Insight

Primer: Banning TikTok

JOSHUA LEVINE | APRIL 11, 2023

Executive Summary

- Congress and the White House are increasingly concerned about the potential threats posed by TikTok, a wildly popular video-sharing social media platform owned by ByteDance, a Chinese technology firm with ties to the Chinse Communist Party (CCP).
- Both Congress and state legislators have introduced bills that range from a blanket ban on TikTok to restricting the app on government devices, citing national security concerns and the potential for the CCP to use the app to manipulate Americans.
- While TikTok's affiliation with ByteDance may present legitimate security concerns, banning the app raises significant constitutional questions, could create justification for further bans on foreign technology, and may fail to prevent Chinese firms or the CCP from collecting Americans' data.

Introduction

TikTok, a video-sharing social media platform that recently eclipsed 150 million active U.S. users, has come under scrutiny in recent years due to potential national security concerns. Much of these concerns are associated with the application's parent company ByteDance, a Beijing-based technology company that employs executives with ties to the Chinese Communist Party (CCP). Millions of Americans use the app to share information and connect with people across the globe, but U.S. officials warn that the firm could potentially collect and share sensitive user data with the CCP, as well as serve as a propaganda arm for the party.

Congress has presented a range of options in response to concerns about TikTok's data collection and ByteDance's connections to the CCP. Some bills would empower the president to limit foreign investment in technology companies and products with operations in the United States. Other bills would simply ban the use of the app on federal devices and for government employees, an approach widely pursued by the executive branch, Congress, and state governments. Finally, some bills would significantly restrict TikTok, and even ban the app entirely.

With bipartisan, bicameral support for legislation to ban or restrict TikTok, Congress should consider the most appropriate path forward. An outright ban of the application, however, would present significant concerns and challenges. First, a ban would face significant legal hurdles and constitutional scrutiny. Second, such a ban could create precedent for further technology bans, which could promote a perverse incentive to use national security as a justification for technological and economic protectionism. Finally, it remains to be seen if a ban on TikTok would actually prevent a Chinese company or the CCP from acquiring Americans' personal data.

This primer discusses the security concerns presented by TikTok, legislation proposed to address these concerns, and some of the problems with banning TikTok in the United States entirely.

Potential Threats Posed by TikTok

TikTok is a wildly popular social media platform, especially among American teens and young adults, who are increasingly choosing TikTok over incumbents such as Facebook and Twitter. The application allows users to post short-form videos that are aggregated and served to other users. Due to the nature of the content and the effectiveness of the company's recommendation algorithm, TikTok has quickly become one of the most popular social media platforms, boasting 150 million U.S. users.

Yet there are significant concerns with the app's popularity. While TikTok is headquartered in Singapore and Los Angeles, the platform is owned by Beijing-based ByteDance, a firm with extensive ties to the CCP. Lawmakers, regulators, national security professionals, and law enforcement have all sounded the alarm on the platform's connection to the Chinese government. While problematic in isolation, Chinese laws also require that Chinese firms and individuals assist Chinese intelligence services when asked for private data, ensure that the military and law enforcement can access firms' networks, data, and communications, and include CCP representatives within their firms. TikTok's CEO has tried to distance his company from the CCP, but many have noted how these obligations could present a national security threat.

Of note, lawmakers are concerned that the CCP could compel TikTok to turn over Americans' user data. TikTok collects personal and geolocation data on users' devices, tracks which videos individuals watch and share, uses first- and third-party trackers for targeted advertising, and employs audio fingerprinting to identify users. This type of widespread data collection is integral to the CCP's "Digital Silk Road," an initiative to drive Chinese competitiveness in digital technology globally. While other apps and digital platforms collect similar types of data on users, the connections between ByteDance and the CCP have prompted widespread concern regarding how this information may be used.

In addition to the specific risks to Americans' data, some fear the CCP could weaponize TikTok to assist in foreign influence campaigns and covertly advance party priorities. Specifically, some have raised concerns that TikTok's algorithm could be used to manipulate the information Americans see on the app to the benefit of the CCP. While TikTok claims it is a private company and would never act in such a way – and some researchers have pushed back on claims of weaponization – legitimate concerns remain.

Proposed Legislation

In response to these concerns, lawmakers have proposed several bills to curtail TikTok's use.

First, there have been efforts to ban TikTok on the devices of government employees or in certain institutions, such as universities. Congress banned TikTok from government devices in December 2022, with the White House issuing guidance for federal agencies in February 2023. This action complements widespread state efforts to ban the app on state government devices and networks. Another bill recently proposed would prohibit the use or presence of TikTok on devices in universities that receive federal funding.

Lawmakers are also considering legislation that would restrict Americans' access to TikTok and other apps affiliated with ByteDance. To that end, both houses of Congress have introduced the bipartisan Averting National Threat of Internet Surveillance, Oppressive Censorship and Influence, and Algorithmic Leadership by the Chinese Communist Party Act (ANTI-CCP Act), as well as the No TikTok on United States Devices Act. These bills would vest the president during peacetime, and without a national emergency being declared, with the power to "block and prohibit all transactions in all property and interests in property of a covered company" under the International Emergency Economic Powers Act (IEEPA), a law that allows the president to take action against an "unusual and extraordinary threat." The "covered company," in this case, would refer to

TikTok, ByteDance, a successor to ByteDance, and any entity owned by ByteDance – such as CapCut, a video editing app, and Hypic, an image editing app – that shares data with the firm or any subsidiaries. While the bills' definitions of covered entities are not identical, both would still allow the president to unilaterally ban TikTok and other ByteDance-owned firms from operating in the United States.

