WILMERHALE

China Tightens Control Over Overseas Securities Listings in Name of Data Security

July 12, 2021

On July 6, the General Office of the Central Committee of China's Communist Party and the General Office of the State Council jointly issued the Opinions on Strictly Cracking Down on Illegal Securities-related Activity in Accordance with Law (the Opinions) to further strengthen regulatory supervision of securities-related activity, including enforcement with respect to overseas listings of China Concepts Stock (CCS) by enhancing data security protection.[1] CCS generally refers to companies which conduct overseas listings with assets and/or earnings primarily based or originating in China.

The Opinions were issued amidst probes into several Chinese internet platform companies by several government departments, including in this instance the increasingly powerful Cyberspace Administration of China (CAC) regarding data security with its implications for national security as well as privacy concerns. Such concerns are in part responses to more insistent demands by overseas regulators, particularly in the US, for transparency by CCS companies, including access to audit working papers.

On July 10, CAC released the draft revision of the Cybersecurity Review Measures (Draft Revision) with comments due by July 25, half the typical 30 days reflecting the urgency of the matter.[2] The Cybersecurity Review Measures which were invoked by CAC as the basis for the probes into the platform companies are themselves relatively new and only came into effect on June 1, 2020. The Draft Revision would require Chinese companies which process personal information[3] of more than

[1] http://www.gov.cn/zhengce/2021-07/06/content_5622763.htm
[2] http://www.cac.gov.cn/2021-07/10/c_1627503724456684.htm
[3] Personal information is defined in Article 76(5) of Cybersecurity Law as various information which is recorded in electronic or any other form and used alone or in combination with other information to recognize the identity of a natural person, including but not limited to name, date of birth, ID number, personal biological identification information, address and telephone number of natural persons.

1 Million users to apply for a mandatory cybersecurity review before conducting an overseas IPO to examine the risks of critical information infrastructure (CII)[4] and important data[5] being maliciously exploited by overseas governments, among other concerns. The 1 Million users threshold is likely to be meaningless as the prospects for a Chinese company to conduct an overseas IPO when the number of its domestic users is less than 0.1% of the population are very limited.

This alert focuses on (i) the current status of cybersecurity investigations into CCS companies recently listed in the US; (ii) the requirements under the Opinions and Draft Revision to tighten data security on offshore securities listings; and (iii) compliance issues confronting CCS companies with respect to data security, cross-border data transfer and privacy protection.

i. Heightened Cybersecurity Review over CCS Companies

On July 2, CAC's Cybersecurity Review Office launched a cybersecurity investigation into Didi Chuxing, the country's largest ride-hailing service, which conducted an ADR listing (NYSE: DIDI) on June 30.[6] On July 4, CAC announced that Didi Chuxing had seriously violated regulations regarding the collection and use of personal information, and ordered removal of its app from all app stores.[7]

The next day, July 5, CAC announced similar cybersecurity investigations into Yunmanman, Huochebang, and Boss Zhipin.[8] Yunmanman and Huochebang are China's two leading truck-hailing apps who label themselves as "Uber for trucks" and which merged into a new company called Full Truck Alliance Co. which conducted an ADR listing (NYSE: YMM) on June 22. Boss Zhipin Inc., one of China's largest online job recruiting platforms, listed in the US (NYSE: BZ) on June 11. CAC, not the China Securities Regulatory Commission (CSRC) or any of China's other financial or foreign exchange regulators, ordered all three platforms to stop registering new users and remove their apps from online stores, stalling their growth and resulting in falling market valuations. All three of these listing vehicles were established as Variable Interest Entities (VIEs)

---

[4] Article 31 of the Cybersecurity Law provides a non-exhaustive list of selected critical industries and areas whose information infrastructure would be regarded as CII, including public communications, information services, energy, transport, water conservancy, finance, public services, and e-governance, and more broadly, other information infrastructure which may cause serious consequences if it suffers any damage, loss of function, or leakage of data. The specific scope of CII has yet to be specified by State Council.

