IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

TIKTOK INC. and BYTEDANCE LTD., *Plaintiffs*, v. DONALD J. TRUMP, in his official capacity as President of the United States; WILBUR L. ROSS, JR., in his official capacity as Secretary of Commerce; and U.S. DEPARTMENT OF COMMERCE, *Defendants*.	Civil Case No. 20-cv-2658

SUPPLEMENTAL DECLARATION OF ROLAND CLOUTIER

I, Roland Cloutier, under penalty of perjury, hereby declare as follows:

1. I am the Global Chief Security Officer ("CSO") for TikTok Inc. For clarity, references in this declaration to "TikTok Inc." are to the U.S. corporate entity and references to "TikTok" are to the software application and business unit.

2. I submitted a declaration on September 23, 2020 to discuss TikTok's data security and source code safeguards. I now submit this supplemental declaration to respond to several of the government's assertions about our data security policies and practices in the Department of Commerce September 17, 2020 memorandum (the "Commerce Memo") that was issued in relation to the Executive Order dated August 6, 2020 regarding TikTok.

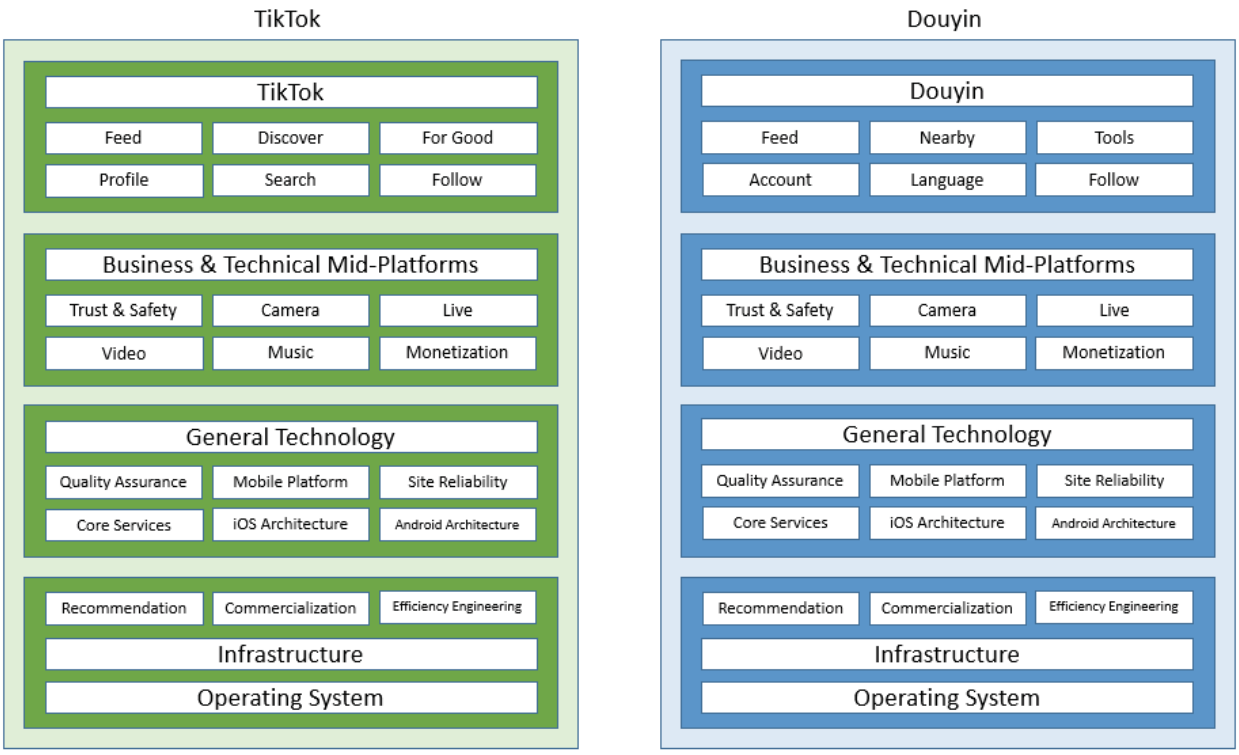
3. This declaration is based upon my personal knowledge and belief and/or upon my review of business records of TikTok Inc. and ByteDance.

A. Segregation of TikTok and Other ByteDance Products

4. On page 15, the Commerce Memo states that "the infrastructure that underlies the

TikTok application is not wholly separate from the Chinese application and the systems of ByteDance," and that "[f]unctionality including storage, internal management, and algorithms is still 'partially shared across other ByteDance products.'" These statements are not accurate.

5. Although some of the same underlying ByteDance technology is used for multiple ByteDance products, that does not mean that those products share the same infrastructure. Rather, these technological building blocks are replicated and integrated separately into each product as part of that product's independent "stack," where they are tailored to the particular product and subject to that product's security controls. The following (simplified) graphic illustrates how the same technologies are separately deployed into TikTok and Douyin (the platform similar to TikTok that is available in the Chinese market):



6. As this diagram indicates, the software stack comprising the TikTok application is entirely separate from the software stack comprising the Douyin application. That means that both the source code and user data for TikTok are maintained separately from the source code and user

data for Douyin (and other ByteDance products), as discussed in my initial declaration. Put another way, the source code for the two products is deployed separately.

