Testimony Before the U.S. Senate Committee on Homeland Security and Governmental Affairs

Written Statement of Testimony

Social Media's Impact on Homeland Security: Part II

Testimony of Vanessa Pappas

Vanessa Pappas, Chief Operating Officer, TikTok Inc.

September 14, 2022

Chairman Peters, Ranking Member Portman, and Members of the Committee:

Thank you for the opportunity to appear before you today to discuss how internet companies are working to prevent online extremism to ensure our platforms do not pose a threat to homeland security.

My name is Vanessa Pappas, and I am the Chief Operating Officer at TikTok, where I oversee TikTok's global operations, including content, marketing, Trust and Safety, and user operations. I live with my family in Los Angeles, where I work in one of more than a dozen offices we have across the U.S.

I've been in the United States for more than twenty years, and have spent my career working in entertainment and media. Prior to joining TikTok, I worked at YouTube where I served as the Global Head of Creative Insights, overseeing the company's strategic growth initiatives to drive its daily active user base across key markets and user segments. Prior to that, I was the Global Head of Audience Development at YouTube, focusing on developing audience growth strategies for creators, media publishers, labels and artists.

TikTok's mission is to inspire creativity and bring joy. Over the past couple of years, we have seen tremendous growth and now more than 1 billion people come to TikTok for an authentic, entertaining experience. Every day, individuals come to TikTok to be entertained, to express themselves, and to learn, and small businesses come to reach new customers and build their brands. I came to TikTok because I believe in this mission and see examples every day about how it is lifting people up and helping drive mutual understanding from people in different parts of the world and from different walks of life. In an increasingly complex world, I see TikTok as a contributor to bringing us together and helping us understand each other better.

We are keenly aware that with this success and growth come greater accountability and responsibility. TikTok is committed to being a trusted industry leader in safety and transparency, and we appreciate the Committee's interest in these efforts.

Safety

TikTok strives to create a safe environment where creative, joyful content can flourish, and we have made decisions that prioritize safety over short-term commercial success. For example, we do not allow political ads on the platform, even though they could be a source of significant revenue. Similarly, we do not accept advertisements for categories of content that may hurt our efforts to support the safety of our community, such as advertisements associated with violence or threats, including guns, knives, explosives, pepper spray, and other weapons; ammunition; and tactical gear such as police or military uniforms, armored vests, handcuffs, or batons.

At TikTok, the focus on safety starts at the top, and as an executive, there's no responsibility more important to me than protecting the people on our platform. One of our leadership team's top goals is to "strengthen safety and build trust." TikTok has Terms of Service and Community Guidelines to help ensure that content on TikTok is safe. Safety reviews are a standard part of our product launch process. We also apply our Community Guidelines to everyone and to everything on TikTok. They define a set of norms and common code of conduct, and they provide guidance on what is and is not allowed on TikTok in order to create a welcoming and safe space for entertainment. Specifically, these Community Guidelines include policies that prohibit harmful misinformation, coordinated inauthentic behavior, and promotion of violence.

We educate our community about these guidelines in a variety of ways in the app. For example, we produce in app videos called @tiktoktips, that help people understand how to produce safe content and avoid content that might get their videos removed from the platform. People are notified when they have violated the guidelines and of the consequence(s) of their violation(s). TikTok also educates creators through a dedicated portal that includes detailed information about our policies.

Strong policies are insufficient if they are not enforced through constant attention by human moderators using modern tools. Content moderation policy and implementation for the United States is led by our U.S. Safety Team in Los Angeles, which reports to me. Moderators will remove content—including video, audio, livestream, images, and comments—that violates our Community Guidelines. We use a mixture of automated and human review for content moderation, with automation helping to scale moderation and human reviewers focused on making decisions that are more nuanced relative to our guidelines. Trust and safety represents our largest labor expense for TikTok's U.S. operations. There are thousands of people working across safety, privacy, and security on a daily basis. TikTok invests heavily in these teams, as well as in technology to detect potential violations and suspicious accounts at scale.

