FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, DC 20554

Brendan Carr
Commissioner

June 24, 2022

Mr. Tim Cook
Chief Executive Officer
Apple Inc.

Mr. Sundar Pichai
Chief Executive Officer
Alphabet Inc. and Google LLC

Dear Mr. Cook and Mr. Pichai,

Last week, an alarming new report shed fresh light on the serious national security threats posed by TikTok. As you know, TikTok is an app that is available to millions of Americans through your app stores, and it collects vast troves of sensitive data about those U.S. users. TikTok is owned by Beijing-based ByteDance—an organization that is beholden to the Communist Party of China and required by Chinese law to comply with the PRC's surveillance demands. Through leaked audio recordings, last week's *BuzzFeed News* report revealed that ByteDance officials in Beijing have repeatedly accessed the sensitive data that TikTok has collected from Americans after those U.S. users downloaded the app through your app stores. "Everything is seen in China," a TikTok official said in the recordings, despite the fact that TikTok has repeatedly represented that the data it gathers about Americans is stored in the United States.

I am writing the two of you because Apple and Google hold themselves out as operating app stores that are safe and trusted places to discover and download apps. Nonetheless, Apple and Google have reviewed and approved the TikTok app for inclusion in your respective app stores. Indeed, statistics show that TikTok has been downloaded in the U.S. from the Apple App Store and the Google Play Store nearly 19 million times in the first quarter of this year alone. It is clear that TikTok poses an unacceptable national security risk due to its extensive data harvesting being combined with Beijing's apparently unchecked access to that sensitive data. But it is also clear that TikTok's pattern of conduct and misrepresentations regarding the unfettered access that persons in Beijing have to sensitive U.S. user data—just some of which is detailed below—puts it out of compliance with the policies that both of your companies require every app to adhere to as a condition of remaining available on your app stores. Therefore, I am requesting that you apply the plain text of your app store policies to TikTok and remove it from your app stores for failure to abide by those terms.

TikTok is not what it appears to be on the surface. It is not just an app for sharing funny videos or memes. That's the sheep's clothing. At its core, TikTok functions as a sophisticated surveillance tool that harvests extensive amounts of personal and sensitive data. Indeed, TikTok collects everything from search and browsing histories to keystroke patterns and biometric identifiers, including faceprints—which researchers have said might be used in unrelated facial recognition technology—and voiceprints. It collects location data as well as draft messages and metadata, plus it has collected the text, images, and videos that are stored on a device's clipboard. The list of personal and sensitive data it collects goes on from there. This should come as no surprise, however. Within its own borders, the PRC has developed some of the most invasive and omnipresent surveillance capabilities in the world to maintain authoritarian control.

Last week's news report only adds to an overwhelming body of evidence that TikTok presents a serious national security threat. And as relevant to this letter it also underscores TikTok's failure to comply with the data security requirements and other terms set forth in the Apple App Store and Google Play Store policies. Some of the concerning evidence or determinations regarding TikTok's data practices include:

- In August 2020, TikTok circumvented a privacy safeguard in Google's Android operating system to obtain data that allowed it to track users online.

- In March 2020, researchers discovered that TikTok, through its app in the Apple App Store, was accessing users' most sensitive data, including passwords, cryptocurrency wallet addresses, and personal messages.

- In 2021, TikTok agreed to pay $92 million to settle lawsuits alleging that the app "clandestinely vacuumed up and transferred to servers in China (and to other servers accessible from within China) vast quantities of private and personally identifiable user data and content that could be employed to identify, profile, and track the physical and digital location and activities of United States users now and in the future."

- The *BuzzFeed News* investigation identified a "Master Admin" located in Beijing that "has access to everything" despite TikTok's claims about storing sensitive data in the U.S.

- In March 2022, a report included current and former TikTok employees stating in interviews that TikTok delegates key decisions to ByteDance officials in Beijing and that an employee was asked to enter sensitive information into a .cn domain, which is the top-level domain operated by the Chinese government's Ministry of Industry and Information Technology.

- Earlier, in 2019, TikTok paid $5.7 million to settle Federal Trade Commission allegations that its predecessor app illegally collected personal data on children under the age of 13.