B. Security Safeguards for TikTok Data in Storage in Leased Datacenters

7. The Commerce Memo asserts at pages 15-16 that TikTok leases servers from Alibaba Cloud in Singapore and from China Unicom (Americas) Operations Ltd. ("CUA") in the United States, and asserts that storing U.S. TikTok user data with these companies creates "significant risks" because of their asserted ties to China.

8. As an initial matter, the Commerce Memo's characterization of our relationship with CUA is inaccurate. CUA only provides datacenter space (i.e., the building itself and electricity) in its capacity as a reseller; it does not actually provide any server machines. Rather, ByteDance owns and operates all servers that are stored within the CUA facility. The ByteDance servers are located in a locked cage inside the facility, and CUA personnel must apply for one-time badge access each time they access the cage. ByteDance also has its own security team monitoring the technical access environment.

9. Moreover, the Commerce Memo does not address the nature of the services we are purchasing from these companies and the steps that we have taken to help protect the security of our user data when it is stored with all of the various companies from which we lease server space (which include not only Alibaba, but also Google, Microsoft, and Amazon).

10. In all instances, when we lease server space from other companies, the only things that we are purchasing are storage and computing capacity; we provide our own software environment. In particular, the operating system that runs on these leased servers is proprietary, the software stack that comprises the TikTok application is proprietary, and the logical controls that protect our software environment are proprietary. In short, the fact that server space is leased from another company does not mean that company has access to the TikTok information being

stored on the server. To the contrary, our security controls are intended to help ensure that the companies from which we lease server space do *not* have access to our software environment. These controls include alerts that would inform us if someone on the physical premises of the datacenter was seeking to access our software environment.

11. Even if someone with access to the physical premises of a datacenter that hosted TikTok data were somehow able to circumvent our software controls (something that has never happened, to my knowledge) and access our software environment, they would remain unable to extract U.S. user data. First, many categories of TikTok user data are encrypted in storage, as noted in my initial declaration, which would mean that any data extracted by such a malicious individual would be indecipherable. Second, as I explained in my initial declaration, user data in these datacenters is sharded, which means that a user's data is broken down into many pieces across many different servers. Sharding provides an additional barrier to prevent someone with physical access to the datacenters where U.S. user data is hosted from extracting TikTok user data.

C. Government Assertions Regarding Transfers of TikTok Data to China

12. On page 16, the Commerce Memo asserts that "there are indications that some data from the TikTok app may be directly transmitted to China, bypassing ByteDance's leased or owned servers altogether in 2020, Cybersecurity firm Penetrum found that 37.70% of the IP addresses the TikTok Android package kit (APK) source code connects to are based in China. An APK installs and configures an application on a phone**.** The majority of these IP addresses are hosted by Alibaba." This statement cites to a white paper published by a company called Penetrum, which purported to conduct a security analysis of TikTok.

13. In legacy versions of the TikTok application, there were Chinese IP addresses referenced in the TikTok source code that were vestiges of earlier versions of the application. As we have updated the application, this obsolete code has been eliminated. Penetrum's white paper

analyzed outdated versions of the app—the paper refers to a significant range of past versions (10.0.8-15.2.3)—and the app has frequently been updated since those versions were made available in the United States. For example, there have been 70 versions of TikTok released in the U.S. Apple app store and 86 versions of TikTok released in the U.S. Google Play app store since version 10 of the application.

14. For the current version of the app made available in the United States, this statistic regarding Chinese IP addresses is clearly incorrect. At our request, a third-party security vendor based in the United States has conducted multiple security reviews of our source code. In conducting these reviews, the vendor considered, among other things, the number of IP addresses that the TikTok application connected to in China and the nature of any such connections. These reviews of the current version of the app found that TikTok's source code referenced only four IP addresses in China, and that zero of these IP connections were active. In other words, the four IP address connections were determined to be inactive remnants left behind from outdated versions of the product, and the vendor found no actual data traffic between TikTok and these Chinese IP addresses. Our team has since further analyzed these four IP addresses and determined that two were actually pointing to servers in Singapore, and the other two did not appear in the source code itself, but rather were in code comments (annotations added by software engineers to help explain the code). In other words, of the four IP addresses identified by the vendor, there were no IP addresses pointing to China in the source code and no active connections to servers in China.

15. Lastly, the Commerce Memo on page 14 refers to language on TikTok's website to the effect that TikTok Inc. may disclose user information "to respond to subpoenas, court orders, legal process, law enforcement requests, legal claims, or government inquiries." We also make clear, however, that international authorities (i.e., non-U.S. authorities) "should use the MLAT

[Mutual Legal Assistance Treaty] or letter rogatory process to seek user information from TikTok."[1] In other words, and as explained in my initial declaration, we would not comply with a request for U.S. user data from the Chinese government. Similarly, the Commerce Memo states on the same page that although TikTok Inc. "has published transparency reports highlighting the number of requests for personal information from governments around the world," China "is notably absent from this list." The reason China was omitted is straightforward: the TikTok application is not made available in China, and as noted in my initial declaration, to date there has never been a request from the Chinese government for TikTok user data.