We understand that verifying certain information during dynamic and fast moving events can be challenging and so, to minimize risk, we work with independent fact checkers to evaluate content for false or misleading claims. We currently have 13 fact-checking partners, including Agence France-Presse (AFP), Australian Associated Press (AAP), Animal Político, Deutsche Presse-Agentur (Dpa), Facta, Estadão Verifica, Lead Stories, Logically, Newtral, Newschecker, PolitiFact, Science Feedback, and Teyit. These fact-checking partners support 33 languages and assess content in 64 markets around the world. All of our fact-checking partners are accredited

by the International Fact-Checking Network as verified signatories of the International Fact-Checking Network's code of principles.

TikTok also encourages people who identify violations of our Community Guidelines to report such violations through the app. People can report violative videos by pressing on the video, selecting "Report", and following the instructions provided when prompted. Systems are also in place to allow trusted flaggers to escalate content for human review.

Violent Extremism and Hateful Behavior

In addition to removing content that violates our policies, we also employ proactive measures, informed by the analysis U.S. intelligence agencies and trusted organizations in civil society, to prevent the spread of hateful ideologies and violent extremist groups on our platform. For example, we have a zero tolerance stance on content that promotes white supremacy or nationalism and remove accounts with repeated content violations. In addition, we remove race-based harassment and the denial of well-documented and violent events. We work with a range of experts, including the Anti-Defamation League (ADL), to continually expand our database of hateful terms and symbols, and incorporate them into our models, moderation systems, and training materials.

We take into account publicly available information from experts, including the United Nations Security Council and Southern Poverty Law Center, to designate dangerous or hateful individuals and organizations. In appropriate cases, we work to ban all content associated with violent extremist groups and individuals from appearing on the platform. Examples include foreign terrorist organizations, drug cartels, and groups such as QAnon, Three Percenters, and Oath Keepers. Users who search for this content, including related hashtags or keywords, are redirected to our Community Guidelines.

An example of our approach to violent extremism can be seen in content related to the attack on the Capitol on January 6, 2021. TikTok is an entertainment-first platform, which is why it was not the platform of choice for those who organized the violence at the Capitol. From our review of 850 sets of Department of Justice charging documents related to the January 6 attack, there were 686 references to social media companies. TikTok was mentioned in only 18 of those 686 cases.

Transparency

In addition to keeping our platform safe, we are committed to being transparent about how we accomplish that goal. Every quarter, we release a Community Guidelines Enforcement Report. These reports contain detailed information about the type and volume of content we remove. For instance, in the first quarter of 2022, our proactive removal rate for content violating our violent extremism policy was 91.4 percent. That means that more than 9 times out of 10, we discovered and removed the content on our own before receiving any reports from users or third parties.

Additionally, 83.9 percent of the removals under our violent extremism policy happened before the content received any views, and in 88.4 percent of the cases, the removals occurred within 24

hours of the content being posted. Our proactive detection rates have improved each year, and we are dedicated to continuing this trend.

Twice a year, we also disclose data about requests we receive from law enforcement or governments. TikTok is committed to responding to law enforcement requests for user information in a manner that respects the privacy and other rights of our community members. Each request we receive is carefully reviewed. In our semiannual reports, we include a detailed breakdown of these requests, including the countries from which they originate.

We are also building Transparency and Accountability Centers in Los Angeles and Washington, DC, that will allow us to share information about how we moderate and recommend content. We have brought parts of the tour into an online experience during the pandemic and would be happy to arrange a virtual tour for Members and Committee staff at your convenience, or invite you to join us in the physical centers when construction is complete. We have also confirmed that Oracle will be vetting validating our content recommendation and moderation models.

Algorithm

TikTok's For You feed is part of what enables connection and discovery. It is central to the TikTok experience and where most people spend their time. When you are watching the For You feed, you are presented with a stream of videos curated to your interests, making it easy to find content and creators you love. This feed is powered by a recommendation system that delivers content to each user that is likely to be of interest to that particular user. Part of the magic of TikTok is that there's no single For You feed—while different people may come upon some of the same standout videos, each person's feed is unique and tailored to that specific individual.

