Protecting U.S. National Security Interests

TikTok recognizes our heritage has raised questions about whether TikTok poses a national security threat. In response to these concerns, we launched an initiative - undertaken voluntarily and wholly at TikTok's expense - to build a secure environment for protected U.S. user data*, to ensure the platform remains free from outside influence, and to implement additional safeguards on our content recommendation and moderation tools. We take national security very seriously, and our work to address related concerns remains thorough and ongoing. Here's the progress we've made:

U.S. Data Security

In May 2022, TikTok created a new organization called TikTok U.S. Data Security (TikTok USDS). This special purpose subsidiary is staffed by U.S.-based employees (with some exceptions in the U.K. and Australia to provide global coverage). USDS controls access to protected U.S. user data, content recommendation, and moderation systems in the secure Oracle Cloud. This structure brings heightened focus and governance to our data protection policies and content assurance protocols to keep U.S. users and their data safe. Teams within USDS are dedicated to delivering on our commitments, and span functions such as Engineering, User Operations, Privacy, Security Operations, Trust and Safety, Legal, Finance, and more. Many of the organization's leaders have U.S. national security experience.

Software Assurance: Preventing Backdoors and Content Manipulation

All source code entering the secure environment will be inspected by Oracle. If the source code has not gone through the review process, it will not run in this environment.

All TikTok app code will go through Oracle's review process (including technology or human review). Oracle will compile the app, and deploy it to the app stores, maintaining chain of custody for assurance. The code that powers TikTok's recommendations - the For You feed - will be inspected, reviewed, and validated by third parties.

Content moderation processes, both human and machine, will be vetted, reviewed, and tested to ensure that moderation is based only on our published Community Guidelines. All videos removed will be subject to audit.

A Secure Environment for the U.S. App

New protected U.S. user data is stored by default in the Oracle Cloud and USDS infrastructures with controlled and monitored gateways. Once deletion of backup data is complete (a process currently underway), only approved USDS personnel will have access to protected U.S. user data in the Oracle cloud. All business functions that require access to protected U.S. user data will be part of USDS.

There will be limited situations where protected U.S. user data can leave the secure environment to maintain a globally interoperable platform. For example:

- A U.S. TikTok user might want to send a message to a non-U.S. TikTok user, requiring the content of the message to leave the Oracle Cloud Infrastructure to reach its intended recipient.
- A U.S. creator wanting to share their content globally would need their public content - their videos and their public profile information - to leave the Oracle Cloud Infrastructure.

There are some limited exceptions where non-USDS employees may be granted access to protected data, for example, for legal and compliance, but such access must be expressly authorized by USDS pursuant to a robust data access protocol.

(Effective Jan. 2024)

Timeline

March 2021 — Project work begins.

May 2022 — USDS department formalized.

June 2022 — 100% of new, protected U.S. user data routed to Oracle Cloud Infrastructure and USDS controlled infrastructure with traffic temporarily backed-up/ synced to global TikTok servers in Virginia and Singapore.

October 2022 — Stopped synchronizing/ backing-up the data between Oracle systems and the servers in Virginia and Singapore.

January 2023 — Access to TikTok Oracle Cloud Infrastructure can only be accessed by USDS personnel.

January 2023 — First Dedicated Transparency Center opens in Maryland for source code inspection by Oracle.

July 2023 — Oracle begins reviewing entire TikTok app source code.

Transparency, Oversight, and Accountability

This initiative is the framework we developed with the U.S. Government (the Committee on Foreign Investment - or CFIUS - in the U.S.) to allow it to verify that U.S. data on TikTok is secure. Since 2021, we have been working to reach a national security agreement that would legally require TikTok to implement this initiative, but we're already doing that voluntarily.

Under a signed agreement with the U.S. Government, we would take additional steps to provide even more transparency, oversight, and accountability of this program, including:

- TikTok USDS would be governed by an independent board made up of CFIUS-vetted and approved directors, each with significant national security experience;
- USDS key management personnel will be vetted by CFIUS; they will report up to the USDS board, with no reporting lines to TikTok or ByteDance leadership; and
- Employees of USDS will be vetted and hired in accordance with requirements—including restrictions on citizenship and country of origin—put forth by CFIUS.

If an agreement with the US Government is fully implemented, we'll be the only platform whose controls and defenses are regularly vetted, tested, and scrutinized by U.S. national security agencies and their trusted partners, like Oracle. This structure will make us far more secure than other companies in the industry that collect extensive data on U.S. users.

Our Corporate Structure

TikTok's parent company, ByteDance, was founded by Chinese entrepreneurs. It isn't owned or controlled by the Chinese government or any other state entity. ByteDance is a private, global company, nearly 60 percent of which is owned by global institutional investors such as General Atlantic and Susquehanna International Group, with the rest owned primarily by the company's founders and its employees - including thousands of Americans.

The TikTok platform may be global, but we take a local approach to regulatory compliance, working with stakeholders to ensure that we understand local concerns and meet our regulatory commitments.

*How we define protected data:

Protected data broadly means personal information collected from a U.S.-based user of TikTok. Subject to exceptions, protected data include the following categories of data, even if deidentified, anonymized, or aggregated: user data, such as email and birthdate; non-public user content, such as private videos and direct messages; behavioral data, such as user interaction with content including likes and favorites; data inputs to TikTok's recommendation engine, such as video completion and video viewing time; and device and network data, such as IP address and device model.

(Effective Jan. 2024)