Research on Applying the WTO Security Exception Clause to the Security Dispute Caused by Cross-border Data Flows

Take the *Tik Tok Case* as an Example

Chengze Jiang

Law School, Beijing Foreign Studies University
Email: jiangcz0619@163.com

ABSTRACT
Personal data is now routinely flowing between legal jurisdictions, making the personal data of residents in each country particularly vulnerable to acquisition by foreign intelligence services. As a result, barriers to cross-border data flows are spreading globally due to security concerns. For example, TikTok, owned by a Chinese company, ByterDance, is a short-form, video-sharing app that allows users to create and share videos with people worldwide. Since its launch, the TikTok app's popularity has been growing tremendously. In 2020, the United States declared a national emergency regarding the threat that Tik Tok would harm national security and took sanction measures, such as prohibiting the use of the app. If the case goes to the WTO, the security exception clause would be America's best defense. The Security Exception Clause in WTO's framework is based on national sovereignty, seeking to balance between "essential security interests protection" and "free trade." This article will utilize the Tik Tok case to examine the application method of the security exception clause towards disputes caused by cross-border data flows and put forward some suggestions for the future development of cross-border data flows security.

Keywords**:** *Cross-border data flows, WTO, The Security Exception Clause, Tik Tok, Cyber-Security*

1. INTRODUCTION

"Cross-border data flows" refer to the movement or transmission of information across national borders. Society has entered the era of big data, with vast data flows worldwide on a large scale, thanks to the full development of information technology. Cross-border data flows are now playing a more and more crucial role in services like sustaining global commerce, improving health and safety, and promoting social good. In 2014, data flows contributed $2.8 trillion to global GDP. Compared to the traditional trade flows, now it is cross-border data flows that can generate more economic value. According to McKinsey 2016 report, global data mobility increased from 4.7 Tbps to 211.3 Tbps between 2005 and 2014, representing an annual growth rate of 52 percent. A World Bank study also indicates that restricting cross-border data flows "may cut GDP by up to 1.7 percent, investments up to 4.2 percent, and exports by 1.7 percent." Nowadays, cross-border data flow is undoubtedly an efficient technical means and an indispensable part of economic globalization.

However, while cross-border data flows are flourishing, their security has become an issue. Cross-border data flow security can be classified as information security in cyber security. Cyber security, which is defined as the ability to protect or defend cyberspace from cyber attacks, comprises five types, of which information security is the most significant. Information security primarily refers to protecting data's integrity and confidentiality, both in storage and in transit. In the process of cross-border data flows, the risk of personal privacy and proprietary information being leaked and disclosed is pretty high due to many factors, such as ideological differences, political and economic competition between countries, or simply for technical reasons. As a result, many countries have realized the potential security risks behind cross-border data flows and have introduced a series of control measures towards relevant enterprises.

2. BACKGROUND OF THE TIK TOK CASE AND AMERICA'S MEASURES

ByterDance is a company founded in China in 2011 and its product, Tik Tok, where users can post and share their self-created short videos, has proliferated rapidly and successfully established a solid global presence. Users can comment and give "likes" to the videos, and such data will all be collected by the company. Thanks to a powerful artificial intelligence-backed recommendation engine, ByterDance has created a fast-emerging short video social network where the company could recommend videos to different users based on the features of preferences as well as their previous viewing history. What is more, ByterDance has grasped a large amount of personal information as submitting information about real name, gender, language, country, age, ethnicity, and so on is a necessary procedure when registering to use Tik Tok.

ByterDance promises that the customer databases of China and the United States are entirely isolated and cross-border flows of data will not occur between the two countries. The data in the U.S. is not allowed to be transmitted back to China. In 2016, ByterDance established a subsidiary company to operate Tik Tok in the United States. The branch office fully complies with the U.S. domestic laws and policies as it locates the customer database of the U.S. users in Virginia, within the territory of the United States, with backup redundancy in Singapore. Also, the data in China won't flow to America as users in China can only use Douyin(Chinese version of Tik Tok) in the territory of China and are not allowed to register as a user of the U.S. to use the app. TikTok and Douyin have almost the same user interface but no access to each other's content. Chinese users cannot see the videos posted by American users, and vice versa.

