TESTIMONY OF BRENDAN CARR
COMMISSIONER, FEDERAL COMMUNICATIONS COMMISSION

BEFORE THE SUBCOMMITTEE ON NATIONAL SECURITY
OF THE UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON OVERSIGHT AND REFORM

"PROTECTING MILITARY SERVICEMEMBERS AND VETERANS FROM FINANCIAL SCAMS AND FRAUD"

JULY 13, 2022

Chairman Lynch, Ranking Member Grothman, and distinguished members of the Subcommittee, thank you for the invitation to testify. It is an honor to appear before you today and alongside officials from the Federal Trade Commission, the Consumer Financial Protection Bureau, and representatives from non-profit organizations.

The issues that this Subcommittee focuses on are of vital national importance. And I welcome the chance to testify on the online threats that our active service members, veterans, and their families face. Too often, those who have dedicated their lives to defending this country are the targets of financial scams and other frauds. According to AARP—which is well represented at the hearing today by Mr. Broussard—the military community is both targeted and suffers financial loss at higher rates than the civilian population. In 2020, the FTC reports that military consumers filed nearly 175,000 complaints—including fraud, identity theft, and other scams—with loses totaling $122 million.

At the FCC, we have long worked to help America's military members avoid benefits and other scams. So I am pleased to join this group of witnesses in identifying solutions to the fraud that is plaguing the military community.

While the online threats that our service members, veterans, and their families face come from a range of vectors, I want to focus on one particular threat today in my testimony: TikTok, an application with millions of U.S. users—including service members—that is owned by Beijing-based ByteDance. While many of the financial scams and frauds that we see on other online platforms are also perpetrated on TikTok, there is a unique set of national security concerns when it comes to this app. 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, FBI Director Christopher Wray, in a rare, joint appearance with his MI5 counterpart, stated just last week 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.

Many Americans—U.S. service members included—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 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.[1]

---

[1] TikTok, *Privacy Policy* (June 2, 2021), https://www.tiktok.com/legal/privacy-policy-us?lang=en.

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.[2] 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 U.S. users for espionage activities because compliance with the PRC's 2017 National Intelligence law is mandatory in China.

All of the concerns with TikTok are heightened in the context of military members, veterans, and their families. Indeed, Chairman Lynch raised many of these points about TikTok and its overseas ties in 2019 in a letter to the CEOs of Apple and Google. Chairman Lynch wrote that "[b]y collecting personal information on U.S. government personnel who have access to classified information, foreign adversaries may attempt to expose them to blackmail, tailor intelligence spotting or recruitment activities to specific targets, or exert undue foreign influence in U.S. policymaking."

Despite its vast data collection, TikTok has grown in popularity among service members, too. In just one example, U.S. service members around the world have participated in a viral TikTok trend where they upload video and audio of their barracks. Hundreds of video tours have been posted from not only multiple U.S. installations but as far afield as the United Kingdom, South Korea, Japan, Italy, Germany, and Afghanistan. You can easily find videos of military equipment and maneuvers on TikTok as well.

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.[3] 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.[4]

But according to a recent *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."

---

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

[3] 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").

[4] 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.

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.[5]

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 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." 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.

Thankfully, many entities—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. But as noted above, 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. Both 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. 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.

Moreover, 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." Most recently, Senators Mark Warner and Marco Rubio, 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.

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. Just last week, for instance, one TikTok executive stated in a CNN interview that "faceprints . . . is not something that we collect." Yet TikTok's own privacy policy lists "faceprints" on its "What information . . . we collect" page.

---

[5] 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.

TikTok's recent 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 recent, June 30, 2022, letter to Senate Republicans 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.

Given TikTok's pattern of misrepresenting data flows, I recently 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. While I am still waiting for responses from Google and Apple, there is no reason that we need to bet our national security on these companies choosing to do the right thing when it comes to TikTok. The government needs to act now. So here are just some ideas.

First, the Executive Branch agencies should bring their ongoing national security reviews of TikTok to a close and do so with the speed that this threat demands. In June 2021, President Biden issued an Executive Order that aimed to address the national security threats that apps like TikTok pose. The Commerce Department has been engaged in a review since then. Likewise, TikTok's June 30 letter suggested that the Administration—through the Committee on Foreign Investment in the United States (CFIUS)—has been in negotiations with TikTok on their data flows back into China and imposing new protections on those. For its part, TikTok's letter left the impression that CFIUS is poised to sign off on authorizing at least some sets of U.S. user data continuing to be accessible from inside of China. Particularly in light of the fresh revelations about TikTok's persistent misrepresentations, now is not the time to for the government to authorize any U.S. user data going back into China.

Second, instead of authorizing those data flows at this moment, it is time for TikTok to provide a full, public, and transparent accounting of all non-public U.S. user data that has been accessed from inside China since it launched here in the U.S. That could take place in the context of those ongoing Executive Branch reviews or through a hearing or other legislative process determined by Congress. As part of TikTok's disclosure, it must account for all the U.S. user data that may have been viewed or accessed by CCP members.

Third, I would encourage the Federal Trade Commission to take up Senator Warner's and Senator Rubio's call for a federal investigation. That investigation should proceed quickly, and the FTC should consider any interim measures necessary to protect U.S. national security while it completes its review.

Fourth, the government should address the continued use of TikTok on U.S. military installations as well any use that depicts U.S. military operations. As noted above, TikTok is not just collecting the videos that are uploaded but rather a range of sensitive location and other data. So additional actions

should be taken beyond the current bans on service members downloading the app onto their government devices.

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—and I share the concerns of many in Congress that are working right now on a national privacy framework—yet there are a number of factors discussed here in my testimony 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.

* * *

In closing, I want to thank you again Chairman Lynch, Ranking Member Grothman, and Members of the Subcommittee for holding this hearing and for the opportunity to testify. I welcome the chance to answer your questions.