Our uniquely powerful yet easy-to-use tools democratize video creation, enabling everyday people to express themselves creatively and find their community on the platform. This approach has resulted in more authentic content and has helped launch new cultural trends from feta pasta to the resurgence of Fleetwood Mac's "Dreams." It has allowed small businesses to find their voice, and to expand their reach and customer base, and it has been a bright spot for American families during the Covid-19 pandemic. In an October 2021 study conducted by Nielsen, TikTok was the only app where a top reason for usage was "to lift my spirits" and found that people around the globe find TikTok content to be authentic, genuine, unfiltered, and trendsetting.

For people who don't select categories, we start by offering them a generalized feed of popular videos. Their first set of likes, comments, and replays will initiate an early round of recommendations as the system begins to learn more about their content tastes. When people decide to follow new accounts, for example, that action will help refine their recommendations, as will exploring hashtags, sounds, effects, and trending topics on the Discover tab. All of these are ways to tailor the experience and invite new categories of content into the feed.

TikTok's recommendation system ranks videos for people based on a combination of factors, including their own interactions with other videos and device and account settings. All these factors are processed by our recommendation system and weighted based on their value. A strong indicator of interest, such as whether a person finishes watching a longer video from

beginning to end, would receive greater weight than a weak indicator, such as whether the video's viewer and creator are both in the same country. Videos are then ranked to determine the likelihood of a user's interest in a piece of content and are delivered to each unique For You feed.

TikTok is home to creators with many different interests and perspectives, and sometimes users may come across a video that isn't quite to their taste. Users can long-press to add a video to their favorites, and can long-press on a video and tap "Not Interested" to indicate that they don't care for a particular video. People can also choose to hide videos from a given creator or made with a certain sound, or report a video that seems out of line with our guidelines. All these actions contribute to future recommendations in the For You feed.

To keep the For You feed interesting and varied, our recommendation system works to offer diverse and new areas of discovery and delight. For example, the For You feed generally will not show two videos in a row made with the same sound or by the same creator. We also do not recommend duplicated content, content a user has already seen before, or content that is considered spam. However, a person might be recommended a video that has been well received by other people who share similar interests.

Diversity is essential to maintaining a thriving global community, and it brings the many corners of TikTok closer together. What this means is that sometimes people may come across a video in their feed that does not appear to be relevant to their expressed interests or have amassed a huge number of likes. This is an important and intentional component of our approach to recommendation: bringing a diversity of videos into the For You feed gives people additional opportunities to stumble upon new content categories, discover new creators, and experience new perspectives and ideas.

By offering different videos from time to time, the system is also able to get a better sense of what is popular among a wider range of audiences to help provide other people using TikTok a great experience, too. The goal is to find balance between suggesting content that is relevant while also helping them find content and creators that encourage them to explore experiences they might not otherwise see.

The recommendation system is also designed with safety as a consideration. We recently announced the development of a new content classification system that will help ensure that people are getting relevant, interesting, and appropriate content. We are focusing initially on safeguarding the teen experience with this new system, and in the coming months will add content filtering options for our entire community so they can enjoy more of what they love.

Consistent with our safety-first approach, content that is being fact checked and reviewed content that cannot be substantiated will be ineligible for recommendation into the "For You" feed (FYF). Similarly, videos that have just been uploaded, are under review, or are flagged as spam-like content seeking to artificially increase traffic may also be ineligible for recommendation into a user's FYF.

API for Researchers

To provide greater transparency, we are in the process of developing a research API that would allow selected researchers to gain access to certain data about content and activity on our platform, and plan to make it available later this year.

In addition, we have developed a moderation system API that we plan to make available at our Transparency and Accountability Centers. This moderation system API will provide selected researchers an effective way to evaluate our content moderation systems and examine existing content available on our platform. In our Transparency and Accountability Centers, selected researchers will also be able to upload their own content to see how different types of content are either permitted, rejected, or passed to moderators for further evaluation.

The independent experts on our U.S. Content Advisory Council and regional Safety Advisory Councils will also be granted API access as well as access to confidential information, such as our keyword lists (which are used to help detect and flag potentially violative content) for deeper analysis. We do not make keyword lists available publicly in order to avoid providing a roadmap for bad actors who attempt to subvert our safeguards. While we have dedicated teams regularly stress-testing our processes and tools to ensure they're robust and effective, we know that perspectives and insights from experts can strengthen our approach.