This does not mean that there is no possibility for cross-border data flows. The recommendation engine is developed and updated by the parent company in China. In addition, ByterDance admits there exists a close connection between the parent company in China and the subsidiary company in America, and the parent company is responsible for all business activities in the territory of America. Due to the close tie between the Chinese government and ByterDance, the U.S. government is concerned about America's cyber-security. If the information collected by Tik Tok on U.S. users has flowed to China and is being shared with the government of China, the Chinese government can easily track the U.S. nationals' locations, build dossiers of personal information for blackmail, and conduct corporate espionage. Additionally, the US government suspects ByterDance and the Chinese government may transmit some data critical of the U.S. government to the U.S. so as to trigger conflicts, By making use of the recommendation engine, they can also control what can be viewed by the users, making any anti-America movement possible.

On August 8, 2020, based on the CFIUS judgment on ByteDance's acquisition of Musical.ly, the former U.S. President Donald Trump issued a prohibition Order, asking the Chinese business, ByteDance, to sell its TikTok App in 45 days in the name of preserving U.S. national security. At the same time, he issued some executive orders banning Tiktok's use within the territory of the United States. Trump declared a national emergency regarding the threat that Tik Tok will harm the nation's cyber security as it might store sensitive information to commit malicious cyber-enabled actions, including economic and industrial espionage against America and its citizens.

This Tik Tok case has not gone to the WTO. The final settlement was for Oracle and Walmart, two U.S. corporations, to take a 12.5 percent and 7.5 percent stake in Tik Tok, respectively, with Oracle storing all the data. Moreover, the executive orders banning Tik Tok's use were revoked by Trump's successor, President Joe Biden, in June 2021. The result of the successful acquisition is a compromise ByteDance company made for commercial purposes, but that does not mean the sanctions adopted by the United States are entirely justified. In the event of China initiating proceedings against the U.S. measures at the WTO, Bytedance might not have to make such a sacrifice. The most likely defense for the United States would be the security exception clause under GATS in the trial. Whether the security exception clause can be applied to such disputes caused by cross-border data flows is worth pondering.

3. ANAYLISYS OF THE TIK TOK CASE

3.1 the introduction of the security exception clause

The WTO security exception clause is a special regime that allows contracting parties to exempt obligations under trade agreements on the grounds of safeguarding national security. The core to the application of this clause is to find a "balance" between allowing members to take exceptional measures to safeguard national security and preventing members from excessively exercising trade protection in the name of protecting national security.

The security exception clause refers to Article XXI of GATT and Article XIV bis of GATS, which are exactly the same, describing three general situations allowing derogations from any provisions for security reasons. Firstly, any member reserves the right to derogate from any obligation that requires them to furnish any information which it considers that doing so would jeopardize their essential security interests; The provision's core is the second situation, which states that

members can take steps to preserve the country's essential security interests：(i) relating to the provision of services to military institutions; (ii) relating to nuclear fission and fusion; (iii) taken during a war or under other emergencies in international relations. The last situation suggests that members can take any action to maintain international peace and security in accordance with their commitments under the United Nations Charter.[1]

Much of the controversies revolve around the second situation and fall into the scope of "war or other emergencies in international relations." The vagueness of the word "other" as well as the national security itself have brought about many disputes in the clause's application. In the era of the GATT, members had great discretion in invoking the security exception clause. For example, *in United States-Trade Measures Affecting Nicaragua*, the United States argues that the clause gives it total discretion, and the panel is not allowed to examine or judge the validity of or motivation for the invocation. Instead of directly addressing the question of discretion distribution, the panel, in that case, adopts an evasive attitude.

However, in recent years, to legitimize the economic barriers set up to protect their own interests in international commerce, some developed countries, represented by the United States, have been expanding the application scope of the security exception clause. In addition to the essential purpose of protecting national defense and military security, members are increasingly asserting security exceptions in non-traditional areas. To prevent such unlimited expansion of the application scope, in 2019, the panel in *Russia - Measures Concerning Traffic in Transit* has clarified the jurisdiction of WTO towards the application of the clause.[2] A panel can objectively review whether the security exception clause's implementation conditions have been met and examine if the measures taken by members conform to the circumstances listed in the clause.[3] This article summarizes a three-step review method based on the panel report to determine whether the security exception clause can be invoked as a defense basis.

