January 12, 2023

ISSUE BRIEF | China Policy Initiative

Alarm Over TikTok Threat Reaches Critical Mass as Government Responds

Adam Savit and Royce Hood

TOPLINE POINTS

- TikTok is a Chinese Communist Party-controlled app that serves as an ingenious data-harvesting weapon disguised as a social media platform and has become a dominant force in American youth culture.
- Widespread and increasingly bipartisan recognition that TikTok is a clear and present security threat in need of remedy has resulted in a blizzard of policy solutions, from executive action on the federal and state levels to legislation and regulatory remedies, but all have fallen short.
- An effective solution must involve a blanket ban of the app or a forced sale of all ownership to an American company.

Overview

TikTok is a short-form video content mobile application controlled by the Chinese Communist Party (CCP) as a subsidiary of Beijing-based ByteDance, Ltd. It serves as an ingenious data-harvesting weapon for the CCP disguised as a social media platform and has become a dominant force in American youth culture.

Launched in 2017, TikTok became the most downloaded app of 2020, rapidly rising in popularity during the COVID-19 lockdowns and now claiming 1 billion daily users. TikTok's universal appeal stems from its ability to serve rapid-fire, short-form video content on a vast array of topics, from beauty to sports, to politics, and its capability to constantly generate new videos for the user based on a personalized algorithm as they continue to scroll. There is always more content to consume.

Meanwhile, TikTok aggressively and surreptitiously collects data from personal devices that have downloaded and regularly use the app. According to a comprehensive study of the application and its source code by security research firm "Internet 2.0," TikTok accesses device information, including a list of all other apps installed on the phone, Wi-FI network names (SSIDs), unique phone numbers and IP addresses tied to the device or SIM card, all contacts on the device, all folders and files on the device, all calendar events on the device, and GPS information at least every hour. It also accesses and communicates with servers based in mainland China, owned by company Guizhou Baishan Cloud Technology Co., Ltd. According to the study, "the application can and will run successfully without any of this data being gathered," and thus, the only plausible purpose for collecting the information is for data harvesting.

An October 2022 *Forbes Magazine* piece revealed that the app's developers were able to, and had the intention to, target and track certain individuals in the United States, including at least two cases in which the internal audit team planned to collect data about the location of a U.S. citizen who had never had an employment relationship with the company.

In early November of 2022, a voluntary disclosure by ByteDance to its European userbase further revealed that:

> [TikTok] allows certain employees with our corporate group located in Brazil, Canada, China, Israel, Japan, Malaysia, Philippines, Singapore, South Korea, and the United States, remote access to TikTok European user data.

If this holds true for ByteDance's American userbase as well, then their data may be freely transmitted all over the world by TikTok with the approval of ByteDance for use by its employees, including those in the People's Republic of China (PRC). This would contradict explicit claims by TikTok Chief Operating Officer Vanessa Pappas in her September 2022 testimony in front of the Senate Homeland Security and Government Affairs Committee that "under no circumstances would we give [U.S. user] data to China."

Finally, in December 2022, ByteDance admitted that its employees used TikTok to improperly access the personal data of journalists from the *Financial Times* and *BuzzFeed* and used it to track them in a bid to discover who may have leaked confidential company materials.

Government Officials Gradually Awaken to the Threat

This steady flow of alarming information about TikTok that proliferated throughout 2022 has sparked a flurry of public calls for action from policymakers and elected officials at both the federal and state levels:

- In June 2022, Federal Communications Commission (FCC) Commissioner Brendan Carr sent letters to Apple and Google asking them to remove TikTok from their app stores.
- In July, Chairman Mark Warner (D-VA) and Ranking Member Marco Rubio (R-FL) of the Senate Intelligence Committee sent a joint letter to the Federal Trade Commission (FTC) urging an investigation of TikTok's data handling.

- In August, Nebraska and South Dakota announced TikTok bans on state devices, with many more states following their lead in December. See below for a list.
- In November, FCC Commissioner Carr called on the Council on Foreign Investment in the U.S. (CFIUS) to ban TikTok.
- Also in November, FBI Director Christopher Wray warned lawmakers that the Chinese government could use the app to influence users or control their devices.
- Later that month, Senator Rubio and Representative Mike Gallagher (WI-08) wrote in support of a TikTok ban in the *Washington Post* and announced that they would be introducing legislation to do so.
- In a December interview on "PBS NewsHour," CIA Director Bill Burns said that he agreed with Director Wray's assessment that TikTok is a threat to national security and that "the Chinese government is able to insist upon extracting the private data of a lot of TikTok users in this country."

Struggling for a Policy Solution

The widespread and increasingly bipartisan recognition that TikTok is a clear and present security threat in need of remedy has resulted in a blizzard of policy solutions, from executive action on the federal and state levels to legislation to regulatory remedies. The diversity of strategies reflects the complex problems presented by a dynamic and largely virtual social media platform that transcends national borders yet is effectively controlled by a malevolent state actor.

