AIPLA
American Intellectual Property Law Association

July 12, 2019

国家互联网信息办公室网络安全协调局
北京市西城区车公庄大街11号
邮编100044

National Internet Information Office Cyber Security Coordination Bureau
11 Chegongzhuang Street
Xicheng District
Beijing 100044
CHINA

via email (shencha@cac.gov.cn)

Re: Comments on Draft Measures on Security Assessment of the Cross-Border Transfer of Personal Information Of The People's Republic of China ("个人信息出境安全评估办法征求意见")

Dear Sir or Madam,

The American Intellectual Property Law Association (AIPLA) appreciates the opportunity to comment on draft Measures on Security Assessment of the Cross-Border Transfer of Personal Information ("Draft Measures"), published on June 13, 2019.[1]

AIPLA is a national bar association of approximately 13,500 members engaged in private or corporate practice, in government service, and in the academic community. AIPLA members represent a wide and diverse spectrum of individuals, companies, and institutions involved directly or indirectly in the practice of patent, trademark, copyright, trade secret, and unfair competition law, as well as other fields of law affecting intellectual property. Our members represent both owners and users of intellectual property. Our mission includes helping establish and maintain fair and effective laws and policies that stimulate and reward invention while balancing the public's interest in healthy competition, reasonable costs, and basic fairness.

[1] Original text available at: http://www.gov.cn/xinwen/2019-06/13/content_5399812.htm. AIPLA obtained an unofficial English translation to review the Draft Measures.

Due to time constraints, AIPLA focused its comments on specific articles of the Draft Measures identified below. The absence of comments on other articles does not necessarily reflect support or lack of support of these articles by AIPLA.

The Draft Measures on Security Assessment of the Cross–Border Transfer of Personal Information raise a number of concerns. AIPLA commends the People's Republic of China for proposing measures to protect the privacy of personal information in cross-border transfers. However, in general, the Proposed Measures go much farther than other generally-accepted international norms of protection of this type of personal information; they would likely impose undue administrative burdens and substantial risk of the exposure of confidential information on multinational companies operating in China as well as on Chinese entities.

Article 2 would apply to all Network Operators who transfer personal information collected in the course of operation within the territory of the PRC to another country. It would require that they perform a security assessment and that, if the transfer may "endanger national security interests, damage public interest, or does not adequately protect personal information security," then the information shall not be transferred abroad. This provision does not provide clear definitions of when a proposed information transfer may allegedly endanger national security, damage public interest, or not adequately protect personal information. No standards are provided for any of these criteria. Nor does the provision appear to be directed at preserving the privacy of personal information.

Article 3 would require the Network Operator to report to provincial cyber security administrations, rather than a national cyber security administration, before any cross-border transfer occurs. The provision also would require separate security assessments for each Recipient. These requirements will likely pose an undue burden not only on multinational corporations operating in China but also on Chinese entities.

Article 4 would require that certain information be provided in conjunction with a personal information security assessment, namely contracts, security reports, and other materials, any of which would likely contain information that is proprietary, confidential, or constitutes trade secrets of the Network Operator, the entity using the Network Operator's service, or of the Recipient. This provision also appears to be much broader than necessary for protecting the privacy of personal information. AIPLA requests clarification regarding the scope of Article 4(4) so that it is not fully open ended. One point of particular concern is that this Article 4, and all Draft Measures in general, be amended so they clearly do not require Network Operators or Recipients to provide any personal information collected by the Network Operator of an individual (such individual hereinafter referred to as "Subject") to the provincial or national cyber security administration. Such clarification would also be in accord with the spirit to provide adequate assurances that personal data is protected as set out in other cybersecurity laws, e.g., European Union's GDPR Article 45.

Article 5 would allow experts or technical professionals retained by provincial cybersecurity administrations to access these materials to conduct security assessments. The provision contains no provisions providing for the security of confidential, trade secret, or otherwise proprietary information that may belong to the Subject of the personal information, the

Recipient, or the Network Operator. Nor is it directed to maintaining the privacy of personal information. Rather, the proposed measures appear to provide that both the provincial authority and the national cyber security authority have the right to inspect all such information regardless of its status as proprietary, confidential, trade secret, or personal information. This may expose sensitive information or allow it to be used for other purposes. AIPLA recommends that the Draft Measures expressly require that any such confidential, proprietary, trade secret, or personal information be maintained in strict confidence and be used only for purposes of legitimate security assessments to ensure the privacy of personal information, and for no other purpose. The materials should not be disclosed to any third person including, without limitation, experts or technical professionals or persons affiliated with competitors.

Article 6 would require that the security assessment focus on certain specific aspects. Many of these appear to be appropriate to ensuring confidentiality of personal information. Nonetheless, the provision identifies "other aspects that shall be evaluated." This fails to provide adequate guidance regarding what information will be used in making the assessment and poses a further risk that proprietary, confidential, trade secret, or personal information will be exposed to third parties, or released, or used for purposes other than ensuring the security of personal information.

Article 7 would require that the provincial cyber security administration report the security assessment to the national cyber security administration. AIPLA appreciates that this division of labor may be appropriate or even necessary. However, given the likelihood that confidential, proprietary, trade secret, or personal information will be involved in these security assessments, reliance on provincial authorities unnecessarily exposes potentially sensitive information to abuse or misuse, or at least complicates maintaining the security of this information. Designation of a single national authority whose authority is clearly limited to the purpose of ensuring security of personal information may mitigate these risks.

