The US TikTok Ban bill: Analyzing US-China Tensions and Regulatory Frameworks for Big Tech Multinationals

By Mora Surijon

Surijon, Mora (2024) The US TikTok Ban bill: Analyzing US-China Tensions and Regulatory Frameworks for Big Tech Multinationals. The Mathurin Hybrid Initiative, Global Economy & Diplomacy, 1-8; https://www.mathurinhybridinitiative.org/global-economy-diplomacy

Introduction

Recently, the United States House of Representatives passed a rather controversial bill. This legislation would require ByteDance, the Chinese parent company of TikTok, to sell off its U.S. operations within a six-month period or face a ban. With a resounding bipartisan vote of 352-65, the bill's passage was evident.

Departing from this recent development, many questions arise. Some may seem superficial, such as why U.S. lawmakers are concerned about TikTok. Is this platform truly a threat to national security? Does a country have the authority to dictate which social media platforms its citizens use within its borders?

On a deeper level, one might ponder the growing significance of these new digital platforms, initially designed for entertainment, in shaping diverse international political narratives. Can they play a role similar to more traditional media outlets? Do algorithms influence an individual's political stance?

One could also explore the realm of non-state actors and the constraints they impose on states. To what extent should they be granted freedom? What sorts of regulatory frameworks can we envision for digital platforms and how they utilize the data collected from their users? Should there be laws regulating algorithms?

This article is structured into three parts: Firstly, an analysis of how the debate over the TikTok ban reflects a new chapter in tensions between the U.S. and China. Secondly, the case will be examined through a reflection on the growing political relevance of non-state actors, such as private companies that manage digital platforms. Lastly, the topic of possible and existing regulatory frameworks that states can impose on these internet companies and their behavior regarding user data and content manipulation will be addressed. In addition,

comparisons will be made with other states that have already imposed regulations and sanctions, such as the European Union, and China itself.

1. A new chapter in US-China tensions

In recent years, the rivalry between China and the United States has extended to domains such as international institutions, development financing, and global trade. The United States, historically positioned as the global hegemon, has experienced the rise of China, which has sought to challenge established norms and institutions dominated by Western powers. This shift in power dynamics is evident not only in China's growing influence within Western-dominated international organizations but also in its introduction of new narratives and initiatives, such as the Belt and Road Initiative (BRI), the Asian Infrastructure Investment Bank (AIIB), and the BRICS group. China's promotion of South-South cooperation narratives and its adoption of a unique 'market socialism' model further underscore its challenge to Western dominance. This rivalry extends into the private sector as well, particularly in the technology industry, where American companies like Instagram, Facebook, X, and Google have historically held influence.

China has advocated for the need to tell its own story and showcase its political discourse in the media, including social media apps. However, previous global efforts have predominantly relied on US platforms like YouTube, Instagram, Facebook, and X. Being the first Chinese global Internet platform, TikTok serves to disrupt this distribution stranglehold, offering China greater visibility in the global digital sphere. Considering TikTok boasts 170 million users and has become the primary source of information for individuals under 30 worldwide, it is crucial to be able to acknowledge the US possible TikTok ban not only as a data protection policy but also as a means of maintaining its own domain over hegemonic discourse and public opinion spaces. In theoretical terms, this highlights how digital platforms are central in global power dynamics, shaping international discourse and emphasizing the strategic significance of controlling these platforms to mold global narrative and perception.

Even certain journalists have gone so far as to claim that if the bill were to become law, this would unleash a new Cold War between the US and China for the control of solar panels, electric vehicles, and semiconductors. (Maheshwari, McCabe, and Karni, 2024).

2. The “TikTokisation” of politics

TikTok, originally a Chinese-native video sharing platform launched in 2016, has witnessed unparalleled growth since its international expansion in 2017 when ByteDance, its parent company, launched an international version of the app. ByteDance acquired its international predecessor, Musical.ly, for approximately 1 billion USD, further accelerating TikTok's global reach. The application has been praised for its ability to discover and promote emerging talents, as well as create viral trends. Primarily known for its short-form video content, TikTok allows users to create and share videos typically synchronized with background music. This unique format has contributed significantly to its widespread appeal, attracting users across various demographics such as Europe, the Americas, Asia Pacific, and Africa.

