FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, DC 20554

Brendan Carr
Commissioner

13 February 2023

Dr. Jane Thomson, Secretary
Select Committee on Foreign Interference through Social Media
Department of the Senate
PO Box 6100
Parliament House
CANBERRA ACT 2600
AUSTRALIA

Dear Dr. Thompson,

Thank you for the invitation to submit comments to the Australian Senate's Select Committee on Foreign Interference through Social Media. At the outset, I commend the Senate's leadership for its attention to this important topic.[1] As one of the Commissioner's at the U.S. Federal Communications Commission, I welcome the opportunity to share my perspective and some of the lessons learned—both as to the nature of the problem and some suggested solutions.[2] Indeed, I believe that our two nations—two long-standing allies that share common values and challenges—should be closely aligned in our approaches to address this growing threat.

The issues that the Select Committee are focused on are of vital importance, as online threats from malign foreign entities present myriad challenges that can impact societies across multiple vectors. While these online threats come from a range of actors, I want to focus on one particular threat: TikTok, an application with hundreds of millions of users throughout the world that is owned by Beijing-based ByteDance. While I have a base level of concern involving social media platforms in general, there is a unique set of national security concerns when it comes to this app. That is why we are seeing countries around the world take action.

For one, TikTok officials have engaged in a pattern of misrepresentations regarding both the amount and type of sensitive data it collects as well as the extent to which that data has been accessed from inside China. For another, the flow of this non-public, sensitive data into China is particularly troubling given the PRC's track record of engaging in business and industrial espionage as well as blackmail and other nefarious actions. Indeed, U.S. FBI Director

[1] I am the senior Republican Commissioner on the U.S. Federal Communications Commission (FCC), and I have served previously as the agency's General Counsel. The FCC is an independent regulatory agency that has jurisdiction over interstate and international communications by radio, television, wire, satellite, and cable. My full bio is available at https://www.fcc.gov/about/leadership/brendan-carr#bio.

[2] With this submission, I will be addressing Terms of Reference a-c, e. *See* Select Committee on Foreign Interference through Social Media, Terms of Reference, https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Foreign_Interference_Social_Media/ForeignInterference47/Terms_of_Reference.

Christopher Wray, in a rare, joint appearance with his MI5 counterpart last July, stated that "the Chinese government . . . poses the biggest long-term threat to our economic and national security" and the CCP is "set on using every tool at their disposal" to achieve its ends. He recently reiterated these sentiments in testimony before the U.S. Congress, noting that the FBI has serious national security concerns with TikTok.

Many Americans—and citizens of the world outside China—have not been viewing TikTok as a national security threat. They consider it to be just another app for sharing funny videos or memes. But 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's own disclosures state that it can collect 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.[3] 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.[4] 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. And once accessed by personnel in Beijing, there is no check on the CCP using the extensive, private, and sensitive data about global users for espionage activities because compliance with the PRC's 2017 National Intelligence law is mandatory in China.

For years, TikTok officials have been asked point blank whether any of the non-public, sensitive data that TikTok collects on U.S. users has been accessed from inside China or by CCP members. And for years, TikTok has engaged in a pattern of misrepresentations. In some cases, TikTok just dodges the question altogether, stating that it does not "share" data directly with the Chinese government and that it stores U.S. data on servers located here in the U.S. and other places outside of China—an answer that has nothing at all to do with whether the Chinese government is viewing or accessing U.S. user data. In other cases, officials with TikTok's parent company have gone so far as to state unequivocally that no U.S. user data even exists inside of China.[5] In still other cases, TikTok officials have stated that only very limited amounts of data have ever been accessed from inside China and in those rare cases the data has been subject to strict controls.[6]

---

[3] TikTok, *Privacy Policy* (1 January 2023), https://www.tiktok.com/legal/privacy-policy-us?lang=en.

[4] Dan Goodin, *TikTok and 32 other iOS apps still snoop your sensitive clipboard data* (27 June 2020), https://arstechnica.com/gadgets/2020/06/tiktok-and-53-other-ios-apps-still-snoop-your-sensitive-clipboard-data/.

