BROOKINGS

Commentary TechTank

TikTok bans won't guarantee consumer safety

Darrell M. West and Mishaela Robison Thursday, February 16, 2023

Recent weeks have seen bans on the video platform TikTok from a variety of entities. President Joe Biden recently signed legislation that includes a provision banning the application from phones and computers issued by federal agencies. In addition, a dozen states such as Alabama, Maryland, New Hampshire, Texas, and Virginia have implemented similar prohibitions on devices used by their employees. Similarly, numerous universities such as Auburn, University of Georgia, Boise State, University of Iowa, University of Oklahoma, and the University of Texas have banned the app on university-issued phones and from campus Wi-Fi networks. And bans such as these are far from a new concept for American institutions.

While there is an array of possible explanations for these prohibitions—for instance, critics warn the app's algorithms amplify misinformation and disinformation, distort societal discourse, and compromise confidential information—the most cited rationale is national security. The reason behind these concerns is as follows. The app is run by ByteDance, a Chinese-owned company, which has led to widespread fears about national security risks, the sharing of confidential information with foreign officials, and the protection of personal privacy.

Further, Chinese companies certainly warrant detailed scrutiny given the Chinese government's move toward tight control of its own population and surveillance of people in other countries. But Americans should keep in mind that TikTok's connection with China is far from an anomaly in the market; many US firms either manufacture in China or rely upon components developed in China.

How we got here

TikTok has previously attempted to address security concerns through various approaches, such as moving data from American users to servers housed in the United States. But these moves did little to allay concerns, especially when evidence came to light that U.S. user data has been shared with the firm's Chinese employees and the app's developers have employed keylogging tools. Last year, for example, a researcher argued that TikTok's in-app browser included tracking capabilities, which could allow them to know what a user types within that app, such as passwords or credit card information.

Now the firm is proposing a more comprehensive approach known as Project Texas, in which all data from U.S.-based users would be stored in domestic servers that are owned by the American software company Oracle. This data would not be accessible by TikTok or ByteDance employees who are located outside of the country, and TikTok would create a new U.S. data security team to handle privacy protection.

That proposal is the result of discussion with the Committee on Foreign Investment in the United States (CFIUS) and would allow this team of experts to routinely audit the data system. Still, these proposed changes are far from what lawmakers and cybersecurity experts desire.

Security practices such as these have sought to mitigate concerns. Yet, still leave open broader policy questions as to whether TikTok prohibitions are based on national security considerations or competition with foreign firms. There clearly are credible concerns, including from the FBI, regarding national security, and those in support of the application's security handling like the detailed analysis by researchers at Georgia Tech, which concluded that the evidence of national security risks from TikTok is weak and there needs to be more detailed documentation of nefarious behavior to justify these bans. In addition, security critics need to define exactly what they mean by national security concerns.

Are TikTok's data practices different from other companies?

Several experts already have argued that TikTok bans won't make Americans safer. One reason is that much of the information collected by TikTok is like that compiled by many companies that host consumer-facing products. The app undoubtably has information on which videos users have watched, comments they have made about those items, and their geolocation while watching the videos, as well as both users' and their friends' contact information, but that is true for nearly all digital platforms and e-commerce sites around the world.

It also is the case that digital firms compile data on users, and many buy and sell consumer data via third-party vehicles. It has been estimated that leading U.S. data brokers have up to 1,500 pieces of information on the typical American, and that both domestic and foreign entities can purchase detailed profiles on nearly anyone with an online presence. Even with aggregated data, it is possible to identify specific individuals through a relatively small number of attributes, with some research estimating that "99.98% of Americans" could be re-anonymized from relatively small datasets. Still, what sets TikTok apart are the amount and type of trackers they use. Per a 2022 study utilizing Apple's "Record App Activity" feature, TikTok utilizes over twice the average amount of potential trackers for social media platforms. Almost all these trackers were maintained by third parties, making it harder to know what TikTok is doing with the information they collect.

If concerns about TikTok are around the compromising of personal information with government authorities, either in China or elsewhere, there are many firms both within the U.S. and abroad that have been accused of the same. For example, a former Twitter employee has been convicted of acting as a foreign agent for Saudi Arabia and providing confidential information from that platform about dissidents to foreign officials. Geolocation data are routinely bought around the world by data brokers and repackaged for sale to advertisers, governments, and businesses around the world.

Regarding concerns that Chinese companies operating within the U.S. are beholden to Chinese laws, the same can be said of American companies that operate in China. Some observers have expressed worries about Tesla vehicles being made in China for some of the same reasons, and what the company may have to do to maintain good relations with Chinese officials. Furthermore, if the criterion for bans based on national security is access to users' confidential information, there is a long list of American and foreign companies that face security challenges via their Chinese operations. As examples, many digital products sold domestically are made in China. And a wide variety of smart appliances, pharmaceuticals, personal protective equipment, computer chips, and other products are assembled there.

TikTok's standing among social media

Regardless of the rationale for U.S. bans, it is undeniable that TikTok has a large user following. The app has around 1.9 billion monthly global users, with 100 million monthly users in the United States alone. The app is particularly popular with teenagers and young adults who love its easily user-generated content and off-beat videos. In addition to impacting this large user base, a ban on TikTok can equally impact people in a variety of professions, including influencers, social media managers, and tech workers who rely on their brand for product development and marketing.

Because of this, the app's enormous popularity has proved challenging for American social media firms that seek to compete with it. A host of domestic companies have sought to develop alternative services but have not reached the same audience or user engagement as TikTok. Corporate executives have long had concerns with TikTok. Yet, if corporate competition rather than national security is the problem, part of the solution may be for these firms to cultivate and foster innovation that effectively competes with TikTok in the marketplace, especially around consumer engagement.

In the end, if policymakers are serious about addressing Chinese security risks, they should limit the ability of commercial data brokers to sell information to adversarial foreign entities (or their intermediaries), in general. Even if TikTok did not exist, China could purchase confidential information on U.S. consumers from other companies and use that material for nefarious purposes, creating similar national security challenges. The U.S. needs stronger overall platform governance and data privacy regulation to mitigate problems not just from TikTok but from social media platforms overall.