WORLD TRADE ORGANIZATION

S/C/W/374

26 September 2017

(17-5101)

Page: 1/2

Council for Trade in Services

Original: English

COMMUNICATION FROM THE UNITED STATES

MEASURES ADOPTED AND UNDER DEVELOPMENT BY CHINA RELATING TO ITS CYBERSECURITY LAW

The following communication, dated 25 September 2017, from the delegation of the United States is being circulated to the Members of the Council for Trade in Services.

---

1. The United States requested the inclusion of this topic on the agenda for the Council for Trade in Services in order to express its concerns with certain measures China has adopted, and related implementing measures under development, that could significantly impair cross-border transfers of information. This is one key aspect of U.S. concerns regarding China's Cybersecurity Law and related measures. If these measures enter into full force in their current form, they could have a significant adverse effect on trade in services, including services supplied through a commercial presence and on a cross-border basis. We are bringing this matter before this Council because the potential effects extend across all service sectors and have bearing on the rights of other Members.

2. The measures of concern include: The Cybersecurity Law, adopted in November 2016 and taking effect June 2017; and various implementing measures connected with the Cybersecurity Law and China's National Security Law (adopted in July 2015), including the "Measures on the Security Assessment of Cross-Border Transfer of Personal Information and Important Data" and the "Draft National Standard – Information Security Technology – Guidelines for Data Cross-border Transfer Security Assessment."

3. 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. More specifically:

a. The measures would apply to "network operators," which could encompass any foreign service supplier that has a website or uses the Internet to communicate with customers, suppliers, or affiliates. Such a broad definition means that the measures could have a negative impact on a wide range foreign companies.

b. The measures, which pertain to "important data"[1] and "personal information," would severely restrict cross-border transfers unless a broad set of burdensome conditions are met. These conditions would restrict even routine transfers of information, fundamental to any modern business. They include: (a) that the network operator (or in certain cases, a governmental authority) has performed a "security assessment;" (b) that the purpose of the transfer meets standards of legitimacy, necessity, and justification; and (c) that purported risks, including to national security, social and public interests, and lawful interests of individuals, are mitigated. As one aspect of our concerns, a need to demonstrate the necessity of transfers is very troubling, since it impinges on commercial

[1] Important data is defined as "data closely related to national security, economic development and societal and public interests." The Draft Guidelines provide broad descriptions of data that can fall within this definition and lists 27 sectors, including "Communications" and "Electronics and Information," as well as "Steel" and "Food and Drugs." There is also a 28th "Miscellaneous" category that includes inter alia any sector "closely linked with national security and social public interests." This definition is so broad that it could apply to any and all data.

choices and longstanding business arrangements supported by robust trade rules, and many common transactions would not appear to meet the criteria set out.

c. With respect to "personal information," in addition to the conditions already described, a "network operator" would appear to be required to obtain consent from each individual before any cross-border transfer can take place. This is an extraordinarily burdensome requirement that could disrupt business operations without contributing to privacy protections. Many less burdensome options exist to achieve privacy objectives, including compliance with international cross-border privacy frameworks, such as the APEC Cross-Border Privacy Rules System endorsed by China; contractual agreements between network operators and third party recipients; and third-party accreditation.

d. In some circumstances, the outcome of the security assessment would result in an outright prohibition on cross-border data transfers. These circumstances are so broadly and vaguely defined – including when transfers would pose a risk to "national security," "economic development," and "social public interests," and when such transfer may be detrimental to public and national interests – that they could cover a nearly unlimited range of transactions.

e. The measures would impose local data storage requirements on operators in "critical information infrastructure sectors," which the Cybersecurity Law defines in broad and vague terms. Cross-border transfers of data by these operators would be subject to review by China's competent regulatory authorities. Such requirements would inevitably impede cross-border information flows and disrupt normal business operations.

4. Thus, the measures would impose special scrutiny, particular procedures, or bans on the cross-border transfer of expansive and loosely-defined categories of data. The result would be to discourage cross-border data transfers and to promote domestic processing and storage. The impact of the measures would fall disproportionately on foreign service suppliers operating in China, as these suppliers must routinely transfer data back to headquarters and other affiliates. Companies located outside of China supplying services on a cross-border basis would be severely affected, as they must depend on access to data from their customers in China.

5. In this regard, we note that China has undertaken market access and national treatment commitments under the General Agreement on Trade in Services for many services that would be affected by these measures. In addition, China's cross-border commitments apply to a broad range of sectors – from accounting to financial data processing to travel services. None of these cross-border services is feasible without accessing data from China, much of which would appear to fall within the scope of the restricted or banned categories.

6. The United States has been communicating these concerns directly to high level officials and relevant authorities in China. We are bringing the matter to this forum in order to raise awareness among other Members of the nature of the pending measures and their potential impact on trade. We request that China refrain from issuing or implementing final measures until such concerns are addressed. We will keep the Council informed of any further developments on this matter.