Article 8 would require a Network Operator to record cross-border transfers of information and retain this information for at least five years, including certain specified records. AIPLA anticipates that the volume of cross-border personal information transferred would be substantial. This reporting requirement alone would likely impose an undue administrative burden not only on multinational corporations involved in cross-border personal information transfer but also on Chinese entities operating such networks.

Article 9 would require reporting of contracts. This too would appear to impose an undue administrative burden on the parties involved.

Article 10 would permit the provisional cyber security administrations to regularly organize inspections to examine records. No reasonable limitations are provided on the frequency and intensity of these inspections. This provision would likely result in an undue burden on Network Operators covered by the measures.

Article 11 would permit cyber security administrations to suspend or terminate cross-border transfers based on certain criteria, including where the following occur: major incidents where personal information has been divulged or abused; Subjects cannot protect their legal rights; or

the Network Operator or Recipient is incapable of protecting personal information. AIPLA is concerned that these criteria are so broad that they do not provide reasonable guidance to Network Operators.

Article 12 would permit any person to report any violation of these measures. This could provide opportunities for harassment of Network Operators based on frivolous complaints or complaints that are not well-founded. The measures provide no substantive requirements for filing a complaint.

Article 13 specifies the content of the contract. These provisions generally appear to be reasonable and, in particular, obligations that the contract cannot exempt the Network Operator from the draft security measures appear reasonable, provided the security measures themselves are reasonable.

Article 14 identifies certain obligations that the Network Operator shall assume. These appear reasonable, provided the obligations on the Network Operator are sufficiently clear and reasonable. However, Article 14 (2) of the Draft Measures, would require the Network Operator to provide Subjects, upon request, a copy of contracts that the Network Operator has with the Recipient. AIPLA believes that such contracts will likely include confidential information, including trade secrets, and will be unnecessary for the needs of the Subject since adequate transparency and redress for misuse are provided elsewhere in the Draft Measures. AIPLA respectfully suggests that Article 14(2) be omitted form the Draft Measures.

Article 15 provides that the Recipient shall assume specific responsibilities and obligations. As the Recipients are located in foreign countries, many of these obligations are unreasonable and would likely be unduly burdensome. These include providing access to unidentified third parties to the personal information and requiring that the personal information not be retained beyond the period provided in the contract. Moreover, Recipients may not be subject to proper jurisdiction for these requirements and these requirements may conflict with the requirements of the laws of the country in which the Recipient is located.

Article 16 provides that the Recipient shall not transmit the received information to third parties unless certain conditions are satisfied. These conditions appear to be reasonable. Nonetheless, certain of the conditions are not adequately defined to give clear notice regarding their scope, including liability for compensation to be paid where transmission to a third-party causes abuse of the legal rights and interest of the Subject of the personal information.

Article 17 provides that reports of the Network Operator shall include certain specific information. This information appears to be highly invasive, including "financial details, and reputation and network security capabilities of Network Operator and Recipient." This information may readily be subject to abuse and many Network Operators and Recipients will consider this information to be confidential, proprietary, or trade secret information. Moreover, to the extent the measures might require Network Operators or Recipients to reveal potential vulnerabilities, the measures could increase the risk of a breach rather than preserving the security of the Subject's personal information.

Article 19 addresses situations in which China is a party to or has concluded agreements with other countries, regions or international organizations governing cross-border transfer of personal information. AIPLA commends these provisions. However, the provision is not clear about what controls in the event of a conflict. AIPLA recommends that the measure be modified to specify that in the event of a conflict between the provisions that have been agreed upon and the draft measures, the internationally agreed-upon provisions shall control.

Article 20 addresses the collection of personal information of domestic Chinese users and extends the obligations to foreign parties to comply with these measures through a legal representative or entity within the territory. In principle, AIPLA concedes this as a valid goal. In practice, however, this provision could be interpreted to give extraterritorial effect to Chinese law and impose substantial and unduly burdensome obligations on entities located outside of the jurisdiction of the People's Republic of China. (Please also refer to the comment on Article 4 concerning Subject's Personal Information. Clarification that transfer of the Subject's personal information to a Cybersecurity Administration would not be required also accords with the spirit to provide adequate assurances that personal data is protected as set out in other cybersecurity laws, e.g., European Union's GDPR Article 45.)

Article 21 provides certain definitions for the Draft Measures. "Network Operators," are defined as referring to the owners and administrators of a network, as well as network service providers. AIPLA respectfully requests clarification of the scope that would be included within this definition. Does this definition apply to public networks only? Or, would any corporation or organization having a limited-access internal corporate network be considered a "Network Operator"? AIPLA respectfully suggests that clarification be provided that such internal networks be excluded from the regulation. AIPLA further requests clarification of any intended extra-territorial impact of the "Network Operator" definition.

We appreciate the opportunity to provide these comments on the Draft Measures on Security Assessment of the Cross-border Transfer of Personal Information, and we would be happy to answer any questions that our comments may raise.

Sincerely,

Sheldon H. Klein
President
American Intellectual Property Law Association