[5] Important data is not defined in the Cybersecurity Law or the Data Security Law, but is defined in the draft Data Security Management Measures (2019) as data which, if disclosed, may affect national security, economic security, social stability or public health and safety, such as undisclosed government information, information relating to large-scale population, population genetics and health, geography and mineral resources. Important data generally does not include information relating to the operation, production or internal management of enterprises, or personal information.

[6] http://www.cac.gov.cn/2021-07/02/c_1626811521011934.htm

[7] http://www.cac.gov.cn/2021-07/04/c_1627016782176163.htm

[8] http://www.cac.gov.cn/2021-07/05/c_1627071328950274.htm

registered in offshore jurisdictions to enable them to raise capital overseas while maintaining ownership of their onshore licenses which are restricted to domestic parties.

CAC's announcement of investigations invoked the protection of data security and national security as the purpose for the probes, citing as authority the Cybersecurity Review Measures,[9] National Security Law (effective July 1, 2015)[10] and Cybersecurity Law (effective June 1, 2017).[11]

The Cybersecurity Review Measures are initially intended to safeguard supply chain security among CII operators (CIIOs) by requiring that CIIOs undergo a cybersecurity review when procuring network products and services that may affect national security. Article 9 of the Measures includes the risk of important data leakage among the concerns of required security assessments. Such risks include (a) *leakage of sensitive data* – the leakage of undisclosed government information, large-scale population, genetic health, or geographic data which may directly affect economic security, social stability, or public health and safety; and (b) *misuse of sensitive data* -- network product and service providers may collect large volumes of supply information and user information, especially when used by CIIOs. National security and the public interest may be threatened if big data technology is abused to analyze and mine large volumes of sensitive data for arbitrary sharing and publication.[12]

The above three internet platform companies currently under investigation are leading platforms in their respective fields of daily movement, online freight, and public job hunting which possess massive volumes of in-depth data in their respective industries. Such data may directly or indirectly reveal population distribution, commercial activity, population flows, commodity flows, and business operations across China, potentially constituting sensitive data or important data (two terms which have yet to be clearly defined in law and therefore are subject to expansive construction in a country hypersensitive to security), the leakage and abuse of which may be deemed to impair national security.

As discussed in Section (iii) below, the Cybersecurity Law imposes data localization requirements on CIIOs to store personal information and important data within China. The Data Security Law (effective September 1, 2021)[13] and draft Personal Information Protection Law[14] will require data processors to take specific compliance measures, including a CAC-led security assessment, in order to transfer important data and personal information overseas. Under the Data Security Law and the Securities Law (effective March 1, 2020),[15] Chinese government approval must be

---

[9] http://www.cac.gov.cn/2020-04/27/c_1589535450769077.htm

[10] http://www.gov.cn/zhengce/2015-07/01/content_2893902.htm

[11] http://www.cac.gov.cn/2016-11/07/c_1119867116.htm

[12] Expert interpretation -- Hu Ying: Supply chain security risk analysis from the perspective of cybersecurity review, May 4, 2020, http://www.cac.gov.cn/2020-05/03/c_1590051734465847.htm

[13] http://www.cac.gov.cn/2021-06/11/c_1624994566919140.htm

[14] https://www.chainnews.com/articles/762892395785.htm

[15] http://www.mofcom.gov.cn/article/swfg/swfgbl/201101/20110107349287.shtml

obtained before handing over data in response to requests from overseas law enforcement agencies, which affects the already limited prospects for mutual legal assistance and cross-border regulatory cooperation.

Such data localization requirements and cross-border data transmission restrictions create tensions over data sovereignty when CCS companies list overseas and subject themselves to foreign securities regulatory requirements.

CCS companies listed in the US may be forced to reveal audit papers that contain sensitive information on operations in order to comply with US accounting standards or risk being delisted. The interim final rule of the Holding Foreign Companies Accountable Act (effective May 5, 2021) directs the US Securities and Exchange Commission (SEC) to prohibit exchanges in the US from trading the securities of certain identified foreign issuers whose financial statements have not been audited by accounting firms subject to inspection by the Public Company Accounting Oversight Board for three consecutive years.

