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

RSIS COMMENTARY

www.rsis.edu.sg No. 091 – 8 July 2024

What the Proposed United States' Ban on TikTok Really Conceals

By Sean Tan

SYNOPSIS

In consideration of perceived national security risks, a bill signed into law by US President Joe Biden in April 2024 would require TikTok's Chinese parent company, ByteDance, to sell the social media service to an American parent company or face a potential ban. Politicised support for and opposition to the move both obscure a wider range of problems.

COMMENTARY

Typically, a rare instance of US bipartisan support for legislation that could ban or force a sale of TikTok, a social media platform for creating and sharing short videos, would be sufficiently newsworthy. Yet, it is US lawmakers' purported security concerns – given the app's Chinese origins – which has so far prompted headline coverage.

The resulting scrutiny has been equally high-profile. Seemingly, the Protecting Americans from Foreign Adversary Controlled Applications Act (which includes apps from Russia, Iran, and North Korea in addition to China) appears to diverge from historic rulings that maintain the citizens' right to access content defined as foreign propaganda by the US government.

Notions of political censorship have sparked further unease in an already fraught "marketplace of ideas". More tangibly, users on TikTok's own Creator Marketplace have cited concerns about the impact a potential ban would have on businesses, possibly compounding economic struggles and domestic discontent.

Other critics note that there isn't yet any concrete evidence of a clandestine relationship between ByteDance, the owner of TikTok, and the Chinese government, fuelling accusations of the US government attempting to deflect attention from critical

domestic issues. Debates around TikTok have become highly politicised with viral congressional hearings further underlining the app's inseparability from the increasingly polarised geopolitics of the digital environment.

However, lurking within this environment are legitimate social media safety risks that are prone to being overshadowed by the rhetoric of politicisation and great power contestation.

A Blind Spot for Online Harms

Given the outsized influence of both great powers in the technology domain, many debates around TikTok have inevitably been Sino-US-centric. Drawing favourable comparisons with American social media platforms, proponents of the Chinese app praise it for its informative content, which ranges from the whimsical to coverage of serious issues such as the Israel-Hamas war. Regarding the latter, some observe that TikTok's Israel-Hamas coverage has provided a counterweight to US foreign policy narratives of the war, in contrast with American platforms accused of systematically censoring opposing viewpoints. Others even speculate that any cited national security concerns from US lawmakers are merely a guise for suppressing pro-Palestine sentiment.

In a similar vein, some TikTok users may view the platform positively as a bulwark against domination by US Big Tech firms, and a welcome challenge to American technological monopolies. Bipartisan proposals such as the Digital Consumer Protection Commission Act suggest that anti-monopoly measures are broadly favoured. Some argue that a TikTok ban would undo these measures by effectively allowing Meta to establish market dominance.

However, a preoccupation with the principles of fair competition can gloss over social media platforms' ability to proliferate harm regardless of their market audiences. This is particularly the case in the US, where regulatory proposals aimed at Big Tech companies have traditionally been antitrust-oriented. Just as positive depictions of Facebook as a credible information source during the Arab Spring belied its subsequent roles in spreading misinformation, a selective analysis of TikTok's coverage misrepresents genuine dangers, such as the spread of coordinated wartime falsehoods from pro-Russia accounts, and the platforming of far-right movements leading up to elections.

Moreover, while American and Chinese platforms may diverge in their editorial viewpoints, apps from both countries have been strongly linked to very similar – and significant – safety issues relating to the online exploitation of minors. While there are legitimate arguments about preventing a social media monopoly by one platform or country, this measure alone will not prevent Big Tech companies from continuing to proliferate certain risks, regardless of their countries of origin.

Overlooking Privacy Violations

In focusing on alleged ties between ByteDance and the Chinese state, politicised discussions around TikTok also tend to overlook glaring data privacy gaps, which appear on all social media platforms worldwide.

Such gaps in American social media apps are well-documented and constitute a long-standing problem for users that continues to persist. Comparable data privacy issues have been similarly entrenched in TikTok for most of its existence. Two years after secretly accessing confidential user data on iOS devices, ByteDance subsequently admitted to compromising journalists' data and IP addresses for spying purposes. While the company has pledged to adopt localised data storage practices in foreign markets, more recent investigations suggest that it continues to share overseas user data with its China-based employees.

Despite a lack of conclusive evidence to suggest malign Chinese state influence within TikTok, lax data security practices nevertheless provoke speculation about possible exploitation by state-aligned actors. However, this possibility is relevant not only for Chinese state-owned technology companies but for all companies everywhere – including the privately-owned ByteDance – that opaquely collect and share user data. In the hands of other private actors and organisations with state-aligned interests (foreign or otherwise), such data has been shown to lend itself to manipulative activity – such as influence campaigns spanning multiple nations.

Aside from technology companies' state affiliations, another pressing issue lies in the sheer leverage wielded by politically motivated private enterprises within the global information space, which enables them to strategically disseminate, prioritise, and censor information. Combined with snooping and transparency concerns, the effects of outsized private sector influence extend far beyond the US and China. Politicised Sino-US-centric perspectives risk overlooking threats posed by these companies.

What Should Be Done About TikTok?

Politicised manoeuvres to mandate a ban or sale of TikTok will not effectively address concerns about the app. High-profile attempts to ban TikTok have so far proved unsuccessful, and are likely circumventable with VPNs. Forcing a sale to an American company is also questionable, given ByteDance's ongoing joint ownership by American investors, and the fact that TikTok user data have already been hosted on US cloud systems such as Oracle.

Two things should be done instead.

Firstly, rather than target a single social media app, national privacy and data collection frameworks should address the larger amounts of user data that state (and non-state) actors access via hacking or data brokers. Stronger privacy measures would include mandating opt-in (as opposed to opt-out) consent for personal information sharing, as well as greater accountability mechanisms for data brokers that collect and sell confidential information.

In this regard, the February 2024 executive order preventing the transfer of American users' sensitive data to certain countries represents a more logical move. However, it fundamentally fails to address the disproportionate sway that private firms hold over the flow and suppression of information, particularly after acquiring user data.

Secondly, social media platforms must be subject to more stringent transparency and due diligence requirements regarding how content is disseminated and moderated.

These requirements must apply both to social media platforms' own content moderation teams, as well as any partnerships between these teams and other external organisations. This would ensure adequate scrutiny of how private organisations disseminate information, and in turn, prevent them from becoming content "gatekeepers".

Although some of these regulations already exist in some form in other jurisdictions, American lawmakers may question why similar expansive measures are not already in place in the US. The heavily politicised nature of debates around Big Tech regulation represents a significant hurdle, as Sino-US-centric discussions only provide a very narrow analysis of an otherwise comprehensive range of important safety issues. Though growing domestic polarisation and division are undoubtedly significant, these concerns can be easily deepened further if fundamental social media safety issues are not properly addressed or acknowledged first.

Sean Tan is a Senior Analyst at the Centre of Excellence for National Security (CENS), a constituent unit of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore. Before joining CENS, he was based at NTU's Centre for Information Integrity and the Internet (IN-cube), a research centre that aims to help promote information integrity in online spaces.

S. Rajaratnam School of International Studies, NTU Singapore
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798