

DATA PRIVACY &amp; GOVERNANCE HUB

# What TikTok's Updated Privacy Policy Reveals About U.S. Data Protection

APRIL 5, 2026

## Key Takeaways

- TikTok's updated privacy policy now includes the collection of a user's precise location data as well as the ability to process sensitive personal information.
- Although the app was divested to a U.S. joint venture earlier this year to address national security concerns, users are now increasingly worried about their own government's ability to access and use their sensitive data.
- Current regulatory frameworks may be insufficient to address these concerns, exposing the precarity of operating without clear federal rules around data privacy.

## What Happened

TikTok, one of the most popular social media apps available, recently updated its privacy policy, sparking concern among users about what kind of data is being collected and how it's being used. Last year, Americans were temporarily banned from the app due to the passage of a U.S. federal regulation, the [Protecting Americans From Foreign Adversary Controlled Applications Act](#), which required the app to be divested or banned for national security concerns.

A Chinese parent company, ByteDance, then owned the platform, and [lawmakers were uncomfortable](#) with the amount of user data a foreign adversary was gathering on American citizens, in tandem with their potential to manipulate the algorithm, spread disinformation, or illicit propaganda. ByteDance was also partially owned by the state of China, and, with the massive number of American users, this law was passed in an effort to keep Americans' data

safer. TikTok was finally [sold](#) to a conglomerate of American companies earlier this year and is currently operating under a U.S. joint venture.

## **Privacy and Governance Concerns**

Unfortunately, the [concerns](#) regarding data privacy did not end with this shift in ownership. Users noticed shortly after the divestment that, when they opened the app, a new pop-up prompted them to agree to TikTok's updated privacy policy terms and conditions.

One of the biggest changes in the policy is the [collection of a user's precise location data](#), which can be as accurate as [pinpointing](#) the floor of an apartment building. Although some aspects of this location update can be disabled, the app can still track a user's IP address, just as many other social media platforms do.

The [policy](#) also outlines that TikTok can process "racial or ethnic origin, national origin, religious beliefs, mental or physical health diagnosis, sexual life or sexual orientation, status as transgender or nonbinary, citizenship or immigration status, or financial information." This phrasing in particular has left users on high alert, even more so as Trump's crackdown on immigration enforcement continues in major cities across the U.S.

The policy does not state that TikTok is scouring accounts for this information, but rather that it is collecting the data as it appears in any content the user creates or interacts with. The collection of this data is likely to bolster personalized [ad targeting](#). Users' concerns still ring true, however, considering the U.S. government regularly calls upon social media platforms through the legal process, and they are required by law to comply.

The old privacy policy was not as clear or detailed, but the [California Consumer Privacy Act](#) requires the new U.S. owners to inform users about what data is collected about them, painting a clearer picture of what engaging with the platform truly entails. The aggregation of precise location data alongside sensitive personal information creates a detailed profile of users that, in the wrong hands, could be used to target, discriminate against, or surveil vulnerable individuals. The concentration of this information makes TikTok a valuable target to potential threat actors, particularly given the volume and sensitivity of personal data it stores.

## Why It Matters / Policy Considerations

It appears that even though the app was forced to be sold to American companies due to concerns about data privacy and national security, [citizens now remain worried](#) about their own government's ability to collect sensitive information and use it against them. Current policy only mandates clarity about the type of information collected and does not address disclosure of how the information is being used.

TikTok's new ownership and updated data privacy policy force Americans to reckon with their willingness to share sensitive personal data in a digital landscape where that data can be gathered, shared, and potentially exploited by both social media platforms and, possibly, the government. The absence of a federal data privacy law leaves a fragmented landscape in which protections vary by state, creating inconsistent standards and significant gaps in user privacy. Transparency and accountability would be bolstered by a policy that gives users a clear idea not only of what data is being collected but also of how it is being used.