As the Cybersecurity Law imposes data localization requirements on CIIOs, and the Data Security Law and draft Personal Information Protection Law have yet to take effect, the Cybersecurity Review Measures were invoked by the CAC to prevent such newly listed CCS companies from handing over important or sensitive data to the SEC without having to prove that such platforms are CIIOs with access to important data. Didi Chuxing reportedly was warned not to proceed with its IPO but did so anyway, and the stock prices of all three of these platform companies as well as other CSC companies have fallen.[16]

ii. Call for Enhanced Regulations on Overseas Listing

The Opinions call for further strengthening supervision and enforcement of cross-border listings. Specifically, the Opinions call for the relevant authorities to improve laws and regulations in such areas as data security, cross-border data flows, and confidential information management; accelerate amendment of regulations on strengthening confidentiality and file management work related to the issuance of securities and overseas listings; deepening cross-border audit supervision cooperation in accordance with the principles of law and reciprocity; strengthening supervision over CCS; and establishing and improving the extraterritorial application of capital markets law.

Although the high-level Opinions are thin in detail, the rules applicable to overseas listings of CCS companies will soon be revised to reflect enhanced data security and other concerns, which will likely affect older CCS companies as well as future listings. Note that work papers generated by

[16] L. Wei and K. Zhai, Chinese Regulators Suggested Didi Delay Its U.S. IPO, July 5, 2021, https://www.wsj.com/articles/chinese-regulators-suggested-didi-delay-its-u-s-ipo-11625510600?mod=hp_lead_pos1

underwriters and other securities services firms in China for overseas listing of CCS companies are in principle required to be stored in China pursuant to certain regulations jointly promulgated by CSRC and several State Council departments in 2009.[17]

As discussed above, the Draft Revision of the Cybersecurity Review Measures would require operators (*not just CIIOs*) that possess personal information of more than 1 Million users to apply for a mandatory cybersecurity review with the CAC before listing overseas (Article 6). The Draft Revision would also include an overseas listing among the keyes for cybersecurity review and would require that cybersecurity review consider the risks of CII, core data (*a term that is undefined*), important data and massive personal information being influenced, controlled or maliciously exploited by a foreign government following the overseas listing of a Chinese company (Article 10(5)). Such provisions, if promulgated in their current form, would potentially subject all Chinese companies, not just a few CIIOs, contemplating overseas listings that process massive personal information, core data or important data to cybersecurity review.

While the new regulatory requirements do not directly address VIE structures employed by Chinese companies to attract foreign capital through offshore holding companies while satisfying domestic licensing requirements through onshore companies, VIEs may also encounter more stringent scrutiny with respect to cybersecurity, including with respect to the transfer of data overseas by the onshore companies. There may also be rules requiring VIE structures to obtain approval from the CSRC before listing overseas. For listed companies, approval may be required for additional stock issuance or stock placements. Such constraints could affect the valuations of VIEs even though Chinese regulators like the State Administration for Market Regulation have begun to acknowledge the legitimacy of VIE structures with respect to merger reviews and other matters.

iii. Compliance Issues Facing Platform Companies

The laws most relevant to platform companies with overseas listings regarding data security, privacy protection and cross-border data transmission are the Cybersecurity Law, Data Security Law, and draft Personal Information Protection Law.

As discussed above in Section (i), the Cybersecurity Law imposes requirements on CIIOs to store personal information and important data in China, and if a CIIO determines that it is necessary to transfer personal information or important data overseas, it must first conduct a data security assessment. The Data Security Law goes further by requiring data processors other than CIIOs to follow relevant rules to be formulated by CAC and other government authorities when transferring important data collected and generated in China overseas (Article 31). The regulations and guidelines for such transfers are still evolving, especially rules governing specific industries, i.e., not just platform companies. Notably, there is still a lack of clear definition of what constitutes

[17] Regulations on Strengthening the Administration of Confidential Archive Relating to Overseas Securities Offering and Listing, http://www.gov.cn/gongbao/content/2010/content_1620613.htm

“important data” which creates great uncertainty regarding when a data security assessment must be conducted and what it must cover.

