



23 February 2018

(18-1181)

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 23 February 2018, from the delegation of the United States is being circulated to the Members of the Council for Trade in Services.

1. On 26 September 2017, the United States submitted a communication (S/C/W/374) to the Council for Trade in Services (CTS) expressing concerns with certain measures China has adopted, and with related implementing measures under development, that could significantly impair cross-border transfers of information. The United States brought this matter before the Council because the potential effects extend across all service sectors and have bearing on the rights of other Members. During the CTS meeting held on 6 October, a number of other WTO Members also expressed a high degree of concern regarding China's existing and proposed regime regarding cross-border transfers of data, including application of proposed restrictions on so called "important data" and on "personal information."

2. As reported in September, the United States has communicated its concerns directly to high-level officials and relevant authorities in China and requested that China refrain from issuing or implementing final measures until such concerns are addressed. At the 6 October CTS meeting, a number of other WTO Members also asked China not to move forward with any measures until and unless key concerns had been addressed. At that CTS meeting, China noted that it was still open to receiving input from Members but otherwise did not provide meaningful feedback on the issues raised. Since then, China has not provided any assurance that it will resolve these concerns.

3. Within the US (and foreign) business community, the level of concern about the direction of China's policies remains high. US industry is particularly concerned that the measures contemplated by China would disrupt communications between a company's China facilities and its other global operations, increase costs, and reduce rather than enhance data security. Industry has emphasized, and we concur, that there are other, more effective ways of achieving legitimate policy objectives without disrupting commercial operations and that global best practices provide a clear way forward.

4. In a separate but related troubling development, China has recently issued a Circular entitled "Cleaning up and Regulating the Internet Access Service Market"¹ (set to enter into force on 31 March 2018) that would seem to impose new restrictions on the use of virtual private networks (VPNs) and leased lines.² This Circular raises numerous concerns and would add to the burdens and restrictions that China's implementation of its Cybersecurity Law would place on cross-border transfers of information.

¹ G.X.B.X.G.H. No.[2017] 32, issued 17 January 2017, by the Ministry of Industry and Information Technology.

² Leased lines and VPN services are specialized services companies use for critical communications for either intra-corporate communications or communications with customers or suppliers. Leased lines rely on a dedicated circuit for exclusive use of a customer; VPN services use encryption to create a "virtual" dedicated channel for the same purpose.

5. In particular, the Circular would restrict cross-border information transfers through leased lines and VPNs to information used "exclusively for internal office purposes." The Circular would expressly prohibit the use of leased lines and VPNs "for connecting domestic and foreign data centers" or to enable "business platforms to provide telecommunications services." The potential impact of the Circular both on foreign service suppliers and their customers in China appears to be quite severe. Leased lines and VPNs are commonly used to ensure the security and confidentiality of information transferred into and out of a country in the course of supplying services. For example, to the extent that it relied on such services, how might a travel agent based in China access international flight information without connecting to a foreign data center? How could data processing or accounting services be supplied on a cross-border basis to Chinese clients/customers without some connection to a foreign data center? As another key example, many software platforms enable text messaging for technical support and customer service purposes – how would an online "chat" between a foreign accounting firm and its client in China, provided over a VPN or leased line be treated for the purpose of the Circular?

6. The Circular, as with China's proposed regime relating to cross-border transfer of information, would appear to create significant new constraints on market access opportunities for cross-border service suppliers. The range of "data centers" and "business platforms" that could be subject to this prohibition is large, potentially encompassing any service that is beyond what might be used to facilitate a company's internal communications. This is particularly concerning, since many such affected services are covered by China's GATS commitments. One obvious example would be cross-border data processing services, for which VPNs or leased lines are a key mechanism to ensure the security and confidentiality of such information. Is it China's intention to restrict use of leased lines and VPN for accessing such services? If so, how does China reconcile this with its obligations under its specific commitment with respect to cross-border data processing services?

7. In addition, since the Circular would have a direct and significant effect on the ability of cross-border service suppliers (including sectors such as cross-border data processing services), to access and use of public telecommunication services (i.e. VPNs and leased lines), it would appear to fall within the scope of Article 5(c) of the Annex on Telecommunications of the General Agreement on Trade in Services ("the Annex"). This provision was designed specifically to ensure access to leased lines and other services (e.g. VPN services) that suppliers use to facilitate the cross-border supply of any scheduled service. Additionally, this provision, for measures significantly affecting access to and use of telecommunications networks and services, requires notification of other WTO Members and provides for consultation with affected Members. If China does indeed plan to move forward with implementation of the Circular, does China intend to provide such a notification and the opportunity for consultation?

8. Since this measure is due to enter into force by 31 March 2018, we request that China expeditiously respond to these questions and concerns.

9. The United States urges China to address these concerns quickly and pursue new policies that promote rather than disrupt cross-border transfers of information and trade in services. The United States will continue to monitor developments in China and provide further updates to the Council. We also welcome the views of other potentially affected WTO Members.
