



TikTok Now Collects Biometric Data of U.S. Users

Chinese-owned social media-platform TikTok made an update to its U.S. privacy policy last week. The massively popular video app, which in 2020 [had](#) 80 million active users in America and growing, will now collect the biometric data of its users, including faceprints and voiceprints.

The biometric data-collection details were introduced in the newly added section, “Image and Audio Information,” found under the heading of “Information we collect automatically,” in [the policy](#). This is the part of TikTok’s privacy policy that lists the types of data the app gathers from users, which was already fairly extensive, and included, among other provisions, content of the private messages the users send to each other, location, and phone and social-media contacts.

The first part of the new section explains that TikTok may collect information about the images and audio that are in users’ content, “such as identifying the objects and scenery that appear, the existence and location within an image of face and body features and attributes, the nature of the audio, and the text of the words spoken in your User Content.”

Tech Crunch, which first reported the update, [says](#): “While that may sound creepy, other social networks do object recognition on images you upload to power accessibility features (like describing what’s in an Instagram photo, for example), as well as for [ad targeting](#) purposes. Identifying where a person and the scenery is can help with AR [augmented reality] effects, while converting spoken words to text helps with features like [TikTok’s automatic](#) captions.”

{modulepos inner_text_ad}

The policy states that this data collection is for enabling “special video effects, for content moderation, for demographic classification, for content and ad recommendations, and for other non-personally-identifying operations.”

The surroundings of a user that they capture with their phone and audio that accompanies the recording will now be collected.

But even more concerning is a part of the new section that references a collection of biometric data.

The policy now states, “We may collect biometric identifiers and biometric information as defined under US laws, such as faceprints and voiceprints, from your User Content. Where required by law, we will seek any required permissions from you prior to any such collection.”

[Biometric identifiers](#) are biologically unique data (e.g. fingerprints, genetic data, and voiceprints) that identify a person. Under provisions of Health Insurance Portability and Accountability [Act](#) of 1996





Written by [Veronika Kyrylenko](#) on June 6, 2021

(HIPAA), biometric identifiers are protected health information that must be held in strict confidence by healthcare agencies and professionals.

While the privacy policy explains why TikTok allegedly needs to collect scenery information, it fails to explain the purpose for collecting face- and voiceprints.

As for the laws regulating biometric collection, in the United States, there is no single, comprehensive federal law regulating the collection and use of personal data in general, or biometric data in particular.

Instead, [explains](#) the tech company *Thales*, the country has a patchwork system of federal and state laws and regulations that can sometimes overlap or contradict one another. In addition to that, government agencies and industry groups have developed self-regulatory guidelines. The company notes how powerful technologies involving artificial intelligence — such as facial recognition — have become.

There are just a handful of U.S. states with biometric privacy laws, including Illinois, Washington, California, Texas, and New York. If TikTok only requested consent “where required by law,” it could mean users in most states would not have to be informed about the biometric data collection or asked for permission to do so.

In 2020, President Trump attempted to ban TikTok, along with another Chinese app, WeChat — which includes messaging, social media, and payment platforms — due to national-security concerns.

“This data collection threatens to allow the Chinese Communist Party access to Americans’ personal and proprietary information — potentially allowing China to track the locations of federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage,” read the text of Trump’s [executive order](#).

TikTok and TikTok users [filed](#) various lawsuits against Trump’s order. In October and December, two federal judges [ruled](#) in separate cases against the administration’s ban, effectively blocking the government from carrying it out.

Trump filed an appeal, and when President Biden took office, his administration put the appeal process on hold as it reviewed the actions taken by his predecessor.

In February, [TikTok paid \\$92 million](#) to settle a class-action lawsuit in Illinois over allegations that it violated the state’s biometric data privacy law.

According to a [study](#) of 96 countries by U.K.-based technology firm Comparitech, China has been ranked the world’s worst offender for its invasive use of biometric data, followed by Costa Rica and Iran. The fourth place is shared by the United States, Saudi Arabia, United Arab Emirates, Bangladesh, the Philippines, and Uganda.



Subscribe to the New American

Get exclusive digital access to the most informative, non-partisan truthful news source for patriotic Americans!

Discover a refreshing blend of time-honored values, principles and insightful perspectives within the pages of "The New American" magazine. Delve into a world where tradition is the foundation, and exploration knows no bounds.

From politics and finance to foreign affairs, environment, culture, and technology, we bring you an unparalleled array of topics that matter most.



What's Included?

- 24 Issues Per Year
- Optional Print Edition
- Digital Edition Access
- Exclusive Subscriber Content
- Audio provided for all articles
- Unlimited access to past issues
- Coming Soon! Ad FREE
- 60-Day money back guarantee!
- Cancel anytime.

Subscribe