

Congress of the United States
House of Representatives

COMMITTEE ON OVERSIGHT AND REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5051
MINORITY (202) 225-5074
<https://oversight.house.gov>

July 14, 2022

The Honorable Janet Yellen
Secretary of the Treasury and
Chair of the Committee on Foreign Investment in the United States
Department of the Treasury
1500 Pennsylvania Avenue NW
Washington, D.C. 20220

Dear Secretary Yellen:

In response to concerns from Congress and key national security stakeholders based on leaked audio and internal documents, TikTok Chief Executive Officer Shou Zi Chew confirmed the company's China-based employees can access U.S. user data.¹ According to TikTok's privacy policy, the user data in question is extremely sensitive: it includes biometric identifiers, faceprints, voiceprints, browsing and search history, and even keystroke patterns or rhythms.² In light of China's data-driven monitoring and surveillance initiatives, there are unprecedented implications for the privacy interests of U.S. users in this case, and a strong possibility that TikTok poses an intractable risk to national security.

In a letter dated June 30, 2022, Mr. Chew assured a group of U.S. Senators that TikTok is creating a framework called Project Texas whereby data for U.S. users will be protected against exfiltration by the Chinese government, among other things.³ Mr. Chew further described the development of that framework as intended to resolve concerns from the Committee on Foreign Investment in the United States (CFIUS).⁴ However, the company's forced admission that U.S. user data is widely available to company officials in Beijing is at odds with previous testimony by TikTok executives who claimed Chinese employees' access to U.S. user data is strictly controlled. Leaked audio and documents make clear, it is not.⁵

TikTok's vice president also recently offered reassurance that the company has "never shared information with the Chinese government, nor would we."⁶ But that commitment is

¹ Letter from Shou Zi Chew, Chief Exec. Officer, TikTok, to Sen. Marsha Blackburn, et. al. (June 30, 2022).

² TikTok Privacy Policy (last updated June 2, 2021), <https://www.tiktok.com/legal/privacy-policy-us?lang=en>.

³ Letter, *supra* note 1.

⁴ *Id.*

⁵ Emily Baker-White, *Leaked Audio From 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed From China*, BUZZFEED NEWS, June 17, 2022.

⁶ Statement of TikTok Vice President Michael Beckerman, *Reliable Sources* with Brian Stelter, CNN (July 3, 2022).

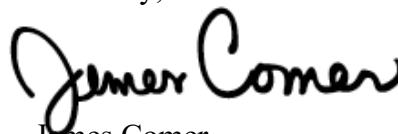
virtually meaningless because the Chinese government would not need to ask the company's permission. Whatever the agreement between TikTok and CFIUS, the Chinese Communist Party (CCP) is unlikely to consider itself bound by the terms, and a new law passed by China's National People's Congress (NPC) allows the CCP to take any data it pleases from any Chinese tech company, including TikTok's parent company ByteDance.⁷ Indeed, according to a member of TikTok's Trust and Safety department during a September 2021 company meeting, "Everything is seen in China."⁸

Many details about the ongoing negotiations between TikTok and CFIUS remain secret. The few details that Mr. Chew recently revealed, however, raise further questions. For instance, despite the ongoing nature of those negotiations, Mr. Chew appears certain that ByteDance employees in China will continue to work on TikTok, and that those employees will develop the algorithm that feeds personalized video recommendations to TikTok's users.⁹ According to Mr. Chew, some forms of sensitive information will remain available to ByteDance employees under conditions approved by CFIUS, to "ensure global interoperability so our U.S. users, creators, brands and merchants are afforded the same rich and safe TikTok experience as global users."¹⁰

The national security implications for ByteDance's inexorable acquiescence to the CCP were sufficiently compelling for U.S. national security agencies and military services to ban TikTok from government-owned devices in 2019.¹¹ TikTok's pattern of misrepresentations regarding the unfettered access that persons in Beijing have to sensitive U.S. user data further requires CFIUS to take a hard position in this case. In light of the fact that any deal between TikTok and CFIUS will have major implications for the security of sensitive data associated with the company's 80 million U.S. based users, we request a briefing on the status of the ongoing negotiations as soon as possible.

To schedule the briefing or ask any follow-up or related questions, please contact Committee on Oversight and Reform Republican staff at (202) 225-5074. The Committee is the principal oversight committee of the U.S. House of Representatives and has broad authority to investigate "any matter" at "any time" under House Rule X. Thank you in advance for your cooperation in this matter.

Sincerely,

A handwritten signature in black ink that reads "James Comer". The signature is written in a cursive, flowing style.

James Comer
Ranking Member
Committee on Oversight and Reform

⁷ Mia Ping-chieh, China's New Law Lets Government Target Tech Firms Over Data

⁸ Emily Baker-White, *Leaked Audio From 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed From China*, BUZZFEED NEWS, June 17, 2022.

⁹ Letter, *supra* note 1.

¹⁰ *Id.*

¹¹ See, e.g., Neil Vigdor, *U.S. Military Branches Block Access to TikTok App Amid Pentagon Warning*, N.Y. TIMES, Jan. 4, 2020.

cc: The Honorable Carolyn Maloney, Chairwoman
Committee on Oversight and Reform