Insight

New Executive Order Starts the Clock on Potential TikTok Ban

JENNIFER HUDDLESTON | AUGUST 7, 2020

Executive summary

- New executive orders from President Trump would ban any U.S. person or company from transacting with Chinese company ByteDance (including its popular social media product TikTok) and Tencent (the company behind chat app WeChat).
- While consumers should be aware of the ties to China and the data collection practices of the social media they use, there are less severe ways to resolve national security concerns surrounding TikTok.
- Banning an app via executive order is novel in the United States, and this move could splinter the internet and set concerning precedent for government action in this market.

Analysis

Last night, President Donald Trump signed executive orders that would ban Americans and American companies from transacting with Chinese technology companies Tencent (aimed at the app WeChat) and ByteDance, including the increasingly popular app TikTok, in 45 days. These orders would effectively ban the use of these apps in the United States. To do so, these executive orders invoke authority under the International Emergency Economic Powers Act and state that additional steps must be taken to deal with the "national emergency" posed by these apps. This action follows many statements by President Trump, Secretary of State Mike Pompeo, and members of Congress about the potential national security risks posed by TikTok. These potential risks could have been alleviated in more targeted ways, however.

Over the past few months, TikTok has become an increasingly popular social media platform particularly with teenagers and young adults. Currently the app is the sixth largest social network and the most downloaded app of 2020. But as its popularity has grown, so have concerns about the app's ties to China and whether the data of its American users could be accessible to the Chinese government.

The exact risk of TikTok data being made available to China is not known. Because its parent company ByteDance is based in China, many have expressed concerns that the Chinese Communist Party would be able to pressure the company to turn over user data including information on American users, based on China's National Intelligence Law. This scenario is highly concerning given the Chinese government's use of data to limit and control its own citizens as well as the risk of what information the Chinese government might be able to obtain from other parts of the world via user data. These data include information about a user's device, network, and location as well as the photos and other information contained in the content uploaded. As TechFreedom's Ashkhen Kazaryan wrote, "We should call a spade a spade: TikTok is a Chinese company, and its track record and immense data collection presents a danger to Americans and democracy. We know what it does with data collection in its own country—it violates human rights in part by operating a mass censorship and surveillance apparatus against its own people."

TikTok has attempted to distinguish itself from its parent company to alleviate some of these concerns. Both TikTok and parent company ByteDance have said that they are not providing data to the Chinese government and would not comply with such requests. But other actions give more validation to national security concerns. For example, in a recent class action lawsuit, the company argued that while it is currently not sending biometric data on its users to servers in China, it could transfer any of its data to its servers in Beijing at any time without violating the law. Such actions would make this data more vulnerable to request from the Chinese government. And while the company shut down its Hong Kong operations rather than comply with China's new data collection and national security law for the city, its content moderation practices block conversation on numerous topics offensive to the Chinese Communist Party including suspending the account of a U.S. teenager who criticized the Chinese government's treatment of Uighur Muslims .

But there are many ways that policymakers could address these concerns without completely banning the app. For example, both the Army and the Navy banned the use of the app on government-issued devices in late 2019 over these security concerns. Earlier this week, the Senate unanimously passed legislation that would ban the app from all government devices. These more targeted approaches can minimize the national security concerns until more information is known about the actual risks of data being accessed by China or until changes to the company structure might alleviate these concerns. Such actions would be aligned with the response to similar security concerns regarding Huawei. Private companies could take similar actions to protect their own networks and data if they felt the current security risks posed by TikTok were serious enough.

Recently it has been indicated that Microsoft would be acquiring at least certain elements of TikTok's operations and allow the app to still be available to American users. This transaction might alleviate many of the national security concerns, but it is not a clear cut or easy answer. Microsoft would only acquire a regional portion (including the United States) of the social network, and it is unclear how that division would impact interactions with other portions (including Europe) and the feasibility of such a split. It is also unclear if this division would exacerbate concerns over the balkanization of the internet as countries decide to ban or allow specific apps or practices. Furthermore, this could result in effectively de facto data localization requirements and their unintended consequences if to continue operations such apps are not only prohibited from storing data in Beijing but face farther requirements. splintering of the internet as countries decide to ban or allow specific apps or practices. Furthermore, to enforce such a split could result in de facto data localization requirements and their unintended consequences if, to continue operations, such apps are not only prohibited from storing data in Beijing but face further requirements regarding their data storage.

The effects of a TikTok ban may extend far beyond just the app itself. Overly broad responses such as a complete ban on Americans using the app could call into question America's hands-off approach to technology that has allowed a free market to flourish. As Axios reporter Scott Rosenberg notes, a TikTok ban could undercut reputational advantages and "squander the U.S.'s high ground as a champion of fair markets and networks." The Electronic Freedom Foundation argues a ban on TikTok and WeChat has potential First Amendment concerns for both the users and the app stores on which it is distributed. And following other executive orders and statements, such an action increases concerns about the degree to which the government is seeking to intervene in social media.

The latest executive order attempts to respond to concerns about national security. Consumers should carefully consider if they are comfortable with the unique risks involved with TikTok when choosing whether to use the app. Nevertheless, a more targeted policy approach would be better than a complete ban. Such an approach would balance the potential national security risks while continuing the competitive approach to technology that has allowed innovation to flourish and new entrants to compete with existing tech giants.