What should be given priority to be proved is whether the disputing members are in a state of "war or other international emergencies". Such emergency is an objective fact, subject to subjective determination. Panels have the right to conduct an objective evaluation to determine whether a member is in the midst of a war or an international emergency, and the procedure should be undertaken in good faith. When evaluating a crisis, the panel needs to test if it falls within the categories listed in the clause and if its severity can meet the standards to be protected.

The next step is to identify the essential security interest that has been violated. The panel in *Russia-Traffic* held that the specific interests that are considered straightforwardly pertinent to the protection of a state from such external or internal threats would rely on the particular situation and perceptions of the state in question and can be anticipated to vary with evolving circumstances. Each member is free to identify what it views to be its essential security interests. Nevertheless, the recognition process needs to be guided by the principle of good faith. [4]

Finally, the member claiming the security exception as a defense must show that the measures adopted are connected to and necessary to protect the "essential security interests" that it seeks to safeguard. Although the clause indicates explicitly that the invoking member has discretion in deciding what action it considers necessary to preserve its essential security interests, this does not imply that the member enjoys "total discretion." Had the standard been "total discretion," there would have been no requirement to incorporate separate paragraphs in Article XIV bis and distinguish between different types of security interests that could be used to justify a measure otherwise inconsistent with the GATS. Moreover, notwithstanding the absence of an introductory paragraph akin to the chapeau to Article XIV, an objective assessment conducted by the panel must contain an examination of whether the claiming member has acted in good faith, notwithstanding the absence of an introductory paragraph similar to the chapeau to Article XIV.

Only when a member completes the above three-step review can it invoke the security exception clause as a defense and justify trade restrictions under the WTO framework.

3.2 Applying the security exception clause to the Tik Tok case

It is self-evident that the controversy in the Tik Tok case has nothing to do with information disclosure and breach of international duties under the UN Charter. The matter under discussion here should be included in "other emergency in international relations. " We should use the aforementioned three-step analysis method outlined in *Russia-Traffic* to interpret the likely resolution of the Tik Tok case if China initiates WTO proceedings against the United States.

3.2.1 Analysis of emergencies in international relations.

Whether the United States is in a state of international emergency is an objective fact that needs to be interpreted by the panel subjectively. There are two main problems here: (1)whether the United States, in a non-traditional emergency, can invoke the security exception clause ; (2) whether the state demand has been satisfied.

3.2.1.1 whether a crisis in the non-traditional area fall within the protection scope

The crisis under discussion here is about cyber information safety caused by information disclosure, and there is only a remote possibility of actual armed conflict. Such a crisis is not directly listed in the clause and is quite different from traditional emergencies like war. Although the WTO has yet to adjudicate a single case directly linked to a crisis in non-traditional security areas, both theoretical analysis and empirical evidence prove that such crises can be covered in the protection scope.

All the other issues in the clause are much more objective and detailed than "emergency in international relations," suggesting that this term is more likely to serve as a miscellaneous clause. Due to space limitations, the provision cannot list all the situations. In Russia-Traffic, the panel reiterates its understanding of "emergency in international relations" as a situation of armed conflict, latent armed conflict, heightened tension or crisis, or general instability engulfing or surrounding a state. However, despite the panel's best efforts to narrow down the concept of international emergency, the vagueness and abstraction of the "heightened tension or crisis" still imply the possibility and legitimacy of other more detailed interpretations. Regarding the dictionary meaning of "heightened tension," we find it refers to a growing likelihood of sudden violence, conflict, or other serious issues. The context of the term "heightened tension or crisis" in conjunction with "latent armed conflict" and "general instability engulfing or surrounding a state" further clarifies the meaning of "heightened tension or crisis." Actual armed conflict is not necessary, and other serious conflicts can also fall within the scope of emergency in international relations.