One of TikTok's remarkable achievements has been its immense popularity among young people. Recent research from the Reuters Institute Digital News Report indicates a fivefold increase in the use of TikTok for news among individuals aged 18–24 across all markets surveyed, rising from 3% in 2020 to 15% in 2022. Moreover, the platform has demonstrated its remarkable reach, with the ability to engage up to 40% of the 18–24 age group across 46 countries spanning four different regions worldwide. According to Ertuna, *"TikTok is not only the primary news source for a growing number of people (especially the youth), but it is also a highly politicized one"* (Ertuna, 2023:77). In this context, we can think of digital platforms similarly to traditional media: as entities that undeniably influence politics.

It's logical to wonder how an app could change the way people think. First and foremost, they utilize algorithms. In the case of TikTok, users land on a personalized "For You" page as they open the app, which consists of an algorithmically generated video playlist. This means that if the algorithm is fed enough, the user doesn't decide what content they see, but rather the platform does. Algorithms are programmed to collect data about the user through interactions with them. If this data is used to customize the advertising shown to the user to sell a product, why couldn't it be used to spread and "sell" political ideas?

In fact, many legislators who advocated for the ban expressed concerns about TikTok manipulating content through their recommendation system, with potential influences on the upcoming 2024 presidential election. Indeed, the platform has been extremely influential in the past three electoral cycles. As Marco Rubio, the Republican vice chairman of the Senate Select Committee on Intelligence, put it; *"(ByteDance) happens to control a company that owns one of the world's best artificial intelligence algorithms. It's the one that's used in this country by TikTok, and it uses the data of Americans to basically read your mind and predict what videos you want to see."* (Hale, 2024)

3. Regulatory frameworks

In a context of increasing globalization, it is inevitable that national governments lose power over the information circulating among their electorate. Unlike the pre-globalization citizens, who belonged solely to the Nation-State that physically encompassed them, this new citizen, turned internet user, can confine themselves to social networks that transcend the borders of States. As Diana Tussie put it, *"Politics is not just about public policy; we must recognize a broad constellation of actors, such as large corporations and their influence over the State (...)"* (Tussie, 2015:171). On top of that, new transnational societies are created on social networks where users interact, but the rulers of these societies are not democratically elected and rather CEOs of companies that created or bought the platform. (Aitken, 2023). In this sense, we can consider the TikTok ban bill as a peak through a much larger window that has been opening for several years: what actions can states take in response to this loss of sovereignty?

Those opposed to the act argued that it goes completely against the democratic and free market competition values that characterize the U.S., raising the question: why can US apps operate in the rest of the world, but foreign apps like TikTok are seen as a threat to national security? However, as we will see below, the U.S. is not the first to demand explanations and impose sanctions on these apps. On the contrary, there are already 157 data privacy laws around the world that are beginning to address this issue, and the EU and China itself have strict policies regarding social media and user data. In fact, in the discipline of International Relations, several concepts have emerged to illustrate this tension, such as cyber sovereignty, internet governance, and information sovereignty. (Aitken 2023:20).

According to Daskal and Sherman, states may seek to control their citizens' data for various reasons: Content Controls, primarily reflected in Chinese laws; Consumer Protection and Privacy, as reflected in the EU's laws; and Protecting Against Foreign Access, which is the main motivation for certain sectors of the U.S. Congress to target TikTok (Daskal and Sherman, 2020:5). Next, I will delve into the analysis of each of these legal systems, exploring their objectives and characteristics with as much depth as the scope of this type of work allows.

3.1 China: Isolation and the "Great Firewall"

The case of China is unique because it introduces the variable of the political regime. The People's Republic of China is characterized by a single-party system, in which the Chinese

Communist Party maintains a monopoly on power and does not allow the formation of opposing parties. There are detentions and censorship for those who criticize or oppose the party, and it appoints the main leaders and officials. From this logic, it follows that the main media outlets are state-owned, giving the party power to control information that reaches its citizens. For this reason, China has established what is known as the "Great Firewall," consisting of laws such as the National Intelligence Law of 2017 and the Counter-Espionage Law of 2014. These laws actively block the flow of information from non-Chinese sources and demonstrate high levels of distrust towards other states (Aitken, 2023:21). In effect, users do not have access to Western social media and sites including Google, YouTube, X, Instagram, WhatsApp, and Facebook. Chinese data privacy laws, therefore, do not arise from the need to protect citizens but rather from the party's need to maintain its leadership.

