Regulating for Globalization

Trade, Labor and EU Law Perspectives

Is India's Ban on TikTok and other Apps Justified by the WTO National Security Exception?

Himanshu Singh Rajpurohit (National Law University Jodhpur) and Tilak Dangi (NALSAR University of Law) · Tuesday, October 27th, 2020

India imposed a ban on 247 Chinese mobile application including TikTok, PubG, Helo, and WeChat on the basis that these applications are involved in activities which are detrimental to the sovereignty and security of India. The Government stated that it has received complaints from many sources regarding the misuse of these apps to steal and transmit user data without authorisation to servers located outside India. China immediately responded by accusing India of discrimination and asserted that the ban is a blatant violation of WTO rules. China has also raised this issue at a recent WTO meeting and accused India of resorting to restrictive and discriminatory measures which undermine the transparency, stability & predictability of the Indian market. India didn't respond formally to China's comments at the said meeting. China's assertions fail to consider that India's ban is justified under the security exception provided in the General Agreement on Trade in Services (GATS).

Chinese apps are an issue because the Chinese Intelligence Law authorizes any data collected to be shared with the government. For example, Article 7 of the Chinese Intelligence Law *mandates individuals, organizations, and institutions to assist Public Security and State Security officials in carrying out a wide array of "intelligence" work. It stipulates that "any organization or citizen shall support, assist, and cooperate with state intelligence work according to law."* Along with Article 7, Article 14 stipulates that "state intelligence work organs, when legally carrying forth intelligence work, may demand that concerned organs, organizations, or citizens provide needed support, assistance, and cooperation." Thus users in India have reason to be concerned about the sharing of data collected by the apps.

TikTok will spy on a user from the moment one installs it. TikTok is an audio/video sharing application that requires a user to provide access to the user's camera, microphone, GPS location data, SD card, information on what other apps are running, notifications that pop up – together providing extensive surveillance of the users. Video recorded by a user is automatically and immediately sent for storage outside India, even before it is edited, filtered, or posted. In March 2020, the Arkansas attorney general, in the United States, officially announced that default TikTok settings were allowing predators to create secret video groupings of Musical.ly's users. Musical.ly has since become TikTok, but the app's format and operation remain the same.

TikTok was investigated as a potential national security risk by the United States as well. "With over 110 million downloads in the United States of America alone, TikTok is a potential

counterintelligence threat we cannot ignore," Senators Schumer and Cotton wrote to Joseph Macguire, Acting Director of National Intelligence. Subsequently, the United State of America's President by executive order has prohibited Americans from carrying out any transactions with the parent company of TikTok. Similarly, these applications have over 200 million daily active users in India. In March, researchers revealed that Android and iOS apps, including TikTok could automatically read anything copied onto your mobile device's clipboard, which makes the threat graver. The application can also copy the device's local data as well as that from nearby devices (if the devices are connected within 10 feet share the same Apple ID). Android presents a more significant risk because Android APIs provide even less protection than iOS.

There have been complaints against the UC Browser because it collects and transfers user data to servers in China. Some allegations suggest that even after uninstalling or clearing browsing data, the browser retains control of the domain name system (DNS) of the user's device. Reports from the University of Toronto indicate the presence of "several major privacy and security vulnerabilities that would seriously expose users of UC Browser to surveillance and other privacy violations," which is then been relied upon by the Ministry of Electronics and Information Technology of Indian Government to investigate against UC browser.

Prima facie India's act of banning these applications stands in violation of the most-favoured-nation principle which forms the bedrock of framework governing international trade in services. Even if India has not taken any specific commitment under GATS for the digital services sector, as is clear from India's schedule of commitment there is an obligation to not discriminate between Chinese applications vis-a-vis other foreign & domestic applications in terms of treatment accorded. Additionally for proving a violation of most-favoured-nation treatment, the measure must affect the trade in services for the purposes of GATS. In *US-Gambling* where a blanket ban was imposed on cross-border supply of remote gambling services, such a ban was found to be affecting trade in services. Similarly, in the present case, a complete ban on these applications from rendering services affects trade in service. Moreover, the effects of the ban have even started appearing as a lot of companies' valuation have decreased while others are expecting big losses due to this ban which further buttresses the claim that trade in services is being affected due to this ban.

In that case, India has recourse to Article XIV *bis*, which provides that a member can adopt and enforce any Measure, in the interest of national or international security, otherwise inconsistent with its obligations. In essence, Article XIV *bis*, GATS confers unrestricted discretions upon members to frame measures inconsistent with GATS, in the interest of legitimate security. This is due to three reasons mainly. *First*, the plain reading of the text reveals the use of the term 'its' essential security interest, which means that it is the judgment of the member which is determinative. These actions are intrinsically political in nature and can only be assessed properly by the member in question. *Second*, this is also supported by the context of Article XIV, which lacks the 'it considers' phraseology which is used in Article XIV *bis*, which indicates its self-judging nature. *Third*, the supplementary means of interpretation i.e., travaux préparatoires, provides that the provision is self-judging. The travaux préparatoires of the Article XXI, GATT should be given precedence when interpreting Article XIV *bis* because both provisions have semantic similarities. The history of the GATT reveals that members are empowered to take steps to protect their essential security interest, and the political approach, is subject to judicial deference.

Finally, the Panel's conclusion in *Russia – Traffic in Transit* case is inconsistent with the travaux

préparatoires of Article XXI GATT. The Panel concluded that the security exception is subject to the ITO Charter, based on the misinterpretation of Australia's statement during negotiations in July 1947. In this case, Australia wanted to ensure that a member's right would not be affected by a Measure which it considers necessary for the protection of essential security interests. Thus, the irrevocable self-judging nature of the provision gives complete independence to a nation for determining what is a threat to national security.

Although China claims a ban on these apps violates WTO Rules, the potential threats to national security posed by the very design of Chinese applications are self-evident. Considering the recent tensions at the India-China border, the possibility of misuse of data is very real. There are also real questions about the intent behind the design of these features. China could ask for the same data, but it shouldn't be allowed to take it if that operation threatens India's national security. The exception provided under GATS Article XIV bis safeguards India's ban because it gives complete discretion to a member to decide what national security threats it faces.

This entry was posted on Tuesday, October 27th, 2020 at 3:16 pm and is filed under General Agreement of Trade in Services (GATS), India, Social Media, Trade Law, WTO
You can follow any responses to this entry through the Comments (RSS) feed. You can leave a response, or trackback from your own site.