Including crises in the non-traditional area in the protection scope of security exception clause accords with the demand of social development. With the end of the Cold War and the development of globalization, country-to-country warfare is no longer merely a "political concept."[5] The security issues faced by all countries are increasingly diversified. Various non-traditional security issues are constantly emerging. Considering that modern weapons are too lethal and the war will take a heavy toll, new modes of conflict, such as cyber warfare, are emerging. These new forms of conflict, whose dangers are not inferior to war, should be classified as an emergency in international relations. For example, in WTO dispute settlement practice of cyber warfare, trade rules are applied equally to the natural and cyber world by panels and appellate bodies. [6]In the United states-gambling and Betting Services case, the Appellate Body has demonstrated that, in the absence of manifest exclusion, all of the Members' commitments apply to all delivery types, including the use of the Internet as a delivery medium. In other words, Members' rights and obligations regarding WTO agreements automatically extend to the Internet sector. Also, Tallinn Manual has indicated that using force occurs when cybersecurity issues create situations and consequences comparable to using force in military warfare. The cyber attacks on Estonia and the "Stuxnet" incident can constitute cyber warfare, and these countries have the right to declare under the condition of international emergency. [7]

Thus, the tension or crisis upon non-traditional security issues such as cyber information safety can also constitute an international emergency if the state demand is satisfied.

3.2.1.2 whether the seriousness demand has been satisfied.

Simply proving the existence of a cyber information security emergency is not enough. The United States must also prove that the seriousness of the crisis posed by Tiktok is akin to war.

The panel needs to assess the state of the emergency claimed by the United States. If it is a purely political and economic crisis, the United States can not justify trade restrictions by invoking a security exception clause. The phrase "other emergency in international relations" in conjunction with the use of the word "war" in subparagraph (iii), as well as the interests and matters specified in other subparagraphs, showcasing that the seriousness of the emergency should be comparable to war or the presence of military establishment and fissionable materials, to qualify as an emergency in international relations. Considering the purpose of the security exception clause is to protect a country's essential interests, simply disagreements between member states generated by political or economic differences are not sufficient to constitute an emergency in international relations. For sure, the political or economic disputes among member states are frequent and inevitable. However, such kinds of controversies will never be classified as "emergencies in international relations" within the meaning of the security exception clause, no matter how urgent or crucial the issue is in a political or economic sense. Only the situation whose seriousness is akin to war and other matters addressed in the clause and result in defense or military interests or the maintenance of law and order can be defined as an "emergency in international relations."

In this way, the United States and China should present evidence and express views on the seriousness of the emergency in the Tik Tok case. The United States ought to showcase the imminence of cyber information safety problems. US government can prove this by providing evidence of the information leakage and the Chinese government's illegal use of information collected by Tik Tok, such as tracking the location of

U.S. citizens and so on.[8] With such evidence, the United States can claim that though frictions are the only thing on the horizon in the Tik Tok case, fears are mounting that America's security could be seriously jeopardized and that conflict could escalate.[9] Finally, the possibility of its eventual evolution into information weaponization and cyber warfare should not be excluded. China can prevent the United States' recognition of emergency by demonstrating that the cross-border data flows controversy here is a common long-term economic dispute rather than a sudden emergency. America may not invoke security exception provision unless it offers sufficient evidence that the danger is no less than war and the impairment of defense and military interests or maintenance of law and public order interests. China can provide a series of evidence; for example, Tik Tok has never engaged in illegal information collection to commit malicious cyber-enabled actions, and that ByteDance is in a strong position to compete fiercely with comparable U.S. companies.

3.2.2Analysis of the threatened essential security interests

The rise of cross-border data flows will inevitably bring about security problems. Whether the security of cross-border data flows is an essential security interest is the focus of discussion. Since it is left to the members to determine what it considers to be its essential security interests, the United States can certainly argue that its essential security interests have been violated.

The United States can propose that to include critical cybersecurity in the scope of national security is not an arbitrary or unreasonable extension of the term, but because many behaviors that threaten "essential security interests" are transferred into cyberspace, which eventually manifests as cybersecurity interests. TikTok has more than 300 million monthly active users and has access to vast swathes of personal information collection and control. Due to the app's terms of service, those dates might be handed over to the Chinese government as the data can be shared with ByteDance, the app's parent firm. The consequence of such cross-border data flows lies in Chinese authorities' ability to track the locations of Federal personnel and contractors, construct dossiers of personal information for blackmail, and undertake corporate espionage, which significantly threatens America's security interests.

