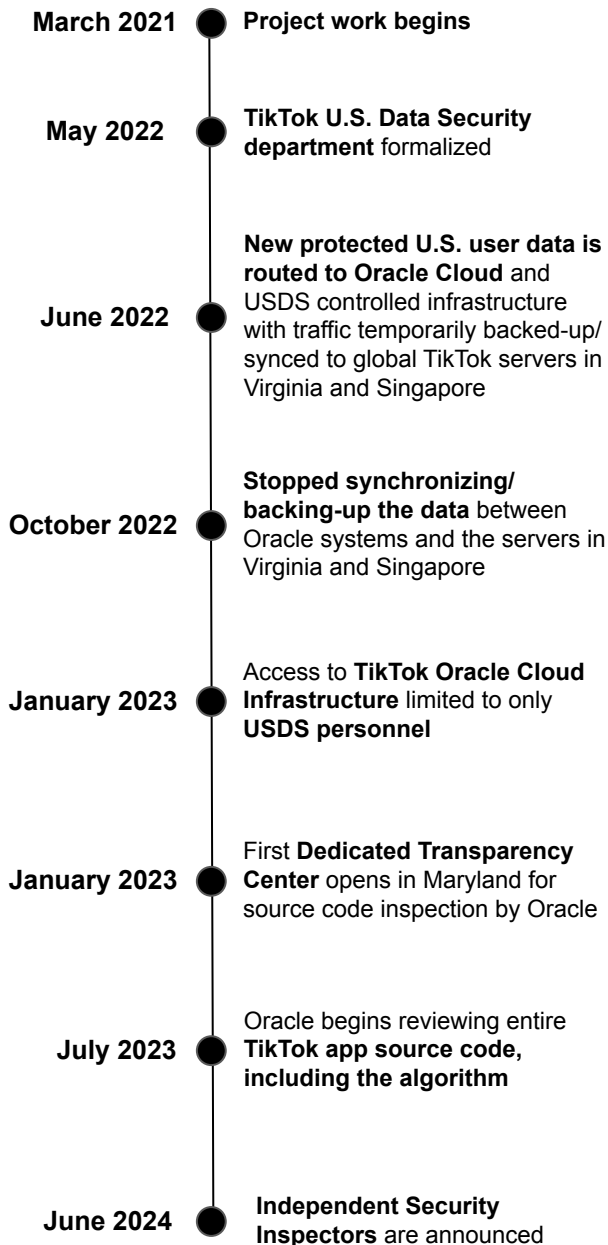# Protecting
U.S. National Security Interests

TikTok takes national security concerns seriously and continues to take proactive steps to ensure U.S. user data is protected through TikTok U.S. Data Security (USDS)—an entity designed to address national security concerns and maintain transparency and oversight.

March 2021 — Project work begins

May 2022 — **TikTok U.S. Data Security department** formalized

June 2022 — **New protected U.S. user data is routed to Oracle Cloud** 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** limited to only **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, including the algorithm**

June 2024 — **Independent Security Inspectors** are announced

TikTok U.S. Data Security Inc.

TikTok created a new organization called **TikTok U.S. Data Security Inc.** in May of 2022, which controls access to protected U.S. user data, content recommendation, and moderation systems in the secure Oracle Cloud.

- 2,400+ TikTok U.S. Data Security Employees

- Teams include **Engineering, User Business Operations, Trust and Safety, Privacy, Security Operations, Legal, E-Commerce, Finance**, and more.

A Secure Environment for the U.S. App

- Protected U.S. user data is **stored by default in the Oracle Cloud** with controlled and monitored gateways.
- **Only approved USDS personnel have access** to protected U.S. user data in the Oracle cloud.
- **All business functions** that require access to protected U.S. user data are part of USDS.

♪ TikTok

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**: Name, email, birthdate.
- **Behavioral data:** Interactions, likes, video views.
- **Device/network data:** IP address

Only USDS personnel are able to access protected US TikTok user data in the Oracle environment, unless authorization is given by USDS pursuant to limited exceptions, such as for legal and compliance purposes.

Preventing Backdoors and Content Manipulation

Source Code: Oracle and Independent Security Inspectors analyze and validate source code, including mobile app code, backend services, third-party libraries, and recommendation algorithms.

Recommendation System + Algorithm: Oracle and the Independent Security Inspectors examines recommendation systems to confirm alignment with platform guidelines and transparency standards.

Dedicated Transparency Centers (DTCs)

Our **Dedicated Transparency Centers (DTC)** provide trusted third parties, such as Oracle and the Independent Security Inspectors, with access to TikTok's full source code, including the algorithms that power our recommendation system.The reviews focus on:

- **Algorithms:** Examines recommendation systems to confirm alignment with platform guidelines.
- **Mobile App Code:** Verifies security and functionality of the TikTok app.
- **Backend Services:** Provides secure infrastructure supporting the app.
- **Third-Party Libraries:** Identifies and addresses risks from external code integrations.

While providing full transparency, the DTCs also safeguard TikTok's proprietary technology and sensitive information.

♪ TikTok