Data Security

Since 2020, we have been clear and transparent about our broader objective to limit the number of employees who have access to user data and the circumstances under which data access is enabled. As we noted in an April 2020 blog post, "[o]ur goal is to minimize data access across regions so that, for example, employees in the APAC region, including China, would have very minimal access to user data from the EU and U.S." Separately, in a September 2020 sworn declaration, TikTok acknowledged that ByteDance personnel in China can have access to TikTok user data based on demonstrated need to perform their roles.

Employees outside the U.S., including China-based employees, can have access to TikTok U.S. user data subject to a series of robust cybersecurity controls and authorization approval protocols overseenby our U.S.-based security team. In addition, TikTok has an internal data classification system and approval process in place that assigns levels of access based on the data's classification and requires approvals for access to U.S. user data. The level of approval required is based on the sensitivity of the data according to the classification system. We monitor and review access to U.S. user data on an ongoing basis.

While we have been transparent about our data access policies and protocols, we also have been working assiduously to address national security concerns identified by U.S. policymakers and regulators, including the Committee on Foreign Investment in the United States (CFIUS). Although I will not be commenting on the CFIUS process during my remarks today because of the confidentiality of the process, I can tell you that we've made very significant progress in that process, some of which has been disclosed in the media. Specifically, as was reported in the

press earlier this year, for more than a year we have been pursuing a multi-pronged initiative called “Project Texas” to strengthen TikTok’s U.S. data security program.

We recently reached a significant milestone by changing the default storage location of U.S. user data to the Oracle Cloud Infrastructure. TikTok now stores 100% of U.S. user data by default in the Oracle cloud environment, and we are working with Oracle on new, advanced data security controls that we hope to finalize in the near future. We still use our U.S. and Singapore data centers for backup, but as we continue our work, we expect to delete U.S. users’ private data from our own data centers. This work puts us closer to the day when we will be able to pivot toward our industry-leading system for protecting the data of our users in the United States, with robust, independent oversight to ensure compliance.

Additionally, we are making operational changes in line with these protocols. In May 2022, TikTok announced the creation of a new division—U.S. Data Security (“USDS”)—to bring heightened focus and governance to our ongoing efforts to strengthen our data protection policies and protocols, further protect our U.S. users, and build confidence in our systems and controls in the United States. This division has U.S.-based leadership. Access to U.S. user data by anyone outside of our new U.S. Data Security team will be limited by, and subject to, robust data access protocols that are being developed in close collaboration with Oracle and the U.S. government.

In order to facilitate a global platform, our goal is to ensure non U.S.-based employees, including China-based employees, will only have access to a narrow set of TikTok U.S. user data, such as public videos and comments available to anyone on the TikTok platform, to ensure global interoperability.

Privacy Policy

TikTok’s privacy policy describes the information we collect and how we use that information. In some cases, our privacy policy describes information that we do not currently collect, but may collect in the future. We appreciate the Committee’s interest in further clarity about what certain terms in our privacy policy mean and whether we are currently collecting certain data elements that are referenced in our privacy policy.

Like other apps, we collect information about what people search for within our app. We do this to recommend more relevant content on TikTok. We do not collect people's Google searches or queries on other search engines. Similarly, if users browse content within our app, we collect that information to serve more relevant videos in their For You feed. In our Privacy and Security Center, we explain that this includes “[b]rowsing history in the TikTok in-app browser to help make platform improvements, such as optimizing page load times and ad measurement.” Like other platforms, we may also collect a limited amount of data related to user activity on advertiser’s apps and websites when those advertisers elect to share such data with us.

TikTok does not currently collect precise geolocation in the United States. TikTok collects coarse (approximate) location information based on things like the subscriber identity module (SIM) card and IP address associated with the user's device. Such location information is much

less precise than GPS coordinates and is used for things like recommending locally relevant content and ads.