Despite the United State's decretion, China also can contest America's assertion of essential security interests. The recognition of essential security interests is subject to certain limitations. "Essential security interests" encompasses a more specific set of considerations than "security interests." Since a member can define its "essential security interests," members might identify the security interests at will. Failures by members to affirm essential security interests in good faith might serve as means for members to circumvent their obligations and duties under the WTO framework. So it is improper to offer the invoking party the absolute discretion right as there would not be any defense against its abuse for all sorts of subjective security concerns.

The good faith principle which all the members have to follow when determining the essential security interests implies that the panel can also have the right to examine the essential security interests. During the process of examining the honesty in a member's conduct, the panel of course ought to estimate the characteristics of the interests. Consequently, the discretion of the WTO members in determining the essential security interests, which one might deem almost unlimited due to the vague terminology, should be subject to limitations reviewable by the WTO judiciary. In this way, in addition to being bound by the good faith principle, members are also bound by the panel as it is authorized to conduct an objective review of members' interpretation and application of essential security interests. This allows for effective control of the invocation of security exceptions only in objectively determined situations, to the benefit of protecting trade interests, while respecting room for maneuver for the WTO members in determining and protecting their essential security interests.

When the panel begins to examine whether the interests violated in the case fall within the scope of essential security interests, the first step is to distinguish between essential security interests and security interests. Essential security interests generally refer to those interests relating to the quintessential functions of the state, namely, the protection of its territory and its population from external threats and the maintenance of law and public order internally. The panel in Russia-Traffic interprets essential security interests as those that relate to the state's most quintessential functions, such as protecting the territory and citizens from external threats and upkeeping the law and public order within the country. The panel can take the background of the disputes into account, the more characteristic and distinctive is the 'emergency in international relations' invoked by the member state, the more likely the interests being impaired relate to the country's basic function, including defense of military threats or the maintenance of law and public order.

China can present evidence and argue that ByteDance Company and Tik Tok do not impair the United States' essential security interests. The accusations in the Prohibition order issued by Trump and the related reports are all speculative and fail to disclose any substantial evidence identifying unusual and extraordinary threats posed by Tik Tok—or any actual national security threat at all. Chinese authorities

could not get the data of American users since the subsidiary company operating Tik Tok in the United States totally complies with the U.S. laws and store all the data captured within the territory of the United States. Also, as no direct or indirect evidence about ByteDance turning over any data back to China can be unearthed by the United States, China has reasons to suspect that the United States is just looking for an excuse to sanction promising Chinese technical corporations in the context of the trade war between the two countries. Instead of protecting security interests, the United States's justifications of security exceptions were pretextual, and it is actually an anti-China behavior.

3.2.3. Analysis of whether the measures taken by the United States are related and necessary to the "essential security interests" that it intends to protect

A member can use only the measures passed the necessity and articulation test to justify trade restrictions on other countries by invoking the security exception clause. According to the therm "which it considers," the members are given self-determination right. However, it does not mean that such decretion is not subject to any restrictions. Members still need to abide by the principle of good faith and bear the burden of proof in conducting measures. Firstly, the members need to prove the necessity of the measures. "Necessity" should be based on the substantial connection between the measure and the goal. The measures adopted should have the least plausibility to the emergency in international relations should cause the least harm compared with other possible measures. Secondly, the invoking party needs to prove the relevance between the emergency in international relations and the essential security interests. The higher the degree of relevance is, the lower the member's burden of proof will be.

The measures taken by the United States were to issue executive orders, which sought to prohibit the use of Tik Tok and force Bytedance, the Chinese-owned parent companies, to sell the subsidiary branch to a U.S. company. However, the U.S. sanctions against Tiktok have not actually been fully implemented. The Tik Tok case ended with Bytedance's compromise and Biden's revocation of the executive order, and it did not reach the WTO trial. Currently, TikTok remains available and popular in the U.S. Since this article wants to explore the possible verdict of the Tik Tok case if China appeals to WTO(in fact, it doesn't), we need to assume that all the measures of the U.S. government have been successfully implemented. The panel needs to test the necessity and articulation of the measure.

Suppose the United States can indeed submit evidence that ByteDance colluded with the Chinese authorities and that the Chinese government can have access to or even make use of the U.S. citizen's personal information and other sensitive information through cross-border data flows. In that case, the United States can certainly argue that the measures taken are relevant and necessary to the "essential security interests" that it intends to protect.