Lawmakers are also considering the Deterring America's Technological Adversaries (DATA) Act, introduced in the House in February. Complementing the ANTI-CPP Act and the No TikTok on United States Devices Act, the DATA Act would also direct the president to use IEEPA to target TikTok, ByteDance, and other entities with similar connections to the CCP. The DATA Act differs by removing user data from existing exemptions laid out in the IEEPA, known as the Berman Amendments, which prohibits the U.S. government from suppressing information flowing to, or coming from, foreign entities. Functionally, this would allow the president to prevent any app, platform, entity, or individual with connections to China or a Chinese firm from importing or exporting Americans' data.

Finally, lawmakers are considering a broader approach to regulating TikTok with the Restricting the Emergence of Security Threats that Risk Information and Communications Technology Act (RESTRICT Act). This bipartisan legislation has been introduced in the Senate and has garnered support from the White House. The bill would empower the secretary of the Department of Commerce in consultation with cabinet secretaries to investigate firms operating in the United States that may have any financial connections to a "country of concern," including receiving financing from an individual or firm domiciled in covered countries. If the secretary of the Department of Commerce and the relevant executive agency heads decide there is "undue and unacceptable risk" from a particular relationship between a firm and a country of concern, the president has the power to compel divestment or take other "mitigation measures." Beyond targeting TikTok and ByteDance, the bill would also cover any firm or individual from a covered country involved with communications technology, hardware and infrastructure, or digital payments if they have any commercial relationships with U.S. firms or American citizens.

Potential Roadblocks and Concerns with Banning TikTok

Congress should carefully scrutinize TikTok to ensure Americans' data are protected, but an overbroad response could raise constitutional questions and cause significant harms.

First, a TikTok ban may be deemed unconstitutional on First Amendment grounds if it is focused in part on the content the app delivers to users, regardless of whether that content is promoted by the CCP. If challenged, these laws would likely have to satisfy strict scrutiny, which would require the government to demonstrate a compelling state interest, as well as that these laws are either narrowly tailored or will be the least restrictive with regard to speech. While there is a compelling interest to protect American national security, researchers have pushed back on the idea that TikTok's content is currently being used to manipulate Americans. Further, a ban may not be narrowly tailored to addressing the harms lawmakers cite, and may limit Americans' ability to use TikTok to interact with other users and share information online. If less restrictive legislation could accomplish the same objective, a court may strike down the ban as unconstitutional.

Second, banning TikTok could establish dangerous precedent regarding the banning of digital platforms generally. If Congress bans TikTok, it could create a playbook for further protectionism in digital markets. By claiming a firm is connected, or even could be connected, to a country or entity of concern, legislators could use this to pressure the executive branch to restrict market access or force a sale. The Committee on Foreign Investment in the United States (CFIUS), the body tasked with evaluating national security risks presented by foreign investments, is exploring avenues to address security concerns posed by the platform. Pushing for a ban

through legislation could undermine its process and make it easier for the federal government to target firms or individuals for much less compelling reasons.

Conversely, approaches such as the RESTRICT Act would give considerable power to the executive branch to decide what companies or individuals can participate in commerce related to American technology. This again creates an incentive to embrace protectionist policies in the name of national security or advance favored domestic industries at the expense of competition and innovation. In addition, the RESTRICT Act could imperil Americans' use of technologies such as virtual private networks and online speech, as the bill vests the executive branch with broad authority to restrict access to products or services of "foreign adversaries." What's more, attempts to circumvent such restrictions could result in monetary fines and even prison time. American national security and competitiveness is critical, but legislators should consider the perverse incentives such expanded authority could create.

Finally, there is no guarantee that a ban on TikTok would meaningfully impact the firms' or the CCP's ability to acquire data on Americans. During his testimony before Congress, TikTok CEO Shou Zi Chew noted that even if the firm is banned in the United States, it could still acquire American's data through third-party data brokers or alternative sources. Further, using open-source intelligence tools, such as data scraping other digital platforms , would allow the CCP or other nefarious actors to access troves of Americans' sensitive information. If Congress wants to protect Americans' data from foreign entities, it could consider enacting a federal data privacy standard that limits data collection writ large, ensuring that no matter what platform a user chooses, their data will be protected and secure.

Conclusion

Some legislation to protect Americans' data from foreign entities such as the CCP focuses narrowly on TikTok and ByteDance, while other proposals offer an approach that could be more broadly applied to other technologies and entities. There are legitimate concerns regarding the national security risks posed by TikTok and ByteDance, but Congress should also ensure that any response addresses the specific concerns with these companies without producing additional harms. As it stands, the bills currently under consideration raise significant constitutional concerns, could create justification for further bans on foreign technology – harming innovation and consumer welfare – and may even fail to prevent Chinese firms or the CCP from collecting Americans' data.