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

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.. I joined TikTok Inc. in April 2020, and my office is in Miami, Florida. Before joining TikTok Inc., I spent ten years as the Chief Security Officer at Automatic Data Processing ("ADP"), and prior to ADP I worked for an additional six years as the Chief Security Officer for EMC Corporation. I have also served as a U.S. Air Force combat security specialist, and an aerospace protection and anti-terrorism specialist for the Department of Defense.

2. My responsibilities include providing cyber risk and data security support for both TikTok Inc. and its corporate parent, ByteDance Ltd. ("ByteDance").

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. TikTok User Data Security Safeguards

4. TikTok is a software application that enables users to create and share short-form videos that is available on a range of mobile devices. There are two main current versions of the TikTok application, only one of which is currently made available in the United States. For purposes of this declaration, I focus on the version of the application that is currently made available in the United States, which I will refer to as TikTok. (Neither version of TikTok is offered in China, where ByteDance operates a similar but separate video-sharing platform called Douyin.)

5. In my role as CSO, I am responsible for overseeing the security of TikTok user data. As part of my responsibilities, I am in charge of ensuring that TikTok user data is safeguarded both when it is in transit (*i.e.*, being transmitted between user devices and TikTok servers) and when it is being stored by TikTok in the Internet datacenters where we host user data.

6. A foundation of our data security strategy is the limited scope of the data that TikTok collects, as described in our Privacy Policy: https://www.tiktok.com/legal/privacy-policy?lang=en. Among my responsibilities is to test and validate our product to help ensure that it is not collecting data beyond the categories set out in our Privacy Policy.

7. With respect to user data in transit, we use industry standard Hypertext Transfer Protocol Secure ("HTTPS") to transmit user data in a secure and encrypted manner. This is the same standard that is used by major U.S. banks and e-commerce platforms to secure their online transactions.

8. With respect to user data in storage, TikTok was designed from the ground up to have a separate network architecture from other ByteDance products and services. TikTok stores

user data on servers in datacenters in the United States and Singapore.[1] We employ logical (i.e., software-based) controls to segregate TikTok user data from any other data residing in the datacenters, and to prevent anyone with physical access to the datacenter from accessing stored TikTok user data without authorization. These controls include alerts to notify us about any attempted unauthorized access. As a practical matter, moreover, even if an unauthorized person were to obtain physical access to a TikTok datacenter, extracting user data would be unfeasible because user data is "sharded"—i.e., an individual's user data is broken down into many pieces, each comprising a fragment of data, and stored across many different servers. We regularly test and validate these logical controls to help ensure that no unauthorized access takes place. When the TikTok application stores U.S. user data, it does so in our U.S. and Singapore datacenters, and does not store any U.S. user data in China.

9. In addition to these logical controls, we also use industry-standard encryption to protect certain elements of TikTok user data in storage. Specifically, TikTok uses the key management service ("KMS") encryption algorithm (AES 256 GCM) to encrypt names, birthdays, home addresses, phone numbers, emails, passwords, PayPal account information, phone contact lists, private videos, direct messages, and the date/time of the user's log-in history in storage.

10. It is impossible to decrypt this encrypted user data without a key that has been generated and managed by our KMS, which is operated by our security team in the United States. We also have internal controls to prevent keys that decrypt this U.S. user data from being accessed by ByteDance personnel without authorization. TikTok relies on China-based ByteDance personnel for certain engineering functions that require them to access encrypted TikTok user data. According to our Data Access Approval Process, these China-based employees may access these

[1] Apart from these datacenters, user content is temporarily stored by a variety of content delivery networks to facilitate its transmission around the world.

encrypted data elements in decrypted form based on demonstrated need and only if they receive permission from our U.S.-based team.

11. In addition to these existing safeguards, we are also in the process of implementing additional protections to safeguard user data. For fields of user data other than the specific fields that are currently encrypted, we are in the midst of a project to extend our permission system to cover these additional fields as well. We are also in the process of creating a new Washington, D.C.-based Data Defense and Access Assurance team that is designed to advance TikTok's capability to manage the enforcement, monitoring, and response to any actual or attempted data access control violations. The program will include advanced features that will automatically track and map the flow of user data to ensure conformity with TikTok's security controls. The program will also add new capabilities to TikTok's broader encryption mechanism, including breaking out more regional access capabilities by country.

12. To date, there has never been a request from the Chinese government for TikTok user data, and we would not provide any data if we did receive such a request. Because of our internal controls governing access to encrypted user data, the only way we can comply with a request for such customer data is if my team accesses, and produces the relevant customer data. We would only perform these steps after consulting with the legal team, which is led by our U.S.-based General Counsel who is American, to ensure the request is valid, but ultimately it is up to me and my team whether to comply with a request. Because my office is ultimately responsible for disclosing encrypted user data in response to government requests, any such request for data from the Chinese government would require approval from my office, which neither I nor my designees would provide.

13. Our data security measures not only protect against inappropriate access to user data by insiders and unwarranted disclosures to government agencies; they also safeguard against data breaches, hackers, and other malicious actors. We take pride in our data security architecture, which has been designed to mitigate the risk of such breaches. In addition to the access control protections discussed above, we also maintain comprehensive logging functionality that collects information about the identity of employees who review TikTok user data and whether they were authorized to access the data. We also have security alerts that kick in automatically based on trigger points that indicate a security risk—for example, when a large data download occurs, our security architecture is designed to alert our team and to monitor any such download. Under my supervision, our security team conducts periodic tests and reviews logs of access to user data to help ensure that no such breach of our systems has taken place.

B. TikTok's Source Code Safeguards

14. Like many multinational corporations, including U.S. corporations, we have software engineers both in the United States and around the world, including in China. To maintain the integrity of our source code in light of our global workforce, we have dedicated workflow systems to make sure that employees must demonstrate a need for information before they can access source code. Even upon a showing of such a need, the employee still has to obtain appropriate authorization to access the source code, and security controls embedded in the network monitor the employee's review and activities.

15. We also maintain a software development life cycle that involves testing of security controls at multiple points in the development process to ensure that reliance on China-based employees does not introduce any security risks to our code. After the design is finalized, engineers test and validate the security controls included in the design. Then, after the software is

built, further testing takes place, and an automated code review examines potential threats in the code and performs quality and security checks that are independent from the engineering process. Afterwards, additional security testing is independently conducted in the United States, separate from any China-based engineering functions, and is intended to be an extra protection for the security of our source code.

16. As part of our source code integrity processes, we regularly update the software for the TikTok application, which consumers can download via app store updates. We generally issue updates approximately once or twice a week, depending on the app store, and many of these updates include security-related fixes. In addition, whenever needed, we also make available hotfixes for more urgent security issues outside our regular update process.

17. Finally, we also leverage independent third-party experts to help ensure that our standards for the security of our source code are being upheld. We have engaged leading U.S.-based third party vendors, for example, to conduct assessments for insider threats and assist with monitoring, implementation, and validation of our security controls. We have also engaged third-party vendors to perform quality and security checks and conduct intensive code reviews to help ensure that no back doors exist in TikTok's source code. As a further protection beyond these third-party engagements, we have a vulnerability reporting policy that invites external security researchers to report information about vulnerabilities.

18. Going forward, as we recently announced on July 29, 2020, we are opening a new Transparency and Accountability Center for moderation and data practices in Los Angeles and Washington, D.C., which will enable outside experts to observe TikTok's moderation policies in real-time, as well as examine the actual code that drives TikTok's algorithms. My office will oversee the code testing process for this Transparency and Accountability Center.

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 19th day of September, 2020.

Roland Cloutier