- India—the world's largest democracy—has already banned TikTok on national security grounds for stealing and surreptitiously transmitting user data in an unauthorized manner.

- Multiple U.S. military branches have also banned TikTok from government-issued devices due to national security risks, including the Navy, Army, Air Force, Coast Guard, and Marine Corps.

- U.S. government officials have also urged troops and their dependents to erase the app from their personal phones.

- U.S. national security agencies have similarly banned TikTok from official devices citing national security risks, including the Department of Defense, Department of Homeland Security, and the TSA.

- The RNC and DNC have warned campaigns about using TikTok based on security concerns and the threat of officials in Beijing accessing sensitive data.

- Citing data security concerns, private U.S. business operations have also banned TikTok from company devices, including Wells Fargo.

- Once accessed by personnel in Beijing, there is no check on the CCP using the extensive, private, and sensitive data about U.S. users for espionage activities because compliance with the PRC's 2017 National Intelligence law is mandatory in China.

The concerns over TikTok are shared on a bipartisan basis by a wide range of U.S. officials, independent cybersecurity experts, and privacy and civil rights groups. For instance, in 2019, then-Senate Minority Leader Chuck Schumer and Senator Tom Cotton described TikTok as a "potential counterintelligence threat we cannot ignore." Senators Mark Warner and Marco Rubio, the respective Chairman and Vice Chairman of the U.S. Senate Select Committee on Intelligence have also expressed their concerns about TikTok, and in particular its obligation to comply with the demands of the Chinese state, notwithstanding commitments the company has made to its own users or U.S. law. Congressman Adam Schiff, Chair of the House Permanent Select Committee on Intelligence, has also warned of the inherent risks associated with the app. Numerous other Senators have expressed their concerns as well, including Senators Ted Cruz and Marsha Blackburn, who pressed TikTok's head of public policy for the Americas during a Congressional hearing last fall. Others have pointed to TikTok's policies around data collection as particularly problematic. The ACLU, for instance, has expressed concerns about TikTok's "vague" policies, especially with respect to the collection and use of biometric data.

Numerous provisions of the Apple App Store and Google Play Store policies are relevant to TikTok's pattern of surreptitious data practices—a pattern that runs contrary to its repeated representations. For instance, Section 5.1.2(i) of the Apple App Store Review Guidelines states that an app developer "must provide access to information about how and where the data [of an individual] will be used" and "[d]ata collected from apps may only be shared with third parties to

improve the app or serve advertising." Subsection (ii) clarifies that "[d]ata collected for one purpose may not be repurposed without further consent unless otherwise explicitly permitted by law." Similarly, the Google Play Developer Policy Center includes provisions covering user data, and it states that developers must disclose an app's access, collection, use, and sharing of data. The Google policies also limit use of data to the purposes disclosed.

TikTok's recent statement that it is moving U.S. user data to Oracle servers located in the U.S. does not address the concerns raised here. TikTok has long claimed that its U.S. user data has been stored on servers in the U.S. and yet those representations provided no protection against the data being accessed from Beijing. Indeed, TikTok's statement that "100% of US user traffic is being routed to Oracle" says nothing about where that data can be accessed from.

There is ample precedent for removing TikTok from the app stores too. In 2018, for instance, Apple removed an app titled Adware Doctor from the Mac App Store because it collected user data and sent it to a server located in China without user consent. Similarly, Google recently pulled dozens of apps from the Google Play Store after concluding that they used a software element that surreptitiously harvested data.

Moreover, Apple and Google have long claimed to operate their app stores in a manner that protects consumer privacy and safeguards their data. Therefore, I am requesting that you apply your app store policies to TikTok and remove it from the Apple App Store and the Google Play Store for failing to comply with those policies. If you do not remove TikTok from your app stores, please provide separate responses to me by July 8, 2022, explaining the basis for your company's conclusion that the surreptitious access of private and sensitive U.S. user data by persons located in Beijing, coupled with TikTok's pattern of misleading representations and conduct, does not run afoul of any of your app store policies.

Sincerely,

Brendan Carr