Measures that have nothing to do with protecting essential security interests cannot be considered relevant and necessary since it violates the good faith principle. Some U.S. scholars believe that the actual motive of the executive order is political retaliation rather than security interests protection. In June 2020, despite boasting that more than 1 million citizens have requested the tickets to attend the Saturday rally, Trump did not fill his rally arena to the capacity as the actual number of registered attendees was less than 10,000. In the days leading up to Trump's rally, a coordinated effort on TikTok urged people to register online for the free event but not show up. Trump became so furious as a large number of TikTokors who asked for tickets have trolled him, and he subsequently issued an executive order banning TikTok. In many people's view, instead of protecting the U.S.'s security interests, it is political revenge to silence citizens who hold different opinions.

If the measures taken by the U.S. have caused unnecessary damage to China and ByteDance Company and there apparently existed better approaches, they can not pass the necessity test. The panel can examine whether there are measures that would have the same effect but would do much less harm to the other member state. Suppose the United States is aware of such an available measure but ignores the option for the sake of its own interests. In that case, the measures may not be considered necessary and relevant. For example, China can claim that, if the United States is particularly concerned about monitoring of government employees, banning them from using TikTok is a more elegant and appropriate solution than banning the app.

4. SUGGESTIONS ON RATIONALLY PROMOTING CROSS-BORDER DATA FLOWS SECURITY

The Internet creates the potential to deliver massive amounts of data to almost any location in the world instantly and at virtually no cost. Such cross-border data flows trigger not only economic competition but also disputes over national security. As data is flowing between legal jurisdictions, security issues arise as personal data might be particularly vulnerable to acquisition by foreign intelligence services. For the purpose of protecting national security, more and more countries choose to enact barriers to cross-border data flows, which makes it more expensive and time-consuming to transfer data abroad. For example, a new concept called "data localization," confining data within a country's borders by forced local data residency

regulations, has evolved and spread globally. Data localization is aimed at a rising range of specific data types as well as broad categories of data that are deemed "essential" or relevant to national security. The number of nations that have enacted data localization measures has nearly doubled from 67 in 2017 to 144 in 2021, and the overall number of data localization policies (including express and de facto) has more than doubled.

The Tik Tok case is not the first dispute over the cross-border data flows security, and in the future, more and more similar cases are likely to emerge. Measures taken in those cases might run counter to the WTO's aim of promoting trade liberalization as they pose a rising threat to the potential for an open, rules-based, and innovative global digital economy. Enterprises, especially those who provide data-intensive services, use data to create value, and when data cannot flow freely overseas, many can never maximize that value. Restrictions to cross-border data flows will be detrimental to economic productivity and innovation. However, promoting global trade liberalization does not mean that members should give up national security, which is critical since it affects all aspects of economic and social development in every society. Therefore, improving the security of cross-border data flows is a top priority. Enterprises that provide data-intensive services, member states, and the WTO can all adopt some measures to improve the cross-border data flow security so as to further promote its development.

For enterprises that provide services for data flows across borders must pay more attention to data privacy. A good solution would be to create completely isolated databases for each country, where the data is stored within a certain country's territory, or sign agreements to keep the database in a relatively independent, mutually trusted third party. At the same time, ByteDance's solution of multinational corporation cooperation is worth considering. Instead of totally abiding by the executive orders and selling the subsidiary company in the U.S. directly to a local company, which would bring about significant losses, ByteDance sold part of its shares to Oracle and Walmart, two U.S. corporations. It will be a partnership, with Oracle controlling the database and ByteDance providing support and other services. In this way, ByterDance's ownership and right of control to the American subsidiary company have been guaranteed, and the U.S. government's concerns and fear about the security of cross-border data flows will be eliminated.

Countries should establish a regulatory system for cross-border data flows under the overall security concept. Cross-border data flow is essentially the transfer of data between different jurisdictions. If the countries from which the data flow and the countries from which the data flow take different measures to regulate and protect cross-border data, it may lead to disputes. Therefore, domestic legislation needs to make interpretations on two issues: one is the differentiated application of laws and regulations abroad after the data outflow; the other is the coordination of the jurisdiction over the data outflow by the original domestic regulatory data regulator. Meanwhile, domestic legislation must provide strict supporting management mechanisms to regulate the scrutiny of cross-border data flows, and how such data may be provided to overseas parties should be strictly limited. For example, in China, the cross-border data flow should pass the security assessment conducted by the national cyberspace administration or get certification from professional institutions. The standard contract stipulated by law must be concluded with the offshore recipient when cooperating with foreign companies.

