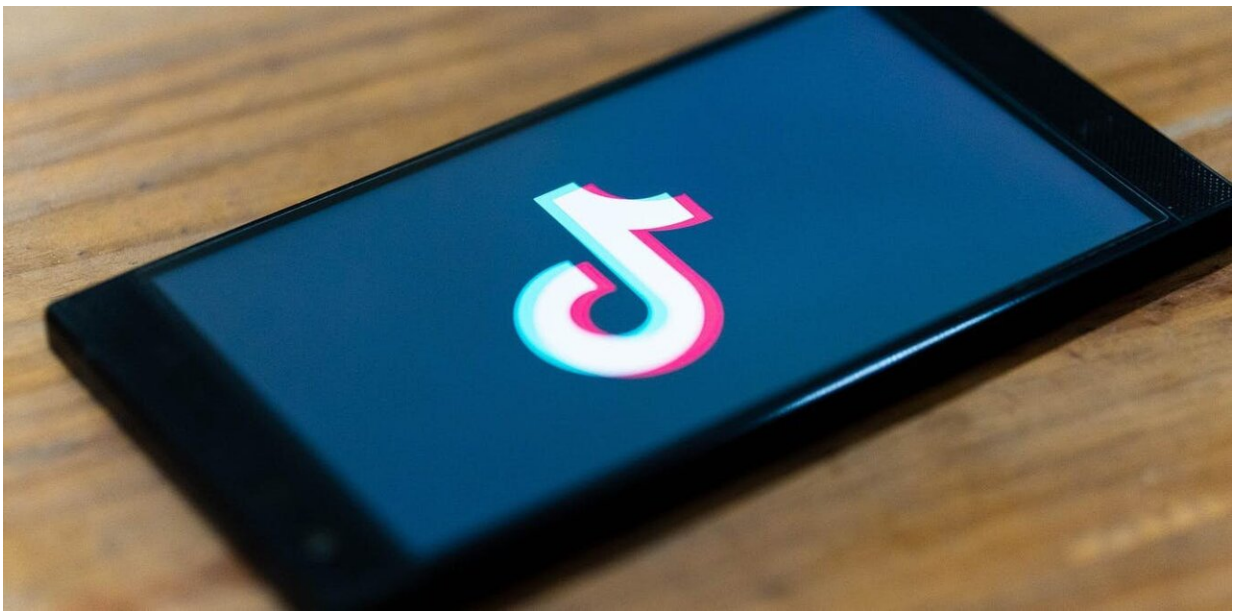
Concerns over TikTok feeding user data to Beijing are back, and there's good evidence to support them

July 6 2022, by David Tuffley



Credit: Pixabay, CC BY-SA

When English statesman Sir Francis Bacon famously said "knowledge is power," he could hardly have foreseen the rise of ubiquitous social media some 500 years later.

Yet social media platforms are some of the world's most powerful businesses—not least because they can collect massive amounts of user

data, and use algorithms to turn the data into actionable knowledge.

Today, TikTok has some of the best algorithms in the business, and a suite of data-collection mechanisms.

This is how it manages to be so addictive, with some 1.2 billion users as of December 2021. This number is expected to rise to 1.8 billion by the end of the year.

It's against the background of these huge numbers that the U.S. Federal Communications Commission (FCC) wrote a strongly worded letter to the chief executives of Apple and Google last Tuesday, urging them to remove TikTok from their app stores on the grounds that the company—or more precisely its Chinese parent ByteDance—can't be trusted with U.S. users' data.

What are the concerns?

In his letter, FCC commissioner Brendan Carr says: "TikTok is owned by Beijing-based ByteDance—an organization that is beholden to the Communist Party of China and required by the Chinese law to comply with the PCR's [(People's Republic of China)] surveillance demands."

TikTok's privacy policy says it won't sell personal information to third parties, but reserves the right to use information internally for business development purposes. That internal use may include use by its parent company, ByteDance.

TikTok U.S. has repeatedly denied breaching U.S. data privacy regulations. It says user data are stored on U.S. servers and not shared with ByteDance. But Carr says these measures fall short of guaranteeing the privacy of U.S. users: "TikTok's statement that '100% of U.S. user traffic is being routed to Oracle' (in the U.S.) says nothing about where

that data can be accessed from."

Following robust questioning by U.S. senators, TikTok has admitted its U.S.-stored data are in fact accessible from China, subject to unspecified security protocols at the U.S. end.

Australian users also have their data stored on U.S. servers, with backups in Singapore. But it's not known whether these data—which could include users' browsing habits, images, biographical information and location—are subject to the same safeguards as the U.S. data.

Leaked audio

The unusually blunt language from Carr may have been occasioned by leaked audio obtained by Buzzfeed from more than 80 internal TikTok meetings.

According to a Buzzfeed report from mid-June, China-based employees of ByteDance have repeatedly accessed non-public data about U.S. TikTok users. The tapes overwhelmingly contradict TikTok's earlier data privacy assurances.

For example, in a September 2021 meeting a senior U.S.-based TikTok manager referred to a Beijing-based engineer as a "master admin" who "has access to everything." That same month a U.S.-based staffer in the Trust and Safety Department was heard saying "everything is seen in China."

In short, the recordings corroborate the claim that China-based employees have often accessed U.S. data, and more recently than earlier statements asserted.

Might it all be harmless?

On the one hand TikTok is in the business of entertaining users, with a goal to keep them on the platform and expose them to targeted advertising. On the other hand, TikTok can be used to spread misinformation and influence users to their detriment.

It has been shown to host COVID conspiracy theories and other medical misinformation, and was reportedly used with a goal to influence Kenya's general elections coming up in August.

Seen in this weaponized context, the U.S. government's strenuous objections to TikTok come into clearer focus.

Moreover, past events have also raised good reason to suspect Chinese actors of mass data harvesting online.

In 2020, Australian media outlets reported on a data leak from Zhenhua Data, a Chinese company with clients including the Chinese government and the People's Liberation Army.

The leak was said to contain data on more than 35,000 Australians—including dates of birth, addresses, marital status, photographs, political associations, relatives and social media accounts. This information was gathered from a range of sources, including TikTok.

Would banning TikTok be effective?

Removing TikTok from Google's and Apple's app stores can only be done on a country-by-country basis. India banned the platform in June 2020.

If the Australian government were to make the TikTok domain inaccessible from Australia, it could still be accessed through a virtual private network (VPN). A VPN service allows users to create a secure private network within a public one, thus disguising their country of origin. It's the same tool that allows file-sharing on Pirate Bay and access to other countries' Netflix programs.

But even if TikTok was banned in Australia and had access removed, or if users mass-terminated their accounts, existing data on the company's U.S. and Singapore-based servers would remain there. And we now know these data are accessible to TikTok's parent company, ByteDance, in Beijing.

What should TikTok users do?

Like any technology, TikTok itself is neither good nor bad. But the way in which it's used creates potential for both.

The best defense with any potentially dangerous technology is to approach it with healthy skepticism and share as little as possible. In the case of TikTok (and other social media) this may involve:

- not disclosing your full name
- not disclosing your age and birthday
- not disclosing your physical location (including through pictures or video)
- turning off the "suggest your account to others" setting.

You can also request an account deletion. But don't expect TikTok to delete all the data associated with it. That's TikTok's data now, and you agreed to handing it over when you signed up.

This article is republished from The Conversation under a Creative

Commons license. Read the original article.

Provided by The Conversation