In this way, the power has advanced in the creation of important national digital platforms (such as Baidu, Youku, WeChat, Temu, Shein, QQ, etc.). However, it refuses to integrate Western applications, following its authoritarian informationalism model (Jiang, 2010:72). This model practices content censorship. What does this mean? According to Melin, *"The purpose of censorship has been that the leader controls the type of information that can influence and affect the citizens' perception and behavior"* (Melin, 2021:39). In fact, the reasons why TikTok is under investigation in the US pertain to the censorship of certain types of politically sensitive and inconvenient content for the Party, such as the suppression of Muslims in China, of the Uyghurs in Xinjiang, and jokes about how the COVID-19 pandemic was handled by the government of Xi Jinping. (Melin 2021:49).

It is crucial at this point to not confuse the Chinese Communist Party with the TikTok application, as if they are the same actor. While the company ByteDance is Chinese, in response to accusations of sharing data with the Party, the platform has been very transparent and accountable in its data handling. This is primarily demonstrated in Project Texas (implemented in the U.S.), which established that Oracle, a trusted American company in Austin, Texas, would store American data Additionally, this company would be monitored by an internal committee called TikTok U.S. Data Security, which would need approval from the U.S. government (Silva, 2023). Project Clover has a similar logic but was implemented in the EU. These projects respond to data localization mandates, or as defined by Daskal and Sherman: *"the required storage of certain kinds of data in certain geographic locations"* (Daskal and Sherman, 2020:7).

3.2 European Union: Legalization and the GDPR

Unlike China and its isolationist and prohibitive logic, EU data legislation understands that the storage and processing of personal data by private companies are necessary conditions for the functioning of the internet nowadays, and therefore is based on creating a legal framework that, without prohibiting such practices, safeguards user rights.

The General Data Protection Regulation (GDPR) is the European Union's data protection law that came into effect in 2015, centered around the concept of consent. This principle ensures that activities related to the processing, storage, transfer, and deletion of personal data are carried out ethically and legally. Consent is defined as the voluntary and conscious authorization that individuals give for their data to be used by third parties, such as companies, organizations, or government entities. It is important that this consent is clear, informed, and freely given, without coercion from the data processing company.

In addition to consent, there are other legal mechanisms that contribute to protecting individuals' privacy. These include the right to be forgotten, which allows people to request the deletion of personal data that is no longer necessary or accurate. There are also security breach notifications, which require organizations to inform individuals about any security breaches that may affect their personal data. Likewise, mandatory privacy impact assessments help identify and mitigate potential privacy risks before carrying out certain data processing activities. Finally, the implementation of "privacy by default and by design" ensures that privacy protection is integrated into all aspects of system and service design and operation from their initial conception. These combined mechanisms provide a robust legal framework for ensuring user safety in the digital environment (Cababie, 2017:14).

The EU has also implemented the Digital Markets Act (DMA) to address the market dominance of large tech companies that benefit from the aggregation of data. These multinational corporations, often referred to as "gatekeepers," are subject to a set of rules and regulations aimed at changing the way they operate within the EU. The goal is to create a more equitable and competitive digital environment. These companies operate within the framework of capitalism, seeking expansion into new markets to generate profits from thousands of consumers. Therefore, they are willing to adapt to new regulatory frameworks, like the DMA, to maintain their operations in certain regions.

While China (and now possibly the U.S.) stands out for "punishing" apps with access bans, thereby reducing their market share, the EU has mostly adopted the approach of imposing fines. According to the International Network of Privacy Law Professionals, there have been a

total of 311 fines imposed by EU countries on large tech companies, including penalties of up to 405 million euros for Instagram and 14.5 million euros for TikTok. However, if the goal is truly to protect data, do these penalties effectively achieve that, or do they simply allow the company to continue operating as usual after paying the fines? According to Atkin (2023), this process is more taxative than punitive, as the fined companies generate billions of dollars in annual revenue, and the fines function more like a tax that does not inflict significant harm on the company. If we consider this perspective, the only legal system that truly protects its citizens' data from foreign forces is China's isolationism. However, considering the informational authoritarianism that characterizes it, we cannot guarantee that the underlying objective of this policy is not to control the information that enters rather than the information that leaves. Additionally, is users' data truly protected if it is stored and used by the state rather than a company?

