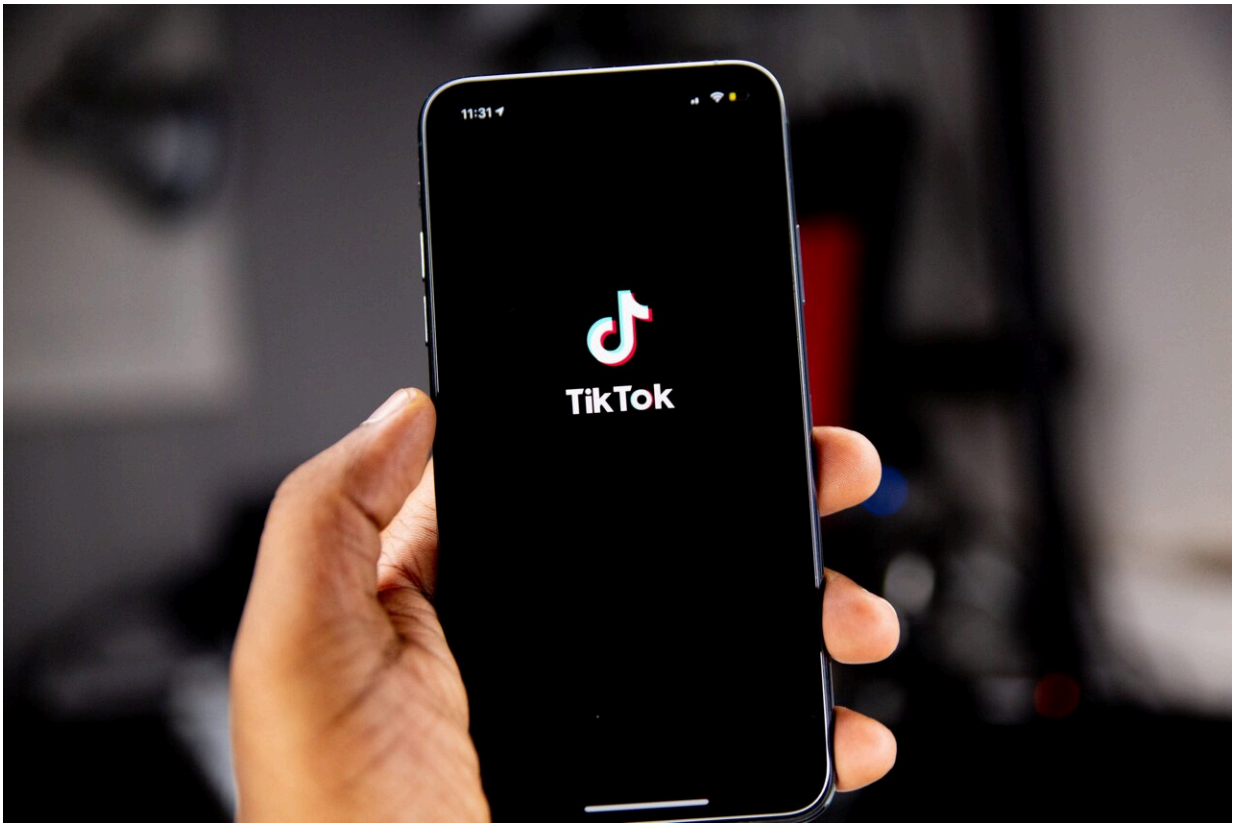
Is TikTok stealing more than just your time?

December 22 2022, by Lisa Ercolano



Credit: Unsplash/CC0 Public Domain

More than 86 million Americans use the social media app TikTok to create, share, and view short videos, featuring everything from cute animals and influencer advice to comedy and dance performances. Though users consider the app harmless fun, a growing number of cybersecurity experts and elected officials aren't so sure.

They point out that TikTok's parent company, the Beijing-based ByteDance, has been accused of working with the Chinese government to censor content and could also collect sensitive data on users. To date, at least 14 U.S. states have enacted legislation or created rules blocking government computers' access to the app, and a bipartisan bill introduced last week in Congress seeks a ban on the app for all U.S. users.

Christopher Wray, FBI director, spoke publicly on the issue earlier this month, warning that control of the popular social media app is in the "hands of a government that doesn't share our values."

Cybersecurity expert Anton Dahbura, executive director of the Johns Hopkins University Information Security Institute, sat down with the Hub to discuss the issue.

Critics of TikTok warn that it could be used to collect data on millions of users. Is this a realistic worry?

Yes, it's very much a realistic concern. For instance, basic information such as the locations of users of the app can be used by foreign actors to determine whether someone works in a facility that may be of interest, such as a military or other government facility. But manufacturing, high tech, food production, educational institutions, and many other facilities are also of interest. For instance, the Chinese government was accused of a data breach of a Marriott Hotel customer database, allegedly to find out who had been staying there.

The Chinese government has a long history of intellectual property theft, so the scope of what they're looking for goes well beyond classified information or disruptive attacks, but extends to industrial espionage to obtain proprietary information. And they can quickly sort through

millions of records to find the persons that are of interest to them. They have the ability to connect people, so their interest isn't limited to people who actually work at key facilities, but also their friends, and even people who live nearby or in the same building. Once they have a person of interest, they can use them in different ways to obtain what they want, such as gaining access through nefarious means to an enterprise system where the person works by launching very specific phishing attacks against the person. Sooner or later, they'll find a way in.

The average person may find it hard to believe that the Chinese government would have any interest in their information. Should they be more concerned?

The Chinese government has the resources to assemble information in ways that most of us haven't thought of. Many people don't realize that they, their friends, family, neighbors or associates are likely to have something that the Chinese government wants and that can compromise or damage the United States. As they say, it's far better to be safe than sorry.

Some warn that using TikTok could expose Americans to information requests from the Chinese government, though TikTok claims it rigorously protects users' information and outlines its privacy policies when users enroll. Should users feel their information is secure?

Although the legal aspects of this are outside of my areas of expertise, I would venture to say that all bets are off when it comes to the Chinese government gaining access to Americans' personal information, regardless of the attempts to set up a legal framework for that access.

Any potential security threat would certainly supersede a user agreement.

Some have raised the issue that the app could be used to compromise/alter the software of TikTok users' devices, potentially even taking control of those devices. Is this a realistic concern?

It's a possibility, although in the case of the Chinese government, their primary motive is the acquisition of information. They have figured out how to tie pieces of information together for their purposes in ways that most of us had never imagined. FBI Director Christopher Wray has expressed general concerns about the Chinese government having access to the software in phones for cyber operations such as espionage or disruption of computers, mobile devices, and critical infrastructure, but there hasn't been a specific revelation about this.

How about the notion that ByteDance could manipulate and curate content intended to influence Americans' views on issues important to China?

This is an issue that we should be concerned about across all social media platforms. There hasn't been any specific information by the U.S. authorities about TikTok manipulating content. Although FBI Director Wray has expressed general concern, I believe that for the moment we should focus on the larger issue of bias in social media in general, especially when the bias and/or misinformation is amplified by the algorithms the companies use to manage the flow of content.

Why are people so concerned about TikTok and not about Chinese-manufactured Apple products?

The difference is that FBI Director Wray raised the specific issue regarding TikTok and referred to TikTok as a "serious threat." Of course, the U.S. government has banned the sale and import of communications from a number of telecommunications companies, including Huawei, so when there is a credible threat, we're seeing the U.S. government take decisive action. To my knowledge, there is no concern about Apple products that are manufactured in China.

Provided by Johns Hopkins University