[5] Jeff Stone, *TikTok's security boss makes his case. Carefully.* (Aug. 27, 2020), https://www.cyberscoop.com/tiktok-lawsuit-security-questions-roland-cloutier/ (quoting Global Chief Security Officer for TikTok's parent company, ByteDance, as saying "[t]he data doesn't even exist in China, so there's a whole bunch of ways to look at this, but the biggest fundamental truths are that the Chinese government doesn't ask for it, because it doesn't exist in China").

[6] Letter from Shou Zi Chew, CEO, TikTok, to U.S. Senators Marsha Blackburn, Roger Wicker, John Thune, Roy Blunt, Ted Cruz, Jerry Moran, Shelley Moore Capito, Cynthia Lummis, and Steve Daines at 3 (June 30, 2022), https://www.blackburn.senate.gov/services/files/A5027CD8-73DE-4571-95B0-AA7064F707C1.

But according to a June 2022 *BuzzFeed News* report that obtained leaked audio from 80 internal TikTok meetings, the company's claims about protecting U.S. user data have been nothing other than gaslighting. Turns out, "Everything is seen in China," according to a TikTok official quoted in the reporting. Indeed, the *BuzzFeed News* investigation identified a "Master Admin" located in Beijing that "has access to everything" despite TikTok's claims to the contrary. Moreover, the investigation reports on an external auditor that stated, "I feel like with these tools, there's some backdoor to access user data in almost all of them." Subsequently, in a September 2022 Senate hearing here in the U.S., TikTok's COO refused to state whether the personnel accessing U.S. user data were members of the CCP.

This reporting builds on a separate investigation from March 2022 that 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.[7]

And more recently, it was reported in *Forbes* that TikTok accounts controlled by Communist China's propaganda arm targeted specific U.S. politicians with criticism and sought to undermine trust in American institutions.[8] This material was posted without any disclosure that the accounts were operated by a foreign government. Indeed, the same report found that TikTok was the "only major social media platform in the U.S. that does not label videos posted by Chinese state media entities."

ByteDance personnel, overseen by a team based in China, have now been caught red-handed using the app to spy on the location of multiple journalists that wrote negative pieces about TikTok. And they engaged in this conduct at the precise moment when TikTok was attempting to negotiate a deal with U.S. national security officials that would allow it to keep operating—in other words, at a moment when TikTok had every incentive to operate in a trustworthy manner. Indeed, a *Forbes* article provided extensive details of an illicit surveillance campaign involving journalists who were covering TikTok.[9] According to *Forbes*, "ByteDance [employees] tracked multiple *Forbes* journalists as part of this covert surveillance campaign, which was designed to unearth the source of leaks inside the company following a drumbeat of stories exposing the company's ongoing links to China." The ByteDance employees tracked the journalists by "improperly gaining access to their IP addresses and user data."

These recent news reports only add to an overwhelming body of evidence that TikTok presents a serious national security threat. Some of the concerning evidence or determinations regarding TikTok's data practices in the U.S. include: In August 2020, TikTok circumvented a

[7] Emily Baker-White, *Inside Project Texas, TikTok's Big Answer To US Lawmakers' China Fears* (Mar. 10, 2022), https://www.buzzfeednews.com/article/emilybakerwhite/tiktok-project-texas-bytedance-user-data.

[8] Emily Baker-White & Iain Martin, *On TikTok, Chinese State Media Pushes Divisive Videos About U.S. Politicians* (Dec. 1, 2022), https://www.forbes.com/sites/emilybaker-white/2022/11/30/tiktok-chinese-state-media-divisive-politics/?sh=72eb0a04bf09.

[9] Emily Baker-White, *TikTok Spied On Forbes Journalists* (Dec. 22, 2022), https://www forbes.com/sites/emilybaker-white/2022/12/22/tiktok-tracks-forbes-journalists-bytedance/?sh=12686d8c7da5.