We do not use facial, voice, or other physical features to identify U.S. users. We offer a variety of special effects that people can use when creating videos. When a user creates a video, they can choose to apply an effect to their face (e.g., add sunglasses) or to change the tone of their voice (e.g., like a chipmunk). To enable such effects, we collect and process information about the images and audio that are part of the user's video, such as the location of facial features within an image (e.g., detecting the location of eyes for a sunglasses effect) and aspects of the audio (e.g., to raise the pitch to sound like a chipmunk).
We use keystroke patterns and rhythms as one of the signals to identify, detect, and thwart inauthentic or spammy behavior. There have been media reports suggesting that when someone accesses a website by using TikTok's in-app browser, TikTok captures everything that the user is typing (including credit card information). Such reports are inaccurate. We do not collect precise keystroke or text input through the code at issue, but instead solely use this information for debugging, troubleshooting, and performance monitoring.

As discussed earlier in my testimony, we recently announced the creation of a new division—USDS—to help strengthen and improve our systems and controls in the United States. Access to U.S. user data by anyone outside of USDS will be limited by, and subject to, robust data access protocols that will be developed in close collaboration with Oracle and the U.S. government.

These operating protocols will necessarily and significantly constrain our ability to share U.S. user data within our broader group of corporate entities. TikTok, which is not available in China, is subject to the laws of the jurisdictions where it operates. As we have stated before, we have not been asked for US user data by the Chinese government. We have not provided such data to the Chinese government, nor would we if asked.

Relationship with ByteDance

TikTok is a flagship product of ByteDance Ltd., a global technology company operating a range of content platforms that inform, educate, entertain, and inspire people across languages, cultures, and geographies.

As a global entertainment platform, TikTok spans most major markets except China, where ByteDance offers a different short-form video app called Douyin. TikTok is provided in the United States by TikTok Inc., which is incorporated in California and subject to U.S. laws and regulations. Like many global technology companies, we have product development and engineering teams all over the world collaborating to deliver the best product experience for our community. TikTok is led by an executive team in the United States and Singapore and has global offices including Los Angeles, Silicon Valley, New York, Dublin, London, Paris, Berlin, Dubai, Singapore, Jakarta, Seoul, and Tokyo.

ByteDance Ltd. is the ultimate parent entity that is incorporated outside of China. The board is comprised of our CEO Rubo Liang, Bill Ford of General Atlantic, Arthur Dantchick of Susquehanna International Group, Philippe Laffont of Coatue, and Neil Shen of Sequoia.

ByteDance's investors include global institutional funds such as Blackrock, Coatue, Fidelity, General Atlantic, KKR, Sequoia, Softbank, and Susquehanna International Group. Today, over sixty percent of ByteDance Ltd. is owned by Western investment firms, with most of the rest of the company owned by the founders and employees.

Conclusion

We appreciate the challenges that we face as an industry, and TikTok will remain steadfast and vigilant in promoting safety, transparency, and trust on our platform. Thank you for the opportunity to discuss these important issues before the Committee.

EXHIBIT A TO SUBMISSION

TikTok

June 30, 2022

The Honorable Marsha Blackburn
United States Senate
357 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Roger Wicker
United States Senate
555 Dirksen Senate Office Building
Washington, DC 20510

The Honorable John Thune
United States Senate
511 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Roy Blunt
United States Senate
260 Russell Senate Office Building
Washington, DC 20510

The Honorable Ted Cruz
United States Senate
127A Russell Senate Office Building
Washington, DC 20510

The Honorable Jerry Moran
United States Senate
521 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Shelley Moore Capito
United States Senate
172 Russell Senate Office Building
Washington, DC 20510

The Honorable Cynthia Lummis
United States Senate
124 Russell Senate Office Building
Washington, DC 20510

The Honorable Steve Daines
United States Senate
320 Hart Senate Office Building
Washington, DC 20510

Dear Senators Blackburn, Wicker, Thune, Blunt, Cruz, Moran, Capito, Lummis, and Daines,

Thank you for your letter dated June 27, 2022. We appreciate the opportunity to address the concerns you set forth. Many of your questions appear to stem from a recent BuzzFeed article, which contains allegations and insinuations that are incorrect and are not supported by facts. We appreciate the opportunity to set the record straight by answering your questions.