As for the WTO, it shall fully consider the security of cross-border data flows from substantive and procedural perspectives so as to make adjustments in legal interpretation and specific application. From the standpoint of substantive law, the WTO should directly respond to the issue of protection in the field of non-traditional security, such as cybersecurity. What is more, more detailed criteria and standards for determining emergencies in international relations should be provided in legislation and judicial decisions. And the panel should be authorized to conduct objective reviews of members' identification of essential security interests to prevent the abuse of power. From the perspective of procedural law, the WTO needs a more rigorous procedural system to regulate the security exception clause. Since the application of the security exception clause stemmed from the protection of State sovereignty, it was likely that many countries would be eager to exercise their self-determination right to and take measures immediately to protect their security interests, which would then lead to disputes concerning the necessity. Therefore, the WTO could make some procedural provisions. For example, the WTO could advance the review process in the face of the emerging security field of cross-border data flows. Before taking the measure, Members shall inform the WTO and enter into consultations with the relevant parties. Members can discuss the proportionality and necessity for the invocation of the security exception clause. If the Parties cannot reach an agreement on such compensation through consultations, the members can then choose to take the measure.

5. CONCLUSION

In the TikTok case, the conflict between data flows and national security was highlighted. The United State's sanctions on Tik Tok impedes cross-border data flows and thus inhibits Trade Freedom. We should reflect on TikTok ban and seek ways to respond accordingly. There is a urgent need to figure out a set of

proposals to provide legal support and basis for ByterDance-like IT service enterprises to safeguard their legitimate interests in international economic and trade exchanges, to provide theoretical support for WTO members to open up to a higher level, and to escort enterprises to go global.

REFERENCES

[1] Panos Delimatsis,Thomas Cottier; Article XIV bis GATS: Security Exceptions, in:

International Economic Law eJournal. October 2008

[2] Russia - measures concerning traffic in transit essay reference, Report of the Panel, WT/DS512/R, 5 April 2019 [Hereinafter DS512 Panel Report]

[3] Chao Wang, Invocation of National Security Exceptions under GATT Article XXI: Jurisdiction to Review and Standard of Review, in: Chinese Journal of International Law, Volume 18, Issue 3, September 2019, Pages 695–712, https://doi.org/10.1093/chinesejil/jmz029

[4] G.Vidigal, WTO Adjudication and the Security Exception: Something Old, Something New, Something Borrowed – Something Blue?, in: Legal Issues of Economic Integration,Legal Issues of Economic Integration Volume 46, Issue 3 (2019) pp. 203 – 224

[5] Jay Manoj Sanklecha, The limitations on the invocation of self-judging clauses in the context of WTO dispute settlement. In: October 2019Indian Journal of International Law 59(1-4) DOI:10.1007/s40901-019-00108-6

[6] Rolf H.Weber, Cybersecurity in the Internet of Things: Legal aspects, in: EvelyneStuder, Computer Law & Security Review,Volume 32, Issue 5, October 2016, Pages 715-728. DOI:https://doi.org/10.1016/j.clsr.2016.07.002

[7] Peng, Shin-yi, Cybersecurity Threats and the WTO National Security Exceptions (June 6, 2015). Journal of International Economic Law, Volume 18, Issue 2, 449-478 (2015)., Available at SSRN: https://ssrn.com/abstract=2640447

[8] Trachtman, Joel P., The Internet of Things Cybersecurity Challenge to Trade and Investment: Trust and Verify? (April 18, 2019). Available at SSRN: https://ssrn.com/abstract=3374542 or http://dx.doi.org/10.2139/ssrn.3374542

[9] Voon, Tania and Mitchell, Andrew D., Australia's Huawei Ban Raises Difficult Questions for the WTO (April 22, 2019). Available at SSRN: https://ssrn.com/abstract=3390675 or http://dx.doi.org/10.2139/ssrn.3390675