Article 36 of the Data Security Law and Article 41 of the draft Personal Information Protection Law provide similar prohibitions on Chinese parties submitting data or personal information stored in China at the request of overseas judicial or law enforcement agencies without Chinese government approval.

The draft Personal Information Protection Law would provide that a data processor before transferring personal information overseas needs to obtain a stand-alone consent from the individual (Article 39), conduct an internal risk assessment and retain records of such transfers (Article 55), and choose one of the four mechanisms for the required assessment: (a) undergoing a CAC-administered security assessment; (b) obtaining certification from a professional institution accredited in accordance with CAC requirements; (c) entering into a standard transfer agreement with the overseas recipient; or (d) other mechanisms as stipulated in laws and regulations (Article 38).

Most significantly, Article 57 of the draft Personal Information Protection Law would impose the following obligations on basic internet platform service providers which have a significant number of users and operate complex types of businesses when processing personal information to (a) establish an independent organization largely comprised of external personnel to supervise the personal information processing activities; (b) cease to provide services to products or services providers on the platform which have seriously violated laws and regulations regarding personal information processing; and (c) periodically publish personal information protection social responsibility reports.

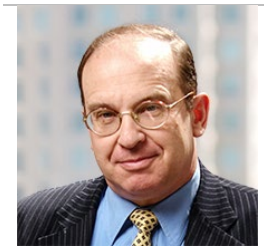
An entity which illegally transfers important data overseas may incur a fine up to RMB 10 Million and/or face suspension of its business or revocation of business permits or licenses in serious cases, with persons directly responsible facing a fine up to RMB 1 Million. Entities which provide data to overseas judicial and law enforcement agencies without authorization may incur penalties of up to RMB 5 Million and face suspension of business or revocation of business licenses or permits in serious cases, and personnel in charge who are directly responsible for the provision, and other directly responsible personnel, may incur fines of up to RMB 500,000. Entities which improperly process personal information may incur penalties of up RMB 50 Million or 5% of revenue in the previous year, and/or face suspension or cessation of its business, with persons directly responsible facing a fine of between RMB 100,000 and RMB 1 Million. Criminal charges may be brought in cases of severe violations.

Conclusion

The Opinions call for heightened scrutiny on data security when regulating CCS companies listing abroad. China will likely impose more stringent restrictions on cross-border data transfers by companies listed and to be listed overseas even when such data transfers are required by the applicable overseas listing rules, making such companies face an inherent dilemma created by conflicting compliance rules in different jurisdictions. Potential rule changes affecting VIEs may also cause CCS companies to think twice when choosing between listing overseas and listing in China.

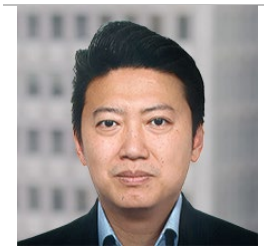
Conversely, although "overseas" under Chinese law is generally defined to encompass Hong Kong and Macao given their status as Special Administrative Regions, the central government's rapidly expanding security control over such regions indicates that the CAC and other authorities will feel more comfortable about CCS companies listing in Hong Kong rather than the United States or other jurisdictions. If so, the future path for Chinese companies raising capital in overseas securities markets may lead to Hong Kong rather than New York, London or elsewhere.

Contributors



Lester Ross
PARTNER

Lester.Ross@wilmerhale.com
+ 86 10 5901 6588



Kenneth Zhou
PARTNER

Kenneth.Zhou@wilmerhale.com
+ 86 10 5901 6588

Tingting Liu
COUNSEL

Tingting.Liu@wilmerhale.com
+ 86 10 5901 6588