Before doing so, we would like to contextualize what many of the people quoted in the article were talking about and what the company has been broadly working to achieve. For well over a year, we've been pursuing a multi-pronged initiative called "Project Texas" to strengthen the company's data security program. Security experts can confirm that these initiatives are often painstaking and complex, even with expert assistance from world-class companies like Oracle and Booz Allen. Some people working on these projects do not have visibility into the full picture, working on a task

without realizing that it's a single step in a much bigger project or a test to validate an assumption.

That's critical context for the recordings leaked to Buzzfeed, and one thing their reporting got right: the meetings "*were in service of Project Texas's aim to halt this data access.*"

The broad goal for Project Texas is to help build trust with users and key stakeholders by improving our systems and controls, but it is also to make substantive progress toward compliance with a final agreement with the U.S. Government that will fully safeguard user data and U.S. national security interests. We have not spoken publicly about these plans out of respect for the confidentiality of the engagement with the U.S. Government, but circumstances now require that we share some of that information publicly to clear up the errors and misconceptions in the article and some ongoing concerns related to other aspects of our business.

While we are disappointed that leaks have put us in this position, we are pleased to share the substantial progress on our objectives. As we recently reported, we now store 100% of U.S. user data by default in the Oracle cloud environment, and we are working with Oracle on new, advanced data security controls that we hope to finalize in the near future. That work puts us closer to the day when we will be able to pivot toward a novel and industry-leading system for protecting the data of our users in the United States, with robust, independent oversight to ensure compliance.

We are taking additional measures beyond data security, which we will briefly touch on in our responses below.

We have been clear dating back to an early 2020 blog post that we are working on a broad set of objectives: "*Similar to industry peers, we will continue to drive our goal of limiting the number of employees who have access to user data and the scenarios where data access is enabled. Although we already have controls in place to protect user data, we will continue to focus on adding new technologies and programs focused on global data residency, data movement, and data storage access protections worldwide.*" (https://newsroom.tiktok.com/en-us/our-approach-to-security). There is a distinction between data storage and data access, but they are both—together—important components of our efforts to earn trust and improve security for TikTok; our solution will now ensure both the storage of all U.S. user data in the United States and all data sharing outside of the protected enclave in the United States will be pursuant to protocols and terms approved by the U.S. Government.

In light of the context above, we are confident that when you review our responses, you will see that TikTok has not, at any point, misled Congress about our data and security controls and practices. We understand, respect, and appreciate the incredibly important work of your Committee and Congress, and we have always approached our engagements with Members and staff, both in public and in private, with candor and

integrity. We stand by the statements Michael Beckerman made before Congress and are grateful for his leadership.

As we continue our productive conversations with the Administration and continue to explore commercial partnerships with companies like Oracle, we look forward to keeping you and the full Committee apprised of our work to further ensure the security of U.S. user data.

Please see below for TikTok's responses to your questions.

1. **Is it true that TikTok employees located in China currently have, or had in the past, access to U.S. user data? This could include programmers, product developers, data teams, as well as trust and safety and content moderation professionals.**
    a. **If yes, please explain in detail which employees have or had such access and for what purposes.**
    b. **If the employees had this access in the past but no longer do, please identify the applicable date ranges.**

Employees outside the U.S., including China-based employees, can have access to TikTok U.S. user data subject to a series of robust cybersecurity controls and authorization approval protocols overseen by our U.S.-based security team. In addition, TikTok has an internal data classification system and approval process in place that assigns levels of access based on the data's classification and requires approvals for access to U.S. user data. The level of approval required is based on the sensitivity of the data according to the classification system.

The solution that TikTok is implementing pursuant to Project Texas has focused on evaluating and revising TikTok's internal policies and operational controls in relation to U.S. user data access, to take steps to strengthen data security around U.S. user data and, ultimately, to make the organizational, process, and technical changes to help ensure compliance and enhance protection of U.S. user data defined as "protected" through engagement with CFIUS. As we are in the process of undergoing CFIUS national security review, we have kept CFIUS informed of these efforts. This protected user data will be stored in Oracle Cloud Infrastructure with access limited only to authorized personnel, pursuant to protocols being developed with the U.S. Government.

2. **TikTok's privacy policy says you share data you collect with your parent companies and affiliates and that you transmit user information to servers and data centers overseas.**
    a. **Have any ByteDance employees—located in China or elsewhere—had access to U.S. User data, either currently or in the past?**

Please see our response to question 1.