3.3 United States: Private-public alliances protecting against foreign access

The slower pace of the U.S. in creating user data protection laws can be attributed to its focus on ensuring dominance of its national private sector in the internet realm. However, this approach overlooked the inevitable rise of foreign platforms, which resulted in the introduction of more laws like the Patriot Act and the Cloud Act. These laws grant the state authority to collect data from American citizens with the collaboration of big tech companies and facilitate cross-border data transfers for investigative purposes. While these are framed as national security policies, they paradoxically compromise data privacy and facilitate its widespread circulation among more actors. (Aitken, 2023:20)

Because the US first approach was asserting its internet governance power through its private sector, the line between the private and the public sector has become blurry. This results in differential treatment of American-owned platforms like Facebook and foreign-owned ones like TikTok. Meta's perceived threat stems from potential vulnerabilities in its platform, which raises concerns about its susceptibility to hacking. Mark Zuckerberg has close ties to the U.S. Congress and the latter has even consulted him on his opinion regarding regulating internet platforms. In contrast, TikTok is viewed as a national security risk because of its Chinese origin, which raises fears of data sharing with the Chinese Communist Party and potential influence on U.S. electoral processes.

This dichotomy is reflected in Trump’s stance on the TikTok issue. In 2020, during his presidency, he advocated for banning TikTok due to concerns about national security and data

privacy. However, he now opposes the TikTok ban, arguing that it would unfairly benefit Facebook and other liberal platforms that engage in similar data handling practices. Trump perceives the ban as direct interference in business operations, which he views as inconsistent with the values of the free market economy that the U.S. has always championed. This stance is supported by figures like Elon Musk, CEO of X (formerly Twitter).

4. Conclusions

In conclusion, the debate surrounding the TikTok ban reflects a multifaceted interplay of geopolitical tensions, regulatory frameworks, and the evolving role of digital platforms in shaping global discourse. The passage of the U.S. TikTok ban bill underscores the heightened rivalry between the U.S. and China, extending beyond traditional domains into the digital realm. This rivalry is not merely about market competition but also about asserting influence over international narratives and public opinion spaces.

The emergence of TikTok as a powerful political tool highlights the growing significance of digital platforms in shaping political discourse and influencing public opinion, particularly among younger demographics. Algorithms play a crucial role in determining the content users see, raising concerns about their potential to manipulate political discourse and influence electoral processes.

Moreover, the regulatory approaches adopted by different regions, such as China's isolationist model, the EU's emphasis on data protection and privacy, and the US's focus on private-public alliances, reflect varying priorities when addressing the challenges posed by digital platforms. While each approach has its strengths and weaknesses, the ultimate goal remains the preservation of national sovereignty in the digital globalization age.

Surijon, Mora (2024) The US TikTok Ban bill: Analyzing US-China Tensions and Regulatory Frameworks for Big Tech Multinationals. The Mathurin Hybrid Initiative, Global Economy & Diplomacy, 1-8; https://www.mathurinhybridinitiative.org/global-economy-diplomacy

References

Cababie, P. (2017) Análisis de la Política de Protección General de Datos en Europa (GDPR – General Data Protection Regulation) Consecuencias, Compatibilidad, implementación y casos particulares de GDPR.

Daskal, J., & Sherman, J. (2020). Data nationalism on the rise: the global push for State control of data. Data Analyst.

Ertuna, C. (2023). "Tiktokisation" of the war: How the war in ukraine was covered on the social media entertainment platform. In Mapping Lies in the Global Media Sphere (pp. 75-92). Taylor and Francis.

Hale, E. (2024). "Why has the US passed a bill to ban TikTok, and what's next?", Al Jazeera. Available from: https://www.aljazeera.com/news/2024/3/14/why-has-the-us-passed-a-bill-to-ban-tiktok-and-whats-next

INPLP, International Network of Privacy Law Professionals, GDPR Fines Database - List of Fines. Available from: https://gdpr-fines.inplp.com/list/

Jiang, M. (2010) Authoritarian Informationalism: China's Approach to Internet Sovereignty, SAIS Review of International Affairs, 30 (2), 71-89

Maheshwari, S., McCabe, D. and Karni, A. (2024) "House Passes Bill to Force TikTok Sale From Chinese Owner or Ban the App", New York Times. Available from: https://www.nytimes.com/2024/03/13/technology/tiktok-ban-house-vote.html

Melin, E. (2021). China's sharp power through TikTok : A case study of how China can use sharp power through TikTok.

Silva, C (2023) “What is Project Texas, TikTok’s best chance to avoid a ban?”. Mashable. Available from: https://mashable.com/article/project-texas-tiktok

Tussie, D. (2015): “Relaciones internacionales y Economía Política Internacional: notas para el debate” en Revista Relaciones Internacionales.

V. L. Aitken, Robin (2023) “Data Privacy Laws & Social Media Governance: A comparative analysis of Tik Tok & Meta/Facebook using EU, US, and China’s Data Privacy Laws” on Malmö University, Faculty of Culture and Society (KS), Department of Global Political Studies (GPS).