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

Thankfully, over the last few years, many entities in the U.S.—public and private—have taken notice and are taking action. For example, multiple U.S. military branches have 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, though TikTok continues to be prevalent on service members' personal devices.

Beyond the military, 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. And just last month, in the most comprehensive move to date, legislation was enacted that will ban TikTok from all federal government devices. While at the state level, as of today, nearly 30 U.S. states have banned TikTok on government-issued devices and networks. Citing data security concerns, private U.S. business operations have also banned TikTok from company devices, including Wells Fargo. And internationally, 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. While in the Netherlands, government agencies have been directed to suspend use of TikTok due to data privacy concerns.

Moreover, the U.S. 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." Subsequently, Senators Mark Warner and Marco Rubio, then the respective Chairman and Vice Chairman of the U.S. Senate Select Committee on Intelligence, asked the Federal Trade Commission to promptly launch a federal investigation based on TikTok's apparent misrepresentations about the scope and extent of data flowing back into China, as well as TikTok's relationship with ByteDance—which, according to some reports, has more than one hundred CCP members embedded in that organization's Beijing office alone. U.S. Director of National Intelligence Avril Haines, a high-ranking member of the Biden Administration, has warned that parents should be concerned about their children's personal data and privacy in the face of TikTok's connection to the CCP. And recently, bipartisan legislation was introduced in the U.S. House of Representatives and U.S. Senate that would ban TikTok outright in the United States.

Despite the increased scrutiny surrounding TikTok's data practices, it is deeply concerning that TikTok officials continue to mislead the public about its data collections. For instance, one TikTok executive stated in a CNN interview that "faceprints . . . is not something that we collect." Yet TikTok's own privacy policy—most recently updated on 1 January 2023—lists "faceprints" on its "What Information We Collect" page.

TikTok's statement that it is moving U.S. user data to Oracle servers located in the U.S. does not address the serious national security 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. And TikTok's 30 June 2022 letter to Republican members of the U.S. Senate is similarly wanting. Far from assuaging the Senators' concerns, the letter confirms that U.S. user data has—and will continue to be—accessed in China and that the TikTok platform relies on the algorithm and software developed by ByteDance. Moreover, TikTok itself has thrown cold water on the idea that U.S. user data will be adequately protected under any new arrangement, with one employee stating that "[i]t remains to be seen if at some point product and engineering can still figure out how to get access, because in the end of the day, it's their tools[.] They built them all in China," according to *BuzzFeed News*' reporting.

Last year, given TikTok's pattern of misrepresenting data flows, I called on Apple and Google to apply their 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. Indeed, there is ample precedent for removing TikTok from the app stores. 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. Despite this, TikTok continues to be available on Google and Apple. However, there is no reason that any country needs to bet its national security on certain companies choosing to do the right thing when it comes to TikTok. As noted above, the U.S. has already taken some steps to limit TikTok's domestic reach—many such steps could help inform Australia's approach to TikTok—but more action is required.

In the end, there are many popular apps with no ties to Communist China that sweep up a vast amount of personal and sensitive data, yet there are many factors discussed herein that provide reasons why TikTok is far more alarming than your average app. Indeed, entities that are beholden to the PRC—like the ones in TikTok's ownership chain—are not capitalist entities that are pursuing a profit motive. In the main, the only entities that are allowed to exist inside China are those that the CCP feel comfortable are carrying out its authoritative aims. That is why I support banning TikTok in its current form in the United States, a step that I believe Australia should take as well.

Indeed, the conversation on the security threats posed by TikTok in Australia is well underway. There are already calls in the Australian Senate to ban TikTok and the Department of Home Affairs has been ordered to investigate the data harvesting practices of TikTok, WeChat, and others. And across the Australian government, agencies are banning the use of TikTok on

official devices. The work of the Select Committee will no doubt contribute to these efforts, and I stand ready to provide any additional assistance that may benefit the people of Australia.

Sincerely,

Brendan Carr