In 2020, the federal government made serious and substantive moves to remove the malign influence of TikTok. Seeing the FTC as an insufficient tool, the Trump Administration sought to use the International Economic Emergency Powers Act (IEEPA), which effectively bans any communications tool that is a national security threat to the United States and a variety of other executive instruments. The administration then attempted to compel ByteDance to divest TikTok to a U.S. company, but legal wrangling in the DC Circuit Court effectively prevented further progress.

President Biden signed a federal government employee ban into law as part of the massive 2023 omnibus bill, but his administration has relied on passive processes underway instead of initiating significant action. A 2020 Trump Administration deal came to fruition in June 2022, with U.S.-based Oracle winning a contract for data storage, but principal ownership and operation of the app remained with the U.S. subsidiaries of ByteDance with data still accessible to the main Chinese ByteDance team. Meanwhile, TikTok remains locked in a years-long review with CFIUS to determine if divestment from ByteDance to a U.S. company is possible.

Federal and state governments have quickly taken actions within their immediate purview, but their jurisdiction is generally limited to government phones issued to government employees. Unfortunately, "government device" bans do not prevent the collection of personal data via employees' personal phones, and allowing them access to government networks enables collection through the same means. The recent funding omnibus for FY2023 included a federal ban of this nature, banning the app on government smartphones. A TikTok ban on U.S. military-

issued smartphones has been in effect since 2020 while only "strongly encouraging" service members to delete it from their personal phones.

Action has been taken at the state level by a number of governors, including, as of the publication of this brief, a ban on all state devices in Alabama, Georgia, Idaho, Iowa, Kansas, Maryland, Montana, Nebraska, New Hampshire, North Dakota, Oklahoma, South Carolina, South Dakota, Tennessee, Texas, Utah, and Virginia, and a ban on some state devices in Florida, Louisiana, Pennsylvania, and West Virginia, while the matter is under litigation in Indiana. Again, these bans are applicable to state-owned devices only, not to the general public. Network access is also not prohibited, so personal devices on public universities' internet, for example, can still access the TikTok app.

Major federal legislation meant to serve as a blanket ban on TikTok was introduced in December 2022 by Senator Rubio in the Senate and Representatives Mike Gallagher and Raja Krishnamoorthi (D-IL) in the House. Entitled the "Averting the National Threat of Internet Surveillance, Oppressive Censorship and Influence, and Algorithmic Learning by the Chinese Communist Party Act" or the "ANTI-SOCIAL CCP Act," it would protect Americans by blocking and prohibiting all transactions from any social media company in, or under the influence of, China, Russia, and several other foreign countries of concern. The "CCP" branding in the title, as well as numerous public statements by the sponsors supporting a TikTok ban, indicate that the app is indeed the intended target.

Enforcement of the "ANTI-SOCIAL CPP Act" rests on the same International Economic Emergency Powers Act (IEEPA) identified by the Trump administration in 2020. This appears to put the prospects of permanent enforcement on unstable ground, as according to the Congressional Research Service, it requires a declaration of national emergency, and in fact was enacted in 1977 to limit the duration of a declared emergency when investigations found that the U.S. had effectively been in a "state of emergency for more than 40 years."

Conclusion

To protect the data security of the American government and people, there must be a blanket ban on TikTok, or it must be divorced from the Chinese Communist government through a forced sale of ownership to an American company. The ubiquity of smartphones and easy access to applications, the virtual nature of social media apps like TikTok, and the lack of effective enforcement mechanisms make this a difficult task.

The introduction of the "ANTI-SOCIAL CCP Act" is a landmark step in that it calls for a blanket ban of TikTok from all personal devices at the federal level. The powers included in IEEPA may be enough to put TikTok out of business for a period, perhaps years, while inevitable legal challenges are mounted. Even a relatively brief period out of commission would dramatically damage TikTok's currency among a low attention span youth demographic who would likely migrate to similar products produced by companies based in the U.S., allied countries, or relatively benign countries. However, the potency of enforcement is uncertain until

the bill is enacted, and the permanence of enforcement is in question as it relies on an executive order technically for temporary emergencies.

Banning the app on government phones in the federal government, military, and all states should be commended and encouraged. These measures provide victories that, although insufficient in their reach, are at least tangible and increase awareness of the problem. However, these moves only affect a few million government employees and do not account for their personal phones, which are separate vectors and may access government networks.

There is no perfect solution to this problem, so executive and legislative measures at the federal and state levels should be employed with the goal of making the space in which TikTok is allowed to operate smaller and smaller. Both above tactics are worthy, and other creative remedies should be encouraged. An all-of-the-above approach may be the best strategy for this unprecedented policy problem.

Adam Savit *serves as Director of the China Policy Initiative for the America First Policy Institute.*

Royce Hood *serves as a Policy Analyst for the China Policy Initiative at the America First Policy Institute.*