RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg No. 019 – 3 February 2025

A Better Fix for TikTok: Not a Ban or Sale, but a Comprehensive Federal Data Privacy Law

By Stefanny Nathaliana

SYNOPSIS

The fate of TikTok is to be determined after President Donald Trump's executive order to delay the ban, but it will ultimately result in a ban or sale – neither of which resolves the alleged national security issue presented by TikTok. To effectively address concerns around TikTok, particularly the Chinese government's access to American data, the United States could introduce a comprehensive federal data privacy law à la European Union's General Data Protection Regulation as a root-level solution that protects American personal data and prevents its free distribution abroad in the first place.

COMMENTARY

After a brief termination on 18 January, newly inaugurated President Donald Trump resuscitated TikTok and brought it back to life on US territory – for now. Trump signed an executive order delaying the ban for 75 days to "determine the appropriate course forward" that would protect US national security.

The brief shutdown resulted from the TikTok ban-or-sale law, formally the Protecting Americans from Foreign Adversary Controlled Applications Act (PAFACAA). The law was introduced to address national security concerns that the video app could be a conduit for the Chinese Communist Party's propaganda and be compelled to share American citizens' private information with the Chinese government upon demand. The latter particularly stemmed from Article 7 of China's National Intelligence Law, which states that Chinese citizens and organisations must "support, assist, and cooperate" with China's national intelligence operations.

Although TikTok is currently back online, Trump's executive order does not necessarily relieve it. Why? There is a catch in the executive order: Trump's proposed

solution is a 50-50 joint venture on the video app, and if China fails to approve the deal, he warned of the possibility of significant tariff impositions. Trump may be buying time to pressure ByteDance into selling TikTok to a US company by using tariffs for leverage after China's reluctance to sell since last April. The delay does not change the fact that TikTok's fate ultimately will still end in a ban or a forced sale. Neither banning nor selling TikTok solves the app's national security concerns effectively.

America Banning or China Selling TikTok is Not Fool Proof

Restricting TikTok may reduce some national security concerns relating to the risks of the Chinese government's direct data provision and propaganda through the video app. However, it does not eliminate the possibility of the Chinese government getting American data directly and disseminating its narratives through other Chinese apps.

This challenge is already evident with the rise of another Chinese alternative, *Xiaohongshu* or RedNote. Anticipating the TikTok ban, American "TikTok refugees" have migrated to RedNote over the past weeks, making it the most downloaded app in the US. If RedNote becomes TikTok 2.0, the US must go through another round of political and legal rigmarole over banning the Chinese social media platform or getting them to sell it to an American company. The rise of new foreign apps that pose similar levels of threats would leave the US in an endless cycle of reactive policymaking.

Additionally, China could still obtain US data from other platforms such as Google and Meta. TikTok's data collection is no different from that of US tech giants, and these data can be legally sold in the open market by data brokers, which China can acquire through diverse methods.

A US partial or full ownership of TikTok also does not solve the national security concern around the app. Chinese companies, including ByteDance, are restricted from selling their algorithms to foreign entities without the Chinese government's approval. In December 2023, China revised the "Catalogue of Technologies Prohibited and Restricted for Export", which includes TikTok's data-mining algorithm. Algorithm is what makes TikTok so special over other social media platforms, much like a famous restaurant's "secret sauce".

Owning TikTok without its algorithm not only negates much of its commercial value, but the risk of it manipulating content for US users continues to persist. Besides, there is still a risk of the data flowing back to China because ByteDance's algorithm relies on access to user data. To put it simply, it is challenging to remove ByteDance – and thus the potential influence of the Chinese government – completely from TikTok.

Say that the Chinese government agrees that TikTok should be sold to a US entity with its algorithm and ByteDance should detach from its subsidiary. Even so, China can still get US data from TikTok through third-party data brokers. Additionally, as previously noted, China would not need TikTok to get American data as they are sold in the market.

Last year, the US introduced the Protecting Americans' Data From Foreign Adversaries Act (PADFFAA) – which is different from the aforementioned PAFACAA (Tik Tok law) – that prevents US adversaries from getting American data from third-

party data brokers. Although this Act has not been the main focus of public or legislative discourse, it is a critical measure supporting the TikTok law by eliminating one regulatory gap. However, there is yet another loophole that China could still exploit. Non-US adversaries do not fall under the constraints of PADFFAA. Thus, China could still obtain American data from data brokers in non-US adversary third-party countries.

What the US Really Needs: Comprehensive Federal Data Privacy Law

The current US legislation to address national security concerns around TikTok is much like prescribing medication to treat symptoms without curing the disease. All of the loopholes and regulatory gaps on the TikTok issue – particularly data collection by China – stem from one broader systemic shortcoming: the lack of a comprehensive federal data privacy law in the US.

Currently, the US only relies on a patchwork of state-level and sectoral federal laws for data privacy instead of a comprehensive federal one. The US could adopt best practices from the European Union (EU). The EU has the most comprehensive and progressive legislation for data protection, the General Data Protection Regulation (GDPR), which applies to all companies that collect and process EU data.

The absence of US federal law regulating the data broker industry allows data brokers to collect, process, and sell American data freely. With a federal data privacy law, the US could design a mechanism that regulates international data transfers with adequate safeguards. This would not be exclusive to TikTok but to Chinese, US, and other companies that process American data.

Should this be enacted, China cannot get American data directly from any Chinese app or platforms, and American user data would never leave US soil without strict regulations, even if China purchased them through third-party intermediaries. We can think of this as a root-level solution and the first protective layer that ensures American personal data is restricted at the source and prevents data from being commercially available without barriers in the first place.

The EU's GDPR offers an example by requiring companies to rely on strict protective measures, such as adequacy decisions (if the country's data protection is safe according to the EU), Standard Contractual Clauses, or Binding Corporate Rules for data transfers outside the European Economic Area. Tech giants, including Meta and Google, have already been held accountable for violating GDPR. Most recently, TikTok and other Chinese companies have also received complaints for unlawful EU data transfers to China.

Stefanny Nathaliana is a student in the MSc in International Relations programme and a Student Research Assistant at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore. Her primary research interests lie in US-China relations and security issues, with a developing focus on technology policy.