TikTok

b. What are the locations of the servers and data centers overseas where TikTok transmits U.S. user data?

TikTok has long stored U.S. user data in data centers in the U.S. and Singapore, as well as in cloud-based services offered by AWS, the Google Cloud Platform, and Azure. Our Virginia data center includes physical and logical safety controls such as gated entry points, firewalls, and intrusion detection technologies. It is also important to maintain backup data storage locations to guard against catastrophic scenarios where user data could be lost, and our data center in Singapore serves as the backup data storage location for our U.S. user data.

100% of U.S. user traffic is now being routed to Oracle Cloud Infrastructure. We are still using our U.S. and Singapore data centers for backup, but as we continue our work to deliver on U.S. data governance, we expect to delete U.S. users' protected data from our own systems and fully pivot to Oracle cloud servers located in the U.S.

3. Do any ByteDance employees have a role in shaping TikTok's algorithm?

Subject to the controls described in our response to question 1, ByteDance engineers around the world may assist in developing those algorithms, however our solution with Oracle will ensure that training of the TikTok algorithm only occurs in the Oracle Cloud Infrastructure and will also ensure appropriate third-party security vetting and validation of the algorithm. For more information about how TikTok's algorithm recommends content, please see our Newsroom post: https://newsroom.tiktok.com/en-us/how-tiktok-recommends-videos-for-you.

4. Do any Douyin employees have any access to American user data or a role in shaping TikTok's algorithm?

ByteDance developed the algorithms for both Douyin and TikTok, and therefore some of the same underlying basic technology building blocks are utilized by both products, but TikTok's business logic, algorithm, integration, and deployment of systems is specific to the TikTok application and separate from Douyin.

Under Project Texas and as a result of our work with the U.S. Government, going forward our solution with Oracle will ensure the TikTok application and platform, including the algorithm, is deployed through the Oracle Cloud Infrastructure in the United States with third-party security vetting and validation of the software for the application and platform, including the TikTok algorithm.

TikTok

5. **In the past, TikTok has said that it has never—nor would it ever—provide user data to the Chinese government, even if asked. Yet your privacy policy says you can disclose data collected to respond to government inquiries.**
    a. **Has TikTok ever disclosed any U.S. user data to respond to government inquiries from the Chinese Communist Party?**
    b. **If the Chinese Communist Party asked you for U.S. user data, what is to stop you from providing it? Can the CCP compel you to provide this data, regardless of response? Can they access it, regardless of response?**
    c. **Has ByteDance ever responded to CCP inquiries on TikTok's behalf?**
    d. **Has TikTok ever shared U.S. user data with ByteDance for the purpose of responding to a CCP inquiry?**

We have not been asked for such data from the CCP. We have not provided U.S. user data to the CCP, nor would we if asked.

More information about government requests for user data that we receive across the world is available in our Information Request Reports, available at https://www.tiktok.com/transparency/en-us/information-requests-2021-1/.

6. **Do TikTok employees in the U.S. use software developed by ByteDance, such as Lark?**

Yes.

7. **Does ByteDance have any role—either in the past or in the present—in hiring TikTok employees in the U.S.?**

As would be expected of any global company with subsidiaries, ByteDance plays a role in the hiring of key personnel at TikTok. However, as we have described before, TikTok is led by its own global CEO, Shou Zi Chew, a Singaporean based in Singapore.

8. **Does TikTok own or lease its own office space in the U.S., and does ByteDance have any ownership or lease stake in those facilities?**

TikTok leases office space in cities across the U.S., including Los Angeles, Austin, Chicago, New York, Detroit, Seattle, DC, and Nashville. These leases are through U.S. entities, TikTok Inc. (a California corporation) and ByteDance Inc. (a Delaware corporation).

