemption policy' for Mainland companies which list in Hong Kong.

The Financial Secretary of Hong Kong, Mr. Paul Chan Mo-po has pointed out during an interview recently that Hong Hong, as part of this country, does not have a cyber security problem and that, if technology companies in the Mainland select to go listed in Hong Kong, they will not face unpredictable enforcement actions, which concern the strained relationship between the US and China and even involving Hong Kong. This affirms our conclusion that, from a cyber security aspect, it would be an option worthy consideration for technology companies to opt for listing in the Hong Kong market.

Additionally, the performance of Chinese technology companies in the Hong Kong Stock Exchange is eye-catching, which reflects the preference on technology and innovation business of investors in the Hong Kong market. Therefore, for Chinese new-economy companies that wish to alter their listing plans due to the recent announcement of the Revised Draft or CSRC stipulations, listing in Hong Kong may be an appropriate choice.

If you would like to know more information about the subjects covered in this publication, please contact:

Dennis Fong
+852 2592 1910
dennis.fong@llinkslaw.com.hk

Xun Yang
+86 21 3135 8799
xun.yang@llinkslaw.com

Bosco Leung
+852 2592 1983
bosco.leung@llinkslaw.com.hk

SHANGHAI

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

SHENZHEN

18F, China Resources Tower
2666 Keyuan South Road, Nanshan District
Shenzhen 518063 P.R.China
T: +86 755 3391 7666
F: +86 755 3391 7668

HONG KONG

Room 3201, 32/F, Alexandra House
18 Chater Road
Central, Hong Kong
T: +852 2592 1978
F: +852 2868 0883

LONDON

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

www.llinkslaw.com

Wechat: LlinksLaw

WE LINK LOCAL LEGAL INTELLIGENCE WITH THE WORLD