Protecting U.S. National Security Interests

TikTok's Chinese heritage has raised concerns about whether TikTok poses a national security threat. We've been working to address those concerns through an initiative called Project Texas.

What is Project Texas?

- Project Texas is an initiative to make every American on TikTok feel safe, with confidence that their data is secure and the platform is free from outside influence.
- We've been implementing Project Texas to remove doubts about potential external or foreign influence, create a secure enclave to protect U.S. user data, and put additional safeguards on our content recommendation and moderation tools.

What is USDS?

- TikTok U.S. Data Security ("USDS") is tasked with managing all functions and elements of the TikTok platform related to U.S. data and content.
- This structure brings heightened focus and governance to our data protection policies and content assurance protocols to keep U.S. users safe.
- Teams within USDS are dedicated to delivering on our commitments, and span functions like Safety, Legal, Engineering, Finance, HR, User Ops, Security Compliance, and more.

Did you know?

- ByteDance is a private, global company. Nearly 60% is owned by global institutional investors, 20% is owned by the company's founders, and 20% is owned by 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.

Did you know?

- TikTok does not log keystrokes
- TikTok does not collect precise location in the U.S.
- TikTok does not track your search and browsing behavior across the internet
- TikTok does not build a "shadow profile" on our users to serve ads
- TikTok does not use face or voice prints to identify individuals

Components of Project Texas

Organizational Design - Protecting Against Outside Influence

- TikTok U.S. Data Security is a special purpose subsidiary that oversees all elements of the U.S. TikTok platform related to data and content.
- TikTok USDS will be governed by an independent board made up of U.S. Government vetted and approved directors, each with significant national security experience.
- The USDS board will report directly to CFIUS, with no reporting lines to TikTok or ByteDance leadership.
- USDS officers will be vetted and approved by CFIUS; they will report to the USDS board, with no reporting lines to TikTok or ByteDance leadership.
- Employees of USDS will be vetted and hired in accordance with requirements—including restrictions on country of origin—put forth by CFIUS. They will have no reporting lines to TikTok or ByteDance leadership.

Technology Assurance - Preventing Backdoors and Content Manipulation

- All software and code entering the secure enclave through protected gateways will be inspected by Oracle and a third party source code inspector. Code that has not been inspected and approved cannot operate in the environment.
- Oracle will review and approve all TikTok app code, compile the app, and deploy it to the app stores, maintaining chain of custody for assurance.
- The U.S. TikTok app validated and compiled by Oracle will only be able to communicate with code in the Oracle environment that has also been inspected and approved by Oracle and a third party code inspector.
- The code that powers TikTok's recommendations—the For You Feed—will be inspected and tested to ensure that it recommends content solely on content-neutral user behavior and established and auditable promotion and filtering decisions, such as featuring World Cup content or ensuring that multiple videos from the same creator don't run back-to-back.
- 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 Enclave for the U.S. App - Putting U.S. Data Out of Reach

- Today, all new U.S. user data is stored in the protected Oracle cloud environment with tightly controlled, rigorously monitored gateways.
- Only approved USDS personnel has access to U.S. user data in the Oracle cloud.
- All business functions requiring access to U.S. user data will be housed in USDS.
- There will be limited situations—vetted and agreed to by the U.S. Government—where 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 environment 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 environment.

Compliance Monitoring and Oversight - Holding Us Accountable

- All elements of the TikTok app and backend code will be subject to multiple layers of outside oversight and monitoring, including source code inspection, overall compliance monitoring in USDS operations, content audits, and more.
- Every third party that is a part of this process will have reporting obligations directly to CFIUS.
- CFIUS will have discretion to do site inspections, request audits, and appoint additional monitors.
- Failure to adhere to the commitments in the agreement could result in additional mitigations or a total shutdown of the U.S. service.