9. **Does the Chinese government have an ownership stake or seat on the Board of Directors, or provide personnel in any other leadership position, of the Beijing ByteDance Technology Company?**

TikTok

a. **What role does this seat play in impacting decisions made at ByteDance or TikTok?**
b. **Does this position afford an opportunity for the board member to determine whether and how TikTok or ByteDance will respond to CCP inquiries?**
c. **Does this position afford an opportunity for the board member to view TikTok user data?**
d. **Would you be informed, as a matter of policy, if a board member did view the data? If the board member did share the data, in any capacity, with the CCP?**

As multiple corporate entities share the "ByteDance" name, several China-based ByteDance entities were renamed earlier this year to keep the names of businesses and entities more consistent. Beijing Bytedance Technology Co. Ltd is now called Beijing Douyin Information Service Limited. We will refer to it here using its new name for avoidance of confusion.

ByteDance Ltd., the ultimate parent entity that is incorporated in the Cayman Islands, has a global board, including Bill Ford of General Atlantic, Arthur Dantchik of Susquehanna International Group, Philippe Laffont of Coatue, Neil Shen of Sequoia, and the company's CEO Rubo Liang. The majority of ByteDance's investors are global institutional funds such as Coatue, General Atlantic, KKR, Sequoia, Softbank, and Susquehanna International Group.

Beijing Douyin Information Service Limited is a separately held subsidiary of ByteDance Ltd. Beijing Douyin Information Service Limited does not have any direct or indirect ownership interest in or control over any TikTok entity. Further, employees of Beijing Douyin Information Service Limited are restricted from U.S. user database access. The Chinese state-owned enterprise's acquisition of 1% of Beijing Douyin Information Service Limited was necessary for the purpose of obtaining a news license in China for several China-based content applications, such as Douyin and Toutiao.

The Chinese government does not directly or indirectly have the right to appoint board members or otherwise have specific rights with respect to any ByteDance entity within the chain of ownership or control over the TikTok entity.

10. **How will TikTok's new cloud service arrangement be structured, and how will the company determine which data is "protected" such that it is not shared with employees or others in China?**

TikTok recently published a Newsroom post outlining our U.S. data governance practices and announcing a commercial relationship with Oracle in support of these practices (https://newsroom.tiktok.com/en-us/delivering-on-our-us-data-governance).

TikTok

As described in question 1, U.S. user data at issue is being defined as "protected" through engagement with CFIUS, and will be stored in the Oracle Cloud Infrastructure with access limited only to certain personnel in USDS. Under the contemplated arrangement, access to U.S. user data by anyone outside of USDS will be limited by, and subject to, robust data access protocols, with further monitoring and oversight mechanisms by Oracle to validate compliance.

In order to facilitate a global platform, non U.S.-based employees, including China-based employees, will have access to a narrow set of non-sensitive TikTok U.S. user data, such as public videos and comments available to anyone anywhere in the world, to ensure global interoperability so our U.S. users, creators, brands, and merchants are afforded the same rich and safe TikTok experience as global users.

11. Why is TikTok not planning to ensure that all U.S. user data is blocked from view of employees or others in China?

As described in our response to question 10, access to U.S. user data by anyone outside of our new USDS team will be limited by, and subject to, robust data access protocol that will be developed in close collaboration with Oracle and CFIUS.

We're proud to be able to serve a global community of more than a billion people who use TikTok to creatively express themselves and be entertained, and we're dedicated to giving them a platform that builds opportunity and fosters connections worldwide. We also work hard to safeguard our community, both in how we address potentially harmful content and how we protect against unauthorized access to user data.

Consistent with the operation of this global platform, and as described in our response to question 10, certain China-based employees will have access to a narrow, non-sensitive set of TikTok U.S. user data, such as the public videos and comments available to anyone, to ensure global interoperability so our U.S. users, creators, brands, and merchants are afforded the same rich and safe TikTok experience as global users. But this access will be very limited, it will not include private TikTok U.S. user information, and it will only occur pursuant to protocols being developed with the U.S. Government.

*****

TikTok

We thank you for your questions and appreciate the opportunity to provide additional details and clarification. We know we are among the most scrutinized platforms from a security standpoint, and we aim to remove any doubt about the security of U.S. user data. We're dedicated to earning and maintaining the trust of our community and of policymakers, and will continue to work every day to protect our platform and provide a safe, welcoming, and enjoyable experience for our community.

Sincerely,

Shou Zi Chew
CEO, TikTok

cc:
The Honorable Maria Cantwell
The Honorable Richard Blumenthal