D. Government Assertions Regarding the Collection of TikTok User Data

16. The Commerce Memo includes several assertions about the data collected by the TikTok application, including by citing press reports on pages 18-19 to the effect that TikTok "collect[s] unique identifiers" and that it "secretly access[es] users' clipboards." Neither of these issues arose from any attempt to secretly access user data for nefarious reasons, and both issues have been resolved in the current version of the application. Below, I explain the practices that led to these outcomes and how we resolved them.

i. Unique Identifiers

17. On pages 14 and 18-19, the Commerce Memo cites a Wall Street Journal ("WSJ") article from July 2020 that reported that, in the past, "TikTok skirted a privacy safeguard in Google's Android operating system to collect unique identifiers" called "MAC addresses" from "millions of mobile devices," which "allows the app to track users online without allowing them to opt out."

[1] https://www.tiktok.com/legal/law-enforcement

18. The term "MAC address" is short for "media access control" address. It is a unique identifier that is often used to identify a particular hardware device. In prior versions of the application, TikTok used MAC addresses for analytics, advertising attribution, anti-fraud, and debugging purposes. For each of the versions of the mobile application described by the WSJ article, consumers had notice that such information was collected and the purposes for which it could be used and disclosed. As the Wall Street Journal article and the Commerce Memo observed, the current version of the application made available in the United States does not collect MAC addresses. To help avoid further collection of MAC addresses, TikTok has since been configured to drop MAC addresses that it receives from older versions of the application.

19. Most notably, from my perspective, the WSJ article does not accurately describe TikTok's use of encryption in connection with its past collection of MAC addresses. On pages 18-19, the Commerce Memo describes the WSJ article as finding that TikTok's collection of MAC addresses "was concealed through an unusual added layer of encryption, [that] appears to have violated Google policies limiting how apps track people and was not disclosed to TikTok users." The implication is that TikTok used encryption in order to obscure its practices with respect to the collection of MAC addresses and avoid being sanctioned by Google. This is not true. In fact, TikTok used encryption in this circumstance to protect the data values collected, so that malicious actors would not have a blueprint for evading TikTok's fraud prevention measures. Encryption is a common practice for preventing malicious behavior linked to fraudulent activity. Indeed, Google subsequently conducted a review to determine whether we are in compliance with their applicable policies with respect to this issue and concluded that TikTok could continue to be distributed through their app store.

ii. Clipboard

20. On page 19, the Commerce Memo raises two instances in which, according to press reports from March and July 2020, the TikTok application was able to access any data that a user had copied to the user's clipboard on iPhones and iPads.

21. By way of background, in March 2020, several press articles reported that many prominent apps, including TikTok and other major entertainment and news apps, were requesting access to users' clipboards. There are many legitimate reasons why this would occur. For example, if you copy a website URL address in one app and then open a mobile browser, many browsers will ask if you want to paste the text and go to the URL directly. This is an example of how browsers attempt to make your user experience better, but it requires the app to know that a URL is sitting on the clipboard. There are numerous other reasons why apps might want to see if information is sitting on a user's clipboard.

22. In the case of TikTok, the notification requesting access to users' clipboards had been triggered by our integration of the Google Ads Software Development Kit ("SDK") into the app. Version 7.41.0 of the Google Ads SDK contained a bug that automatically accessed text in users' clipboards when they launched the TikTok iOS App. The integration did not send users' clipboard data to TikTok, and TikTok itself did not collect, store, or use any of the data on users' clipboards. We subsequently updated our app so the Google ad program would not be able to access users' clipboards.

23. The July 2020 press reporting concerns a separate feature in the version of the TikTok app that was made available in May 2020. We are continually developing new features to improve the TikTok user experience, and in May 2020, we had been working to address the problem of spam and similar incidents where users sometimes post the same comments on hundreds of videos. To prevent this behavior, we introduced technology that allowed us to identify

users who were copying comments and placing them over and over in the comment section for different videos as part of an anti-spam feature in the iOS version of the app released on May 22, 2020. This anti-spam feature worked by performing a string matching validation from the device clipboard. Its only function was to validate whether matched text inputted into the application came from the clipboard, and clipboard data was not sent to TikTok's servers (or to any other party). All TikTok received was a yes/no signal whether the comment was likely spam.

24. Nevertheless, because users expressed concern about this feature, we sent an update to the App Store removing this feature in version 16.6.1 of the TikTok application. Google and Apple subsequently conducted reviews to determine whether we are in compliance with their applicable policies with respect to this issue and concluded that TikTok could continue to be distributed through their app stores.

Pursuant to 28 U.S.C. § 1746 and under penalty of perjury, I affirm that the foregoing facts are true and correct to the best of my knowledge.

Executed this 12th day